PARKING MANAGEMENT INFORMATION SYSTEM (PMIS) AGREEMENT

THIS AGREEMENT ("Agreement") is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City") and **PASSPORT LABS, INC**., a Delaware corporation, registered to do business in Colorado, whose address is 128 S. Tryon St., Charlotte, North Carolina 28202 ("Contractor"), jointly "the parties."

RECITALS

WHEREAS, the City desires to retain a qualified Contractor to provide the City with specialized equipment, ministerial services, professional experience and expertise and other assistance and support specified in this Agreement and necessary to assist and support the City in successfully implementing and operating a complete, fully functional PMIS within the City; and

WHEREAS, the desired PMIS and all related services shall include, at a minimum, all required equipment, hardware, software, communication networks, database management functions, provision for read-only access to the database as specified by the City's Executive Director of the Department of Transportation and Infrastructure or the Chief Information Officer or their designees, report and recordkeeping functions, form, report and notice generation capabilities, a DMV interface, a fully compatible hand-held citation system, comprehensive collection and accounting functions, and all other professional, operational, maintenance, training and support services necessary to provide to the City a fully tested, operational and compatible PMIS; and

WHEREAS, the scope of the project involves both permitting and enforcement in this single agreement and the City may choose to eliminate either functionality without impacting the remaining functionality: and

WHEREAS, the City has therefore determined to contract with the Contractor for these purposes; and

WHEREAS, the Contractor represents that it has the present capacity and is experienced and qualified to perform; and

WHEREAS, the Contractor has agreed to provide the hosted solution under the terms and conditions as set out below.

WHEREAS, the Contractor is willing and able to perform, in accordance with the terms and conditions of this Agreement, as an independent Contractor.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the City and Contractor incorporate the recitals set forth above and the parties mutually agree as follows:

SECTION 1. DEFINITIONS.

Whenever used herein, any schedules, exhibits, order forms, or addenda to this Agreement, the following terms shall have the meanings assigned below unless otherwise defined therein. Other capitalized terms used in this Agreement are defined in the context in which they are used.

1.1. "Acceptance" means the Deliverable demonstrates to the City's reasonable satisfaction that the Deliverable conforms to and operates in all material respects according to the Acceptance Criteria, and if required, has successfully completed Acceptance Testing in all material respects, and for Deliverables not requiring Acceptance Testing that the Deliverable reasonably conforms in all material respects to the Acceptance Criteria or the City's requirements.

1.2. "**Acceptance Certificate**" means a written instrument by which the City promptly notifies Contractor that a Deliverable has been Accepted or Accepted with exceptions, and Acceptance Criteria have been met or waived, in whole or in part.

1.3. "**Acceptance Criteria**" means functionality and performance requirements determined by the City and set forth on the Order Form for the applicable Product or Service, based upon the Specifications, which must be satisfied prior to City's Acceptance of a Deliverable, or the System. City and Contractor shall agree upon written Acceptance Criteria in the Order Form for the applicable Product or Service.

1.4. "**Acceptance Date**" means the date on which the City issues an Acceptance Certificate for the System or a Deliverable.

1.5. "**Acceptance Test**" means the evaluation and testing method, procedures, or both, that are set forth in the Order Form for the applicable Product or Service and are used to determine whether or not the System or a Deliverable requiring Acceptance Testing performs in accordance with the Acceptance Criteria.

1.6. "**Agreement**" means this Parking Management Services Agreement between City and Contractor, inclusive of all schedules, exhibits, attachments, addenda, and other documents incorporated by reference between the City and Contractor, Contract Number 202262615.

1.7. "**City Data**" means all information, whether in oral or written (including electronic) form, created by or in any way originating with City and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with City, in the course of using and configuring the Services provided under this Agreement, and includes all records relating to the City's use of Contractor Services. City Data also includes Confidential Information disclosed to Contractor.

1.8. "**Cloud Unavailability**" means a running virtual machine stops functioning due to cloud infrastructure failure below the applicable commitment level, and such failure is recorded in Contractor's trouble ticket system.

1.9. "**Confidential Information**" means any and all records or data that is disclosed in written, graphic or machine recognizable form and is marked, designated, labeled or identified at

the time of disclosure as being confidential or its equivalent, or, if the information is in verbal form, it is identified as confidential or proprietary at the time of disclosure and is confirmed in writing within thirty (30) Calendar Days of the disclosure and is not subject to disclosure under CORA. Confidential Information shall include, but is not limited to, PII, PHI, PCI, Tax Information, CJI, personnel records, financial, statistical, personnel, human resources data or Personally Identifiable Information and/or Personal Information as described in the C.R.S 24-73-101, et seq; attorney/client privileged communications; information which is exempt per federal laws (including but not limited to copyright, HIPPA), all of which is not subject to disclosure under CORA. Confidential Information does not include information which: (a) is public or becomes public through no breach of the confidentiality obligations herein; (b) is disclosed by the party that has received Confidential Information (the "Receiving Party") with the prior written approval of the other party; (c) was known by the Receiving Party at the time of disclosure; (d) was developed independently by the Receiving Party without use of the Confidential Information; (e) becomes known to the Receiving Party from a source other than the disclosing party through lawful means; (f) is disclosed by the disclosing party to others without confidentiality obligations; or (g) is required by law to be disclosed.

1.10. "**CORA**" means the Colorado Open Records Act, §§24-72-200.1, et. seq., C.R.S.

1.11. "**Critical Incident**" means that City's Service (whether colocation or Cloud) is unavailable or has been materially impacted.

1.12. "**Data Incident**" means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of any communications or information resources of the City. Data Incidents include, without limitation (i) successful attempts to gain unauthorized access to a City system or City information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a City system for the processing or storage of data; or (iv) changes to City system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent. It shall also include any actual or reasonably suspected unauthorized access to or acquisition of computerized City Data that compromises the security, confidentiality, or integrity of the City Data, or the ability of City to access the City Data.

1.13. "**Deliverable**" means the Products or Services or documents or tangible work products described in an Order Form to be provided to the City by Contractor or the outcome to be achieved or output to be provided, in the form of a tangible object or software that is produced as a result of Contractor's work that is intended to be delivered to the City by Contractor under this Agreement.

1.14. "**Documentation**" means, collectively: (a) all materials published or otherwise made available to City by Contractor that relate to the functional, operational and/or performance capabilities of the Services; (b) all user, operator, system administration, technical, support and other manuals and all other materials published or otherwise made available by Contractor, including marketing materials that describe the functional, operational and/or performance capabilities of the Services; (c) any Requests for Information and/or Requests for Proposals (or documents of similar effect) issued by City, and the responses thereto from Contractor, and any document which purports to update or revise any of the foregoing; and (d) the results of any

Contractor "Use Cases Presentation", "Proof of Concept" or similar type presentations or tests provided by Contractor to City or as required to be produced by Contractor subject to the terms of this Agreement. .

1.15. "**Downtime**" means any period of time of any duration that the Services are not made available by Contractor to City for any reason, including scheduled maintenance or Enhancements.

1.16. "**Effective Date**" means the date on which this Agreement is fully approved and signed by the City as shown on the Signature Page for this Agreement. The Effective Date for Services may be set out in an Order Form or similar exhibit.

1.17. "**Enhancements**" means any improvements, modifications, upgrades, updates, fixes, revisions and/or expansions to the Services that Contractor may develop or acquire and incorporate into its standard version of the Services or which the Contractor has elected to make generally available to its customers.

1.18. "**Equipment**" means any hardware, machinery, device, tool, computer, computer component, computer system, including add-ons, or peripherals of tangible form together with the necessary supplies for upkeep and maintenance, and other apparatus, to be provided to the City by Contractor under this Agreement.

1.19. "**Error**" means any defect, problem, condition, bug, or other partial or complete inability of a Product to operate in accordance with the applicable Specifications.

1.20. "**Intellectual Property Rights**" includes without limitation all right, title, and interest in and to all (a) Patent and all filed, pending, or potential applications for Patent, including any reissue, reexamination, division, continuation, or continuation in part applications throughout the world now or hereafter filed; (b) trade secret rights and equivalent rights arising under the common law, state law, and federal law; (c) copyrights, other literary property or authors rights, whether or not protected by copyright or as a mask work, under common law, state law, and federal law; and (d) proprietary indicia, trademarks, trade names, symbols, logos, and/or brand names under common law, state law, and federal law.

1.21. "**Order Form**" means a quote in the form attached hereto as an Exhibit, setting forth certain Products and/or Services to be provided pursuant to this Agreement. Any reference to an "Order Form" in this Agreement includes Products and/or Services purchased by City pursuant to Contractor's online ordering process. An Order Form can also be a statement of work or scope of work if attached to this Agreement.

1.22. "**PCI**" means payment card information including any data related to credit card holders' names, credit card numbers, or other credit card information as may be protected by state or federal law.

1.23. "**PII**" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother 's

maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§24-72-501 and 24-73-101, C.R.S.

1.24. "**PHI**" means any protected health information, including, without limitation any information whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes, but is not limited to, any information defined as Individually Identifiable Health Information by the federal Health Insurance Portability and Accountability Act. If this Agreement involves the transmission of PHI a separate Business Associates Agreement will become a part of this Agreement.

1.25. "**Product(s)"** means software, Equipment, and supplies delivered, or to be delivered, pursuant to an Order Form.

1.26. "**Protected Information**" includes, but is not limited to, personally-identifiable information, student records, protected health information, criminal justice information or individual financial information and other data defined under §24-72-101 et seq., and personal information that is subject to local, state or federal statute, regulatory oversight or industry standard restricting the use and disclosure of such information. The loss of such Protected Information would constitute a direct damage to the City.

1.27. "**Project Manager**" means the individual who shall serve as each party's point of contact with the other party's personnel as provided in this Agreement.

1.28. "**RFP Response**" means any proposal submitted by Contractor to City in response to City's Request for Proposal ("RFP") titled PARKING MANAGEMENT INFORMATION SYSTEM, 0621A2021, July 1, 2021.

1.29. "**Service**" means Contractor's computing solutions, provided to City pursuant to this Agreement, that provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces. Service also includes all professional services provided under the Agreement.

1.30. "**Service Level Agreement**(s)" mean the provisions set forth on Attachment F attached hereto, which are incorporated into this Agreement by this reference.

1.31. "**Specifications**" means the most current cumulative statement of capabilities, functionality, and performance requirements for the Products or Services as set out in the Acceptance Criteria, Order Forms, Documentation, Contractor's representations, Contractor's proposal, and the City's Request for Proposals.

1.32. "**Subcontractor**" means any third party engaged by Contractor to aid in performance of the work or the Service. Contractor shall provide to the City upon request a list of Subcontractors providing material services to the Service.

1.33. "**System**" means the operational combination of all Products and Services to be provided by Contractor to City under this Agreement.

1.34. "**Third Party**" means persons, corporations, and entities other than Contractor, City or any of their employees, contractors, or agents.

1.35. "**Third Party Host**" means the entity where the physical location of the server(s) of the Contractor's software resides.

SECTION 2. RIGHTS AND LICENSE IN AND TO DATA.

2.1. The parties agree that as between them, all rights in and to City Data shall remain the exclusive property of City, and Contractor has a limited, nonexclusive license to access and use City Data as provided in this Agreement solely for the purpose of performing its obligations hereunder.

2.2. All City Data created and/or processed by the Service is and shall remain the property of City and shall in no way become attached to the Service, nor shall Contractor have any rights in or to the City Data without the express written permission of the City and may not include Protected Information, with the exception of activity data.

2.3. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

2.4. The City retains the right to use the Service to access and retrieve data stored on Contractor's Service infrastructure at any time during the term of this Agreement at its sole discretion.

2.5. Operational Data is data specific to City's operation that is provided to by City to Passport to be used in the configuration and provision of the passport System for Customer's use. Operational Data is specific to City's operation, which is not available to Passport publicly or by other means. Operational Data may include, but is not limited to, zone information, rate information, operational schedules, business metrics, business rules, parking and other inventory and assets, and relevant details of partner agreements. In each case, Operational Data may refer to past, present, or future states of such items. Operational Data is the sole and exclusive property of City. City grants passport a license to use the City's Operational Data on a case by case basis where it is not otherwise considered proprietary by a third party, during the term of this Agreement for purposes of this Agreement.

SECTION 3. DATA PRIVACY.

3.1. Contractor will use City Data only for the purpose of fulfilling its duties under this Agreement and for the City's sole benefit and will not share City Data with or disclose it to any Third Party without the prior written consent of the City or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use City Data for Contractor's own benefit and, in particular, will not engage in "data mining" of City Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the City.

3.2. Contractor will provide access to City Data only to those Contractor employees, contractors, and Subcontractors ("Contractor Staff") who need to access City Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to City Data, Contractor Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of City Data they will be handling.

3.3. If Contractor receives Protected Information of a Colorado resident under this Agreement, Contractor shall implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of Contractor's business and its operations. Unless Contractor agrees to provide its own security protections for the information it discloses to a third-party service provider, Contractor shall require all its third-party service providers to implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information disclosed and reasonably designed to help protect the personal identifying information subject to this Agreement from unauthorized access, use, modification, disclosure, or destruction. Contractor and its third-party service providers that maintain electronic or paper documents that contain Protected Information under this Agreement shall develop a written policy for the destruction of such records by shredding, erasing, or otherwise modifying the Protected Information to make it unreadable or indecipherable when the records are no longer needed.

3.4. Contractor may provide City Data to its agents, employees, assigns, and Subcontractors as necessary to perform the work under this Agreement, but shall restrict access to Confidential Information to those agents, employees, assigns, and Subcontractors who require access to perform their obligations under this Agreement. Contractor shall ensure all such agents, employees, assigns, and Subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force at all times the agent, employee, assign, or Subcontractor has access to any Confidential Information. Contractor shall provide copies of those signed nondisclosure provisions to the City upon execution of the nondisclosure provisions if requested by the City.

SECTION 4. DATA SECURITY AND INTEGRITY.

4.1. All facilities, whether Contractor hosted or Third-Party Hosted, used to store and process City Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to provide the requested Service availability and to secure City Data from unauthorized access, destruction, use, modification, or disclosure appropriate for City Data. Such measures, when applicable due to the presence of Protected Information, include, but are not limited to, all applicable laws, rules, policies, publications, and guidelines including, without limitation: (i) the most recently promulgated IRS Publication 1075 for all Tax Information, (ii) the most recently updated PCI Data Security Standard from the PCI Security Standards Council for all PCI, (iii) the most recently issued version of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy for all CJI, (iv) the Colorado Consumer Protection Act, (v) the Children's Online Privacy Protection Act (COPPA), (vi) the Family Education Rights and Privacy Act (FERPA),

(vii) §24-72-101 et seq., (viii) the Telecommunications Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers (TIA-942); (ix) the federal Health Insurance Portability and Accountability Act for all PHI and the HIPAA Business Associate Addendum attached to this Agreement, if applicable. Contractor shall submit to the Manager, within fifteen (15) days of the Manager's written request, copies of Contractor's policies and procedures to maintain the confidentiality of protected health information to which Contractor has access, and if applicable, Contractor shall comply with all HIPAA requirements contained herein or attached as an exhibit.

4.2. Contractor warrants that all City Data will be encrypted in transmission (including via web interface) and in storage by a mutually agreed upon National Institute of Standards and Technology (NIST) approved strong encryption method and standard.

4.3. Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting in providing Services under this Agreement. Contractor shall ensure that any underlying or integrated software employed by the Service is updated on a regular basis and does not pose a threat to the security of the Service.

4.4. Contractor shall, and shall cause its Subcontractors, to do all of the following:

(a) Provide physical and logical protection for all hardware, software, applications, and data that meets or exceeds industry standards and the requirements of this Agreement.

(b) Maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), annual security testing, and improvements or enhancements consistent with evolving industry standards.

(c) Comply with State and federal rules and regulations related to overall security, privacy, confidentiality, integrity, availability, and auditing.

(d) Provide that security is not compromised by unauthorized access to workspaces, computers, networks, software, databases, or other physical or electronic environments.

(e) Promptly report all Data Incidents, including Data Incidents that do not result in unauthorized disclosure or loss of data integrity.

(f) Comply with all rules, policies, procedures, and standards issued by the City's Technology Services Security Section.

(g) Subject to Contractor's reasonable access security requirements and upon reasonable prior notice, Contractor shall provide the City with scheduled access to Contractor's facilities for the purpose of inspecting and monitoring access and use of City Data, maintaining City systems, and evaluating physical and logical security control effectiveness.

(h) Contractor shall perform current background checks in a form reasonably acceptable to the City on all of its respective employees and agents performing services or having access to City Data provided under this Agreement, including any Subcontractors or the employees of Subcontractors. A background check performed within 30 days prior to the date such employee or agent begins performance or obtains access to City Data shall be deemed to be current.

(i) Contractor will provide notice to the security and compliance representative for the City indicating that background checks have been performed. Such notice will inform the City of any action taken in response to such background checks, including any decisions not to take action in response to negative information revealed by a background check.

(j) If Contractor will have access to Tax Information under the Agreement, Contractor shall comply with the background check requirements defined in IRS Publication 1075 and § 24-50-1002, C.R.S.

4.5. If applicable, Contractor shall use, hold, and maintain Confidential and Protected Information in compliance with all applicable laws and regulations only in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all Confidential and Protected Information.

4.6. Prior to the Effective Date of this Agreement, Contractor, will at its expense conduct or have conducted the following, and thereafter, Contractor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Incident:

(a) A SSAE 16/SOC 2 or other mutually agreed upon audit of Contractor's security policies, procedures, and controls.

(b) A quarterly external and internal vulnerability scan of Contractor's systems and facilities, to include public facing websites, that are used in any way to deliver Services under this Agreement. The report must include the vulnerability, age and remediation plan for all issues identified as critical or high.

(c) A formal penetration test, performed by a process and qualified personnel of Contractor's systems and facilities that are used in any way to deliver Services under this Agreement.

4.7. Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans, and tests within seven (7) business days of Contractor's receipt of such results.

4.8. Based on the results and recommendations of the above audits, certifications, scans and tests, Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this Agreement and provide the City with written evidence of remediation.

4.9. If (i) Contractor fails to conduct the reviews and audits described in Section 4.6 or provide the results thereof to the City as described in Section 4.7 or (ii) if the City is required by

law to conduct an audit that is not described in Section 4.6, then the City may require, at its expense, that Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results.

4.10. Contractor shall protect data against deterioration or degradation of data quality and authenticity, including, but not limited to annual Third Party data integrity audits. Contractor will provide the City the results of the above audits.

SECTION 5. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA.

5.1. Except as otherwise expressly prohibited by law, Contractor will:

(a) If required by a court of competent jurisdiction or an administrative body to disclose City Data, Contractor will notify the City in writing immediately upon receiving notice of such requirement and prior to any such disclosure.

(b) Consult with the City regarding its response.

(c) Cooperate with the City's reasonable requests in connection with efforts by City to intervene and quash or modify the legal order, demand, or request; and

(d) Upon request, provide the City with a copy of its response.

5.2. If the City receives a subpoena, warrant, or other legal order, demand or request seeking data maintained by Contractor, the City will promptly provide a copy to Contractor. Contractor will supply the City with copies of data required for the City to respond within forty-eight (48) hours after receipt of copy from the City and will cooperate with the City's reasonable requests in connection with its response.

SECTION 6. DATA INCIDENT RESPONSE.

6.1. Contractor shall maintain documented policies and procedures for Data Incident and breach reporting, notification, and mitigation. If Contractor becomes aware of any Data Incident, it shall notify the City immediately and cooperate with the City regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the City. If there is a Data Incident impacting residents of Colorado or any other jurisdiction, Contractor shall cooperate with the City to satisfy notification requirements as currently defined in either federal, state, or local law. Unless Contractor can establish that neither Contractor nor any of its agents, employees, assigns, or Subcontractors are the cause or source of the Data Incident, Contractor shall be responsible for the cost of notifying each person who may have been impacted by the Data Incident as required by law. After a Data Incident, Contractor shall take steps to reduce the risk of incurring a similar type of Data Incident in the future as directed by the City, which may include, but is not limited to, developing and implementing a remediation plan that is approved by the City at no additional cost to the City.

6.2. Contractor shall report, either orally or in writing, to the City any Data Incident involving City Data, or circumstances that could have resulted in unauthorized access to or

disclosure or use of City Data, not authorized by this Agreement or in writing by the City, including any reasonable belief that an unauthorized individual has accessed City Data. Contractor shall make the report to the City immediately upon discovery of the unauthorized disclosure, but in no event more than forty-eight (48) hours after Contractor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Contractor regarding Data Incidents will be reduced to writing and supplied to the City as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.

6.3. Immediately upon becoming aware of any such Data Incident, Contractor shall fully investigate the circumstances, extent and causes of the Data Incident, and report the results to the City and continue to keep the City informed daily of the progress of its investigation until the issue has been effectively resolved.

6.4. Contractor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

6.5. Within five (5) calendar days of the date Contractor becomes aware of any such Data Incident, Contractor shall have completed implementation of corrective actions to remedy the Data Incident, restore the City's access to the Services as directed by the City, and prevent further similar unauthorized use or disclosure.

6.6. Contractor, at its expense, shall cooperate fully with the City's investigation of and response to any such Data Incident.

6.7. Except as otherwise required by law, Contractor will not disclose or otherwise provide notice of the incident directly to any person, regulatory agencies, or other entities, without prior written permission from the City.

6.8. Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the City under law or equity, Contractor will promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any such Data Incident, including but not limited to providing notification to Third Parties whose data were compromised and to regulatory bodies, law-enforcement agencies or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Incident in such a fashion that, in the City's sole discretion, could lead to identity theft; and the payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Incident.

SECTION 7. DATA RETENTION AND DISPOSAL.

7.1. Using appropriate and reliable storage media, Contractor will regularly backup data and retain such backup copies consistent with the City's data retention policies.

7.2. At the City's election, Contractor will either securely destroy or transmit to the City repository any backup copies of City Data. Contractor will supply the City a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

7.3. Contractor will immediately preserve the state of the data at the time of the request and place a "hold" on data destruction or disposal under its usual records retention policies of records that include data, in response to an oral or written request from the City indicating that those records may be relevant to litigation that the City reasonably anticipates. Oral requests by the City for a hold on record destruction will be reduced to writing and supplied to Contractor for its records as soon as reasonably practicable under the circumstances. The City will promptly coordinate with Contractor regarding the preservation and disposition of these records. Contractor shall continue to preserve the records until further notice by the City.

SECTION 8. DATA TRANSFER UPON TERMINATION OR EXPIRATION.

8.1. Upon expiration or earlier termination of this Agreement or any Services provided in this Agreement, Contractor shall accomplish a complete transition of the Services from Contractor to the City or any replacement provider designated solely by the City without any interruption of or adverse impact on the Services or any other services provided by third parties in this Agreement. Contractor shall cooperate fully with the City or such replacement provider and promptly take all steps required to assist in effecting a complete transition of the Services designated by the City. Outside of enabling City access to data necessary for the transition, any additional transition services shall be provided by Contractor at a specified additional cost, to be scoped dependent on the required resources to complete the transition. Contractor shall extend the Agreement monthly if additional time is required beyond the termination of the Agreement, if necessary, to effectuate the transition and the City shall pay a proration of the subscription fee.

8.2. Upon the expiration or termination of this Agreement, Contractor shall return City Data provided to Contractor in a common and readily usable format if requested by the City or destroy City Data and certify to the City that it has done so, as directed by the City. If Contractor is prevented by law or regulation from returning or destroying Confidential Information, Contractor warrants it will guarantee the confidentiality of, and cease to use, such Confidential Information. To the extent that Contractor is requested to perform any services beyond the return of the City's Data in connection with termination assistance, the same shall be performed pursuant to a written statement of work under this Agreement and paid for by the City, applying Contractor's then-current rates for daily/hourly work, as the case may be.

SECTION 9. SERVICE LEVEL AGREEMENTS; INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE.

See Attachment F.

SECTION 10. COMPLIANCE WITH APPLICABLE LAWS AND CITY POLICIES.

10.1. Contractor will comply with all applicable laws and policies in performing the Services under this Agreement. Any Contractor personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to Contractor upon request. City policies regarding

TS Architecture, Data Retention, Branding, Cash Handling, IoT Policy Payment Card Industry Standards, PCI Compliance and Information Security Incident Management are attached and incorporated into this Agreement.

10.2. ADA Website Compliance:

(a) Compliance and Testing. All Contractor managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines (collectively, "Guidelines"). Prior to launching to the public, Contractor shall test all public-facing digital experiences, both manually and in an automated fashion, as applicable, to confirm and maintain compliance with the Guidelines, and then subsequently, no more than once per each term year thereafter. Such manual and automated testing may only be performed by a third party vendor approved by the Department of Justice. The City has a list of approved third party vendors. The City does not warrant the work of any third party vendor. All testing under this section shall be performed by third party vendors at the Contractor's expense.

(b) Validation, Review and Remediation. Contractor will notify City when its digital experience is ready for City review and validation. City will then validate, prior to launch and each term year thereafter, to confirm that the digital experience is compliant with the Guidelines. Manual testing of the Contractor's digital experience will be verified by City with approved vendors and individuals of varying disabilities which shall include individuals who are blind, deaf, or hard of hearing, and who have mobility or dexterity limitations. Upon completion of all testing, a review will be performed by the City's web accessibility coordinator to confirm completion of all accessibility requirements. In the event that any deficiencies are discovered in the Contractor's digital experience, City will promptly notify Contractor, and Contractor will remediate prior to launch. A digital experience will not launch until all deficiencies are remediated. All digital experiences must include a statement on the site that the experience is accessible, will maintain accessibility, and will provide a mechanism for users to submit feedback about accessibility issues.

(c) In the event that the digital experience fails compliance at any time, Contractor shall bring the digital experience into compliance within ninety (90) days, which may be extended by mutual written agreement of the Parties. Failure to bring the digital experience into compliance for any reason within such time, except as may be mutually extended by the written agreement of the parties, shall be a breach of this Agreement.

SECTION 11. WARRANTIES, REPRESENTATIONS AND COVENANTS.

Contractor represents and warrants that:

11.1. The Service will conform to applicable specifications, and operate and produce results substantially in accordance with the Documentation and the Exhibits attached hereto, and will be free from deficiencies and defects in materials, workmanship, design and/or performance during the Term of this Agreement.

11.2. All technology related services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards.

11.3. Contractor has the requisite ownership, rights, and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to the software and Services free and clear from all liens, adverse claims, encumbrances, and interests of any Third Party.

11.4. There are no pending or threatened lawsuits, claims, disputes, or actions: (i) alleging that any software or service infringes, violates, or misappropriates any Third-Party rights; or (ii) adversely affecting any software, service, or supplier's ability to perform its obligations hereunder.

11.5. The Service will not violate, infringe, or misappropriate any patent, copyright, trademark, trade secret, or other intellectual property or proprietary right of any Third Party.

11.6. The software and Services will contain no malicious or disabling code that is intended to damage, destroy, or destructively alter software, hardware, systems, or data. Contractor's obligations for breach of the Services warranty shall be limited to using its best efforts, at its own expense, to correct or replace that portion of the Services which fails to conform to such warranty, and, if Contractor is unable to correct any breach in the Services Warranty by the date which is sixty (60) calendar days after the City provides notice of such breach, the City may, in its sole discretion, either extend the time for Contractor to cure the breach or terminate this Agreement and receive a full refund of all amounts paid to Contractor under this Agreement.

11.7. Disabling Code Warranty. Contractor represents, warrants and agrees that the Services do not contain and the City will not receive from Contractor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system or Data (a "Disabling Code"). In the event a Disabling Code is identified, Contractor shall take all steps necessary, at no additional cost to the City, to: (a) restore and/or reconstruct all City Data lost by the City as a result of Disabling Code; (b) furnish to City a corrected version of the Services without the presence of Disabling Codes; and, (c) as needed, re-implement the Services at no additional cost to the City. This warranty shall remain in full force and effect as long as this Agreement remains in effect.

11.8. Third-Party Warranties and Indemnities. Contractor will assign to the City all Third-Party warranties and indemnities that Contractor receives in connection with any products provided to the City. To the extent that Contractor is not permitted to assign any warranties or indemnities through to the City, Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent Contractor is permitted to do so under the terms of the applicable Third Party agreements.

11.9. Contractor warrants it has complied and shall comply with all applicable federal, state, and local laws and regulations of its domicile and wherever performance occurs during the term of this Agreement.

11.10. Delivery of Products shall not be construed to represent Acceptance nor shall Delivery of Products relieve Contractor from its responsibility under any representation or

warranty. If the City makes a payment for a Product prior to Acceptance, the payment does not grant a waiver of any representation or warranty by Contractor.

SECTION 12. CONFIDENTIALITY.

12.1. Contractor shall keep confidential, and cause all Subcontractors to keep confidential, all City Data, unless the City Data is publicly available. Contractor shall not, without prior written approval of the City, use, publish, copy, disclose to any third party, or permit the use by any third party of any City Data, except as otherwise stated in this Agreement, permitted by law, or approved in writing by the City. Contractor shall provide for the security of all Confidential Information in accordance with all applicable laws, rules, policies, publications, and guidelines.

12.2. The Receiving Party agrees to exercise the same degree of care and protection with respect to the Confidential Information that it exercises with respect to its own similar Confidential Information and not to directly or indirectly provide, disclose, copy, distribute, republish or otherwise allow any Third Party to have access to any Confidential Information without prior written permission from the disclosing party. However, (a) either party may disclose Confidential Information to its employees and authorized agents who have a need to know; (b) either party may disclose Confidential Information if so required to perform any obligations under this Agreement; and (c) either party may disclose Confidential Information if so required by law (including court order or subpoena). Nothing in this Agreement shall in any way limit the ability of City to comply with any laws or legal process concerning disclosures by public entities. Contractor acknowledges that any responses, materials, correspondence, documents or other information provided to the City are subject to applicable state and federal law, including the Colorado Open Records Act, and that the release of Confidential Information in compliance with those acts or any other law will not constitute a breach or threatened breach of this Agreement.

12.3. The Receiving Party will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement. The Receiving Party shall not disclose City Data or Confidential Information to Subcontractors unless such Subcontractors are bound by non-disclosure and confidentiality provisions at least as strict as those contained in this Agreement.

SECTION 13. COLORADO OPEN RECORDS ACT.

The Parties understand that all the material provided or produced under this Agreement, including items marked Proprietary or Confidential, may be subject to the Colorado Open Records Act., § 24-72-201, et seq., C.R.S. In the event of a request to the City for disclosure of such information, the City shall advise Contractor of such request in order to give Contractor the opportunity to object to the disclosure of any of its documents which it marked as proprietary or confidential material. In the event of the filing of a lawsuit to compel such disclosure, the City will tender all such material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. Contractor further agrees to defend, indemnify and save and hold harmless the City, its officers, agents and employees, from any claim, damages, expense, loss or costs arising out of Contractor's intervention to protect and assert its claim of privilege against

disclosure under this Article including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs and damages that the City may incur directly or may be ordered to pay by such court.

SECTION 14. SOFTWARE AS A SERVICE, SUPPORT AND SERVICES TO BE PERFORMED.

14.1. Contractor, under the general direction of, and in coordination with, the City's Chief Information Officer or other designated supervisory personnel (the "Manager") agrees to provide the Services listed on Attachments A and C and perform the technology related services described on attached Exhibit A (the "Statement of Work" or "SOW"). The Services, when fully accepted, shall conform to the functionality matrices set out as Attachments B and D hereto. The Parties acknowledge that Contractor and the City may work to further define the SOW, in which case that work product ("Follow-Up SOW") will become a part of this Agreement by incorporation. If the Follow-Up SOW materially alters the attached SOW the Parties agree to amend this Agreement in writing.

14.2. As the Manager directs, Contractor shall diligently undertake, perform, and complete all of the technology related services and produce all the deliverables set forth on Exhibit A to the City's satisfaction.

14.3. Contractor is ready, willing, and able to provide the technology related services and the Services required by this Agreement.

14.4. Contractor shall faithfully perform the technology related services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in the Agreement and in accordance with the terms of the Agreement.

14.5. User ID Credentials. Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:

(a) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation).

(b) Account credential lifecycle management from instantiation through revocation.

(c) Account credential and/or identity store minimization or re-use when feasible; and

(d) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).

14.6. Vendor Supported Releases. Contractor shall maintain the currency all third-party software used in the development and execution or use of the Service including, but not limited

to: all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source; with third-party vendor approved and supported releases.

14.7. Identity Management. The City's Identity and Access Management (IdM) system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, economically, and securely. All new and proposed applications must utilize the authentication and authorization functions and components of the IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions, regardless to where the application is hosted.

SECTION 15. GRANT OF LICENSE; RESTRICTIONS.

15.1. Contractor hereby grants to the City a right and license to display, perform, and use the Services and use all intellectual property rights necessary to use the Services as authorized.

15.2. Title to and ownership of the Service will remain with Contractor. The City will not reverse engineer or reverse compile any part of the Service. The City will not remove, obscure, or deface any proprietary notice or legend contained in the Service or Documentation without Contractor's prior written consent.

SECTION 16. DELIVERY AND ACCEPTANCE.

16.1. Right to Perform Acceptance Testing. Prior to accepting Deliverables, the City shall have the right to perform Acceptance Testing to evaluate the Deliverable(s) to ensure they meet Acceptance Criteria, if any, set forth on the applicable Order Form or Statement of Work. Contractor shall cooperate with the City in the development of Acceptance Criteria that shall be codified in the applicable Order Form or Statement of Work that will set forth the location, date, and other specifications of the Acceptance Testing, if any. Acceptance Testing may occur in one or more phases, depending on the integration of contingent products, scalability, performance tuning or other measurable features or milestones.

16.2. After an Acceptance Test and if at any time the Service does not conform, the City will notify Contractor in writing within sixty (60) days and will specify in reasonable detail the identified failures and possible reasons for failure. Contractor will, at its expense, repair or replace the nonconforming product within fifteen (15) days after receipt of the City's notice of deficiency.

16.3. If the City issues an Acceptance Certificate for an "Acceptance with Exception(s)" the City will list the exception(s) and the date for Contractor's correction of the Error(s). If Error(s) are corrected by the listed date(s) the City agrees to commence further Acceptance Testing of the Deliverable or affected portion(s). If the Deliverable passes the Acceptance Tests, the City will issue an Acceptance Certificate.

16.4. If a Deliverable fails a second or subsequent Acceptance Test (or in the event of a single Acceptance Test, the Acceptance Test) in no event shall there be an increase to the original price agreed to by the Parties for the Deliverable.

16.5. The foregoing procedure will be repeated until the City accepts or finally rejects the Deliverable, in whole or part, in its sole discretion. In the event that the Service does not perform to the City's satisfaction, the City reserves the right to repudiate acceptance. If the City finally rejects the Service, or repudiates acceptance of it, Contractor will refund to the City all fees paid, if any, by the City with respect to the Service.

16.6. If the City is not satisfied with Contractor's performance of the technology related services described in the Statement of Work, the City will so notify Contractor within thirty (30) days after Contractor's performance thereof. Contractor will, at its own expense, re-perform the service within fifteen (15) days after receipt of City's notice of deficiency. The foregoing procedure will be repeated until City accepts or finally rejects the technology related service in its sole discretion. If City finally rejects any technology related service, Contractor will refund to City all fees paid by City with respect to such technology related service.

16.7. Contractor warrants that during the term of this Agreement that the Service and any associated components will not materially diminish during the subscription Term.

SECTION 17. TERM.

The term of the Agreement is from May 1, 2022 through May 1, 2027 (the "Term").

SECTION 18. COMPENSATION AND PAYMENT.

18.1. Fee: The fee for the Services and technology related services is described in Attachment E "Pricing" (the "Fee"). The Fee shall be paid pursuant to the City's Prompt Payment Ordinance.

18.2. Reimbursement Expenses: The fees specified above include all expenses, and no other expenses shall be separately reimbursed or incurred hereunder for the provision of the Service(s).

18.3. Invoicing: Contractor must submit an invoice which shall include the City contract number, clear identification of the deliverable that has been completed, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance.

18.4. Maximum Agreement Liability:

(a) Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed **TWENTY-FIVE MILLION DOLLARS AND ZERO CENTS** ($25,000,000.00) (the "Maximum Agreement Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Contractor beyond that specifically described in the attached Exhibits. Any services performed beyond those in the attached Exhibits are performed at Contractor's risk and without authorization under the Agreement.

(b) The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and

encumbered for the purpose of the Agreement. The City does not by the Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. The Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

SECTION 19. STATUS OF CONTRACTOR.

Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever.

SECTION 20. TERMINATION.

20.1. The City has the right to terminate the Agreement for cause if Contractor materially breaches this Agreement and such breach, if capable of cure, has not been cured within thirty (30) days of Contractor's receipt of written notice of such purported breach from City. The City has the right to terminate a portion of the scope under the Agreement and may also terminate the entire Agreement without cause upon sixty (60) days prior written notice to Contractor. However, nothing gives Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Manager.

20.2. Notwithstanding the preceding paragraph, the City may terminate the Agreement if Contractor or any of its officers or employees are convicted, plead nolo contendere, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kick backs, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

20.3. Upon termination of the Agreement, with or without cause, Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for work duly requested and satisfactorily performed as described in the Agreement and shall refund to the City any prepaid cost or expenses. In the event of termination of this Agreement by the City for any reason, the Contractor will use best efforts to actively and in good faith cooperate and coordinate with, and assist, the City and with any successor contractor or provider retained by the City in transitioning the operation and function of the PMIS to an internal City operation or to a successor contractor or provider, in the City's sole discretion, including but not limiting to assisting in transitioning the functioning of PMIS Hardware and Software to accommodate new or different hardware or software proposed to be utilized to operate and maintain an ongoing PMIS, to the end that the operation of the PMIS and the City's operation of its Parking Citation program shall not be materially disrupted or interrupted or rendered dysfunctional by such transition.

SECTION 21. EXAMINATION OF RECORDS AND AUDITS.

Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to Contractor's

performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under the Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require Contractor to make disclosures in violation of state or federal privacy laws. Contractor shall at all times comply with D.R.M.C. 20-276.

SECTION 22. WHEN RIGHTS AND REMEDIES NOT WAIVED; WAIVER OF CONSEQUENTIAL DAMAGES.

In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of the Agreement shall be deemed or taken to be a waiver of any other breach.

EXCEPT FOR INDEMNIFICATION OBLIGATIONS FOR THIRD PARTY CLAIMS, IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, COST OF COVER, PUNITIVE, OR EXEMPLARY DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, ARISING OUT OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF BUSINESS, LOSS OF REVENUE, OR LOSS OF ANTICIPATED PROFITS, EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SECTION 23. INSURANCE.

23.1. General Conditions: Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. Contractor shall keep the required insurance coverage in force at all times during the term of the Agreement, or any extension thereof, during any warranty period, and for three (3) years after termination of the Agreement. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-" VIII or better. Each policy shall contain a valid provision or endorsement requiring notification to the City in the event any of the required policies is canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the

parties identified in the Notices section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. If any policy is in excess of a deductible or self-insured retention, the City must be notified by Contractor. Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of Contractor. Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

23.2. Proof of Insurance: Contractor shall provide a copy of this Agreement to its insurance agent or broker. Contractor may not commence services or work relating to the Agreement prior to placement of coverages required under this Agreement. Contractor certifies that the certificate of insurance attached as Exhibit B, preferably an ACORD certificate, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the Certificate. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.

23.3. Additional Insureds: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), Contractor and Subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees, and volunteers as additional insured.

23.4. Waiver of Subrogation: For all coverages required under this Agreement, with the exception of Professional Liability, Contractor's insurer shall waive subrogation rights against the City.

23.5. Professional Liability (Errors & Omissions): Contractor shall maintain minimum limits of $1,000,000 per claim and $1,000,000 policy aggregate limit. The policy shall be kept in force, or a Tail policy placed, for three (3) years for all contracts except construction contracts for which the policy or Tail shall be kept in place for eight (8) years.

23.6. Subcontractors and Subconsultants: All Subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) shall be subject to all of the requirements herein and shall procure and maintain the same coverages required of Contractor. Contractor shall include all such Subcontractors as additional insured under its policies (with the exception of Workers' Compensation) or shall ensure that all such Subcontractors and subconsultants maintain the required coverages. Contractor agrees to provide proof of insurance for all such Subcontractors and subconsultants upon request by the City.

23.7. Workers' Compensation/Employer's Liability Insurance: Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of $100,000 per occurrence for each bodily injury claim, $100,000 per occurrence for each bodily injury caused by disease claim, and $500,000 aggregate for all bodily

injuries caused by disease claims. Contractor expressly represents to the City, as a material representation upon which the City is relying in entering into this Agreement, that none of Contractor's officers or employees who may be eligible under any statute or law to reject Workers' Compensation Insurance shall effect such rejection during any part of the term of this Agreement, and that any such rejections previously effected, have been revoked as of the date Contractor executes this Agreement.

23.8. Commercial General Liability: Contractor shall maintain a Commercial General Liability insurance policy with limits of $1,000,000 for each occurrence, $1,000,000 for each personal and advertising injury claim, $2,000,000 products and completed operations aggregate, and $2,000,000 policy aggregate.

23.9. Technology Errors & Omissions including Cyber Liability: Contractor shall maintain Technology Errors and Omissions insurance including cyber liability, network security, privacy liability and product failure coverage with minimum limits of $1,000,000 per occurrence and $1,000,000 policy aggregate. The policy shall be kept in force, or a Tail policy placed, for three (3) years.

SECTION 24. REPRESENTATION AND WARRANTY.

Contractor represents and warrants that:

24.1. The Service will conform to applicable specifications, operate in substantial compliance with applicable Documentation, and will be free from deficiencies and defects in materials, workmanship, design and/or performance.

24.2. all technology related services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards.

24.3. all technology related services will conform to applicable specifications and the Exhibits attached hereto.

24.4. it has the requisite ownership, rights, and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to the software and services free and clear from any and all liens, adverse claims, encumbrances, and interests of any third party.

24.5. there are no pending or threatened lawsuits, claims, disputes, or actions: (i) alleging that any software or service infringes, violates, or misappropriates any third party rights; or (ii) adversely affecting any software, service, or supplier's ability to perform its obligations hereunder.

24.6. the Service will not violate, infringe, or misappropriate any patent, copyright, trademark, trade secret, or other intellectual property or proprietary right of any third party.

24.7. the software and Service will contain no malicious or disabling code that is intended to damage, destroy, or destructively alter software, hardware, systems, or data.

SECTION 25. DEFENSE AND INDEMNIFICATION.

25.1. Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees ("Indemnified Parties")for, from and against all third party liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of Contractor or its subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

25.2. Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether claimant has filed suit on the Claim. Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.

25.3. Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.

25.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection

25.5. Contractor shall indemnify, save, and hold harmless the Indemnified Parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the Indemnified Parties in relation to any claim that any Deliverable, Service, software, or work product provided by Contractor under this Agreement (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right.

25.6. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

SECTION 26. COLORADO GOVERNMENTAL IMMUNITY ACT.

The parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, § 24-10-101, et seq., C.R.S. (2003).

SECTION 27. TAXES, CHARGES AND PENALTIES.

The City shall not be liable for the payment of taxes, late charges, or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. § 20-107 to § 20-115.

SECTION 28. ASSIGNMENT; SUBCONTRACTING.

The Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the Manager's prior written consent provided, however, that Contractor may, without such written consent, assign this Agreement and its rights and delegate its obligations hereunder in connection with the transfer or sale of all or substantially all of its assets or business related to this Agreement, or in the event of its merger, consolidation, change in control or similar transaction. Any permitted assignee shall assume all assigned obligations of its assignor under this Agreement. Any purported assignment in violation of this section shall be void and of no effect.

SECTION 29. NO THIRD-PARTY BENEFICIARY.

Enforcement of the terms of the Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in the Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or Contractor receiving services or benefits pursuant to the Agreement is an incidental beneficiary only.

SECTION 30. NO AUTHORITY TO BIND CITY TO CONTRACTS.

Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City's Charter and the Denver Revised Municipal Code.

SECTION 31. AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS.

Except for the functional requirements provided in response to a request for proposal and/or any subsequent enhancement of the SOW or other implementation documentation that may be developed after execution of this Agreement, the Agreement is the complete integration of all understandings between the Parties as to the subject matter of the Agreement. No prior, contemporaneous, or subsequent addition, deletion, or other modification has any force or effect, unless embodied in the Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of the Agreement or any written amendment to the Agreement will have any force or effect or bind the City.

SECTION 32. SEVERABILITY.

Except for the provisions of the Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of the Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.

SECTION 33. CONFLICT OF INTEREST.

33.1. No employee of the City shall have any personal or beneficial interest in the services or property described in the Agreement. Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, et seq. or the Charter §§ 1.2.8, 1.2.9, and 1.2.12.

33.2. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the Agreement. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions, or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate the Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.

SECTION 34. NOTICES.

All notices required by the terms of the Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, or mailed via United States mail, postage prepaid, if to Contractor at the address first above written, and if to the City at:

Chief Information Officer or Designee
201 West Colfax Avenue, Dept. 301
Denver, Colorado 80202

With a copy of any such notice to: Denver City Attorney's Office
1437 Bannock St., Room 353
Denver, Colorado 80202

Notices hand delivered or sent by overnight courier are effective upon delivery. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. The parties may designate substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.

SECTION 35. DISPUTES.

All disputes between the City and Contractor arising out of or regarding the Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the Manager as defined in this Agreement.

SECTION 36. GOVERNING LAW; VENUE.

The Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into the Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or

supplements to same. Venue for any legal action relating to the Agreement will be in the District Court of the State of Colorado, Second Judicial District. Contractor shall perform or cause to be performed all services in full compliance with all applicable laws, rules, regulations and codes of the United States, the State of Colorado, and with the Charter, ordinances, rules, regulations and Executive Orders of the City and County of Denver.

SECTION 37. NO DISCRIMINATION IN EMPLOYMENT.

In connection with the performance of work under the Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.

SECTION 38. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS.

Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City barring Contractor from City facilities or participating in City operations.

SECTION 39. LEGAL AUTHORITY.

Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into the Agreement. Each person signing and executing the Agreement on behalf of Contractor represents and warrants that he has been fully authorized by Contractor to execute the Agreement on behalf of Contractor and to bind Contractor validly and legally to all the terms, performances, and provisions of the Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate the Agreement if there is a dispute as to the legal authority of either Contractor or the person signing the Agreement to enter into the Agreement.

SECTION 40. NO CONSTRUCTION AGAINST DRAFTING PARTY.

The Parties and their respective counsel have had the opportunity to review the Agreement, and the Agreement will not be construed against any party merely because any provisions of the Agreement were prepared by a particular party.

SECTION 41. ORDER OF PRECEDENCE.

In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.

SECTION 42. SURVIVAL OF CERTAIN PROVISIONS.

The terms of the Agreement and any exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of the

Agreement survive the Agreement and will continue to be enforceable. Without limiting the generality of this provision, Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that period.

SECTION 43. INUREMENT.

The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.

SECTION 44. FORCE MAJEURE.

Neither party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, unreasonable delay of carriers, governmental order or regulation, complete or partial shutdown of plant, unreasonable unavailability of equipment or software from suppliers, default of a Subcontractor or vendor (if such default arises out of causes beyond their reasonable control), the actions or omissions of the other party or its officers, directors, employees, agents, Contractors or elected officials and/or other substantially similar occurrences beyond the party's reasonable control ("Excusable Delay") herein. In the event of any such Excusable Delay, time for performance shall be extended for a period of time as may be reasonably necessary to compensate for such delay.

SECTION 45. PARAGRAPH HEADINGS.

The captions and headings set forth herein are for convenience of reference only and shall not be construed so as to define or limit the terms and provisions hereof.

SECTION 46. CITY EXECUTION OF AGREEMENT.

This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.

SECTION 47. COUNTERPARTS OF THIS AGREEMENT.

This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

SECTION 48. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS.

Contractor consents to the use of electronic signatures by the City. The Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of the Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of the Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing

an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

SECTION 49. ADVERTISING AND PUBLIC DISCLOSURE.

The Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of the Contractor's advertising or public relations materials without first obtaining the written approval of the Manager. Any oral presentation or written materials related to services performed under the Agreement will be limited to services that have been accepted by the City. The Contractor shall notify the Manager in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.

SECTION 50. COMPLIANCE FOR IN-SCOPE SERVICES.

Contractor covenants and agrees to comply with all information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any industry standards or guidelines, as applicable based on the classification of the data relevant to Contractor's performance under the Agreement. Such obligations may arise from:

Health Information Portability and Accountability Act (HIPAA)
IRS Publication 1075
Payment Card Industry Data Security Standard (PCI-DSS)
FBI Criminal Justice Information Service Security Addendum

CMS Minimum Acceptable Risk Standards for Exchanges and further covenants and agrees to maintain compliance with the same when appropriate for the data and Services provided under the Agreement. Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers, agents, business partners, contractors, Subcontractors and any person or entity that may have access to City Data under this Agreement maintain compliance with and comply in full with the terms and conditions set out in this Section. Notwithstanding Force Majeure, the respective processing, handling, and security standards and guidelines referenced by this section may be revised or changed from time to time or City Data may be utilized within the Services that change the compliance requirements. If compliance requirements change, Contractor and the City shall collaborate in good faith and use all reasonable efforts to become or remain compliant as necessary under this section. If compliance is required or statutory and no reasonable efforts are available, the City at its discretion may terminate the agreement for cause.

SECTION 51. ON-LINE AGREEMENT DISCLAIMER.

Notwithstanding anything to the contrary herein, the City shall not be subject to any provision included in any terms, conditions, or agreements appearing on Contractor's or a Subcontractor's website or any provision incorporated into any click-through or online agreements related to the work unless that provision is specifically referenced in this Agreement.

SECTION 52. PROHIBITED TERMS.

Any term included in this Agreement that requires the City to indemnify or hold Contractor harmless; requires the City to agree to binding arbitration; limits Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or that conflicts with this provision in any way shall be void ab initio. Nothing in this Agreement shall be construed as a waiver of any provision of §24-106-109 C.R.S.

SECTION 53. ON-CALL SERVICES.

The City may authorize specific assignments for Contractor by placing a written work order signed by the Manager and Contractor (the "Order") describing in sufficient details the services and/or deliverables at the rates provided or as a flat rate. Contractor agrees that during the term of this Agreement it shall fully coordinate its provision of the services with any person or firm under contract with the City doing work or providing services which affect Contractor's services. Contractor shall faithfully perform the work in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals and entities that perform services of a similar nature to those described in this Agreement. Contractor represents and warrants that all services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards; all services will conform to applicable specifications and as attached to the Order, if any; and, it has the requisite ownership, rights and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to any software and services free and clear from any and all liens, adverse claims, encumbrances and interests of any third party.

SECTION 54. PCI DSS COMPLIANCE ONLY FOR CREDIT CARD INTERFACE.

54.1. If Contractor is directly involved in the processing, storage, or transmission of cardholder data on behalf of the City as part of this Agreement, this Section applies. Any Contractor who provides or has access to software, systems, hardware, or devices which process and/or interact with payment card information or payment cardholder data must be compliant with the current version of the Payment Card Industry Data Security Standard (PCI DSS).

54.2. Contractor covenants and agrees to comply with Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Rules (SDP), and with all other credit card association or National Automated Clearing House Association (NACHA) rules or rules of member organizations ("Association"), and further covenants and agrees to maintain compliance with the PCI DSS, SDP, and (where applicable) the Payment Application Data Security Standard (PA-DSS) (collectively, the "Security Guidelines"). Contractor represents and warrants that all of the hardware and software components utilized for the City or used under this Agreement is now, and will be PCI DSS compliant during the term of this Agreement. All service providers that Contractor uses under the Agreement must be recognized by Visa as PCI DSS compliant. Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers (as defined by the PCI Security Council), agents, business partners, contractors, Subcontractors and any person or entity that may have access to credit card information under this Agreement maintain compliance with the Security Guidelines and comply in full with the terms and conditions set out in this Section. Contractor further certifies that the equipment, as described

herein, will be deployed in a manner that meets or exceeds the PA DSS and/or PCI certification and will be deployed on a network that meets or exceeds PCI standards. Contractor shall demonstrate its compliance with PCI DSS by annually providing the City an executed Attestation of Compliance (AOC). Contractor must provide verification to the City, prior to start up and ongoing annually during the term of this Agreement, that all modules of Contractor's system(s) that interface with or utilize credit card information in any manner or form of collection are PCI DSS compliant. If the Contractor is a service provider involved in the processing, storage or transmission of cardholder data or sensitive authentication data (collectively "Data Handling") on behalf of the City that would result in Data Handling being included in the City's PCI scope through connected software or components, then the Contractor must provide a PCI Responsibility Matrix ("Matrix") to be attached to this Agreement as an exhibit. The Matrix must identify where responsibility resides for each PCI control requirement, whether it be with the Contractor, the City or shared by both. Any PCI control requirements that do not apply should be indicated along with any pertinent notes.

54.3. Contractor shall not retain or store CAV2/CVC2/CVV2/CID or such data prohibited by PCI DSS subsequent to authorization of a credit card transaction, shall prohibit disclosure of any and all cardholder information, and in the event of a compromise of credit card information of any kind, Contractor shall notify the City in writing consistent with the Data Incident response notification requirements of this Agreement, and shall provide, at Contractor's sole expense, all necessary and appropriate notification to parties and persons affected by such disclosure and compromise.

54.4. If any Association requires an audit of Contractor or any of Contractor's Service Providers, agents, business partners, contractors, or Subcontractors due to a data security compromise event related to this Agreement, Contractor agrees to cooperate with such audit. If as a result of an audit of the City it is determined that any loss of information is attributable to Contractor, Contractor shall pay the City's reasonable costs relating to such audit, including attorney's fees. No review, approval, or audit by the City shall relieve Contractor from liability under this section or under other provisions of this Agreement.

54.5. In addition to all other defense and indemnity obligations undertaken by Contractor under this Agreement, Contractor, to the extent that its performance of this Agreement includes the allowance or utilization by members of the public of credit cards to pay monetary obligations to the City or Contractor, or includes the utilization, processing, transmittal and/or storage of credit card data by Contractor, shall defend, release, indemnify and save and hold harmless the City against any and all fines, penalties, assessments, costs, damages or other financial obligations, however denominated, assessed against the City and/or Contractor by credit card company(s), financial institution(s) or by the National Automated Clearing House Association (NACHA) or successor or related entity, including but not limited to, any credit card company fines, regardless of whether considered to be consequential, special, incidental or punitive damages, costs of notifying parties and persons affected by credit card information disclosure, the cost of replacing active credit cards, and any losses associated with fraudulent transaction(s) occurring after a security breach or loss of information with respect to credit card information, and shall defend, release, indemnify, and save and hold harmless the City from any and all claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings of any kind or nature, of or by anyone whomsoever, in any way affected by such credit card data or utilizing a credit card in

the performance by Contractor of this Agreement. In furtherance of this, Contractor covenants to defend and indemnify the City and Contractor shall maintain compliance with PCI DSS and with all other requirements and obligations related to credit card data or utilization set out in this Agreement.

SECTION 55. NO EMPLOYMENT OF A WORKER WITHOUT AUTHORIZATION TO PERFORM WORK UNDER THE AGREEMENT.

55.1. This Agreement is subject to Division 5 of Article IV of Chapter 20 of the Denver Revised Municipal Code, and any amendments (the "Certification Ordinance").

55.2. The Contractor certifies that:

(a) At the time of its execution of this Agreement, it does not knowingly employ or contract with a worker without authorization who will perform work under this Agreement, nor will it knowingly employ or contract with a worker without authorization to perform work under this Agreement in the future.

(b) It will participate in the E-Verify Program, as defined in § 8-17.5-101(3.7), C.R.S., and confirm the employment eligibility of all employees who are newly hired for employment to perform work under this Agreement.

(c) It will not enter into a contract with a subconsultant or subcontractor that fails to certify to the Contractor that it shall not knowingly employ or contract with a worker without authorization to perform work under this Agreement.

(d) It is prohibited from using the E-Verify Program procedures to undertake pre-employment screening of job applicants while performing its obligations under this Agreement, and it is required to comply with any and all federal requirements related to use of the E-Verify Program including, by way of example, all program requirements related to employee notification and preservation of employee rights.

(e) If it obtains actual knowledge that a subconsultant or subcontractor performing work under this Agreement knowingly employs or contracts with a worker without authorization, it will notify such subconsultant or subcontractor and the City within three (3) days. The Contractor shall also terminate such subconsultant or subcontractor if within three (3) days after such notice the subconsultant or subcontractor does not stop employing or contracting with the worker without authorization, unless during the three-day period the subconsultant or subcontractor provides information to establish that the subconsultant or subcontractor has not knowingly employed or contracted with a worker without authorization.

(f) It will comply with a reasonable request made in the course of an investigation by the Colorado Department of Labor and Employment under authority of § 8-17.5-102(5), C.R.S., or the City Auditor, under authority of D.R.M.C. 20-90.3.

55.3. The Contractor is liable for any violations as provided in the Certification Ordinance. If the Contractor violates any provision of this section or the Certification Ordinance, the City may terminate this Agreement for a breach of the Agreement. If this Agreement is so

terminated, the Contractor shall be liable for actual and consequential damages to the City. Any termination of a contract due to a violation of this section or the Certification Ordinance may also, at the discretion of the City, constitute grounds for disqualifying the Contractor from submitting bids or proposals for future contracts with the City.

EXHIBIT A: STATEMENT OF WORK
EXHIBIT B: CERTIFICATE OF INSURANCE

ATTACHMENT A: BUSINESS AND TECHNICAL REQUIREMENTS
ATTACHMENT B: ENFORCEMENT REQUIREMENT TRACEABILITY MATRIX
ATTACHMENT C: BUSINESS AND TECHNICAL REQUIREMENTS PERMIT
ATTACHMENT D: PERMIT REQUIREMENT TRACEABILITY MATRIX
ATTACHMENT E: PRICING
ATTACHMENT F: SERVICE LEVEL AGREEMENTS
ATTACHMENT G: ARCHITECTURE STANDARDS

Contract Control Number: TECHS-202262615-00
Contractor Name: PASSPORT LABS INC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By: _____

_____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number: TECHS-202262615-00
Contractor Name: PASSPORT LABS INC

By: DocuSigned by: ECAC1E101841469...

Name: Doug Rogers
(please print)

Title: CRO
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

Technology Services Program Management Office (PMO)

Statement of Work (SOW) Exhibit A

Parking Management Information System| PRJ0010495

Pamela Kane

November 30, 2021

DENVER
TECHNOLOGY SERVICES

Revision History

Date	Modified By	Version	Revision Comments
11/30/21	Pam Kane	1.0	Initial Creation
2/8/22	Pam Kane	1.1	Revisions with Passport
3/1/22	Pam Kane, Sean Greer	1.2	Revisions with TS

1.0 Introduction

This Statement of Work ("SOW") dated May 1, 2022 sets forth the scope and definition of the software solution and professional services (collectively, the "Solution") to be provided by Passport, Inc., its affiliates and/or agents ("Passport") to City of Denver, CO. ("City")

High Level Description

The Department of Transportation and Infrastructure (DOTI) is implementing a comprehensive technology solution, the Parking Management Information System (PMIS), to support the agency's business processes including parking enforcement, citation processing, citation adjudication, citation administration, and permit administration. This new solution is a replacement for the current system that has been in place for over two decades.

The Parking Management Information System is a fully integrated system that consists of three main functional areas:

- Parking Enforcement and Management
- Professional Services
- Permitting

The Business and Technical requirements for the work performed by Passport for this SOW are attached as follows:

	Scheduled Completion
Parking Management & Enforcement Business and Technical Requirements	Attachment A
Parking Management & Enforcement Requirements Traceability Matrix	Attachment B
Permit Program Business and Technical Requirements	Attachment C
Permit Program Requirements Traceability Matrix	Attachment D

City Technology and Policy Standards

Passport shall provide a solution compatible with the City's technology standards as outlined in Attachment G.

Timeline

Work shall be performed according to the milestone timeline and timeframes below. Dates or timeframes may change based on mutual agreement between the City and Passport.

Initial Implementation

Parking Management, Enforcement and Professional Services		
M#	**Milestones**	**Scheduled Completion**
M01	Planning and Analysis	6 weeks
M02	Design & Framework	4 weeks
M03	Build and Configure	8 weeks
M04	Data Migration	6 weeks
M05	Testing	4 weeks
M06	Deployment (including pre-deployment prep)	1 week
M07	Training and Documentation	2 weeks
M08	System Acceptance	4 weeks
Permit Program		
M#	**Milestones**	**Scheduled Completion**
M01	Planning and Analysis	4 weeks
M02	Design & Framework	4 weeks
M03	Build and Configure	8 weeks
M04	Data migration	6 weeks
M05	Testing	4 weeks
M06	Pre-Deployment & Deployment	4weeks
M07	Training and Documentation	2 weeks
M08	System Acceptance	4 weeks

M09: Maintenance and Continuous Improvement				
	M#	**Description**	**Cadence**	**Due Date**
Year 1	M09.3	PMIS Technology Roadmap Reviews	Quarterly	2nd week of each quarter
	M09.4	KPIs and Performance Report Card	Monthly	5th day of each Month
Year 2	M09.1	Innovation Reviews	Bi-annual	2nd week of each 2nd and 4th quarter
	M09.2	Compliance Review	Annual	March 15
	M09.3	PMIS Technology Roadmap Reviews	Quarterly	2nd week of each quarter
	M09.4	KPI Objectives and Measurement Review	Annual	June 15
	M09.5	KPIs and Performance Report Cards	Monthly	5th day of each Month
Year 3	M09.1	Innovation Reviews	Bi-annual	2nd week of each 2nd and 4th quarter
	M09.2	Compliance Review	Annual	March 15
	M09.3	PMIS Technology Roadmap Reviews	Quarterly	2nd week of each quarter
	M09.4	KPI Objectives and Measurement Review	Annual	June 15
	M09.5	KPIs and Performance Report Cards	Monthly	5th day of each Month
Year 4	M09.1	Innovation Reviews	Bi-annual	2nd week of each 2nd and 4th quarter
	M09.2	Compliance Review	Annual	March 15
	M09.3	PMIS Technology Roadmap Reviews	Quarterly	2nd week of each quarter
	M09.4	KPI Objectives and Measurement Review	Annual	June 15
	M09.5	KPIs and Performance Report Cards	Monthly	5th day of each Month
Year 5	M09.1	Innovation Reviews	Bi-annual	2nd week of each 2nd and 4th quarter
	M09.2	Compliance Review	Annual	March 15
	M09.3	PMIS Technology Roadmap Reviews	Quarterly	2nd week of each quarter
	M09.4	KPI Objectives and Measurement Review	Annual	June 15
	M09.5	KPIs and Performance Report Cards	Monthly	5th day of each Month

Milestones and Technical Development Projects

Documented within this Statement of Work is the agreement for the initial implementation of Passport's proposed Parking Management Information System, as well as continuous work and commitments for the duration of the SOW. Milestones described within, specifically Milestones MO1 through MO8, apply to both the initial implementation and any subsequent technical development projects during the life of the SOW.

2.0 Project Management

Passport Project Management Responsibilities

1) Coordinating the development of project plans in consultation with the City Project Manager (CPM), City Contract Manager (CCM) and team members.
2) Managing escalations where needed, in conjunction with CPM and CCM where applicable.
3) Management of Passport and Partner resources and teams to ensure the timely delivery of items identified as "In scope" within this SOW.
4) Ensuring that members of the City staff are educated in the Passport application to understand the implications of initial design decisions.
5) Providing the City with timely and detailed descriptions of the items identified as "City task" within this SOW.
6) Providing the City of expected completion dates for all items identified as "City task" within this SOW and project plans.
7) Providing the City the impact on the expected delivery dates of all "City task" items when prerequisite City tasks.
8) Monitoring the progress of the SOW and monitor risks to on-time project completions with the SOW.
9) Coordinating the completion and approval of change orders.

City Project Management and City Contract Manager Responsibilities

1) The timely delivery of items identified as "City task" within this SOW and the project plans.
2) Providing Passport the expected delivery dates for items identified as "City task" within this SOW.
3) Ensuring that change orders contain a full specification of the changes required.
4) Ensuring that customizations are fully specified and documented.
5) Ensuring that all City team members have a clear understanding of their responsibilities within the SOW.

City Resources

The requirement for City resources is variable with:

1) The duration of the SOW.
2) The degree of internal City consultation.
3) The level of internal City agreement.
4) The number of customizations.
5) The familiarity of City staff with the environment.

Passport Resources

At a minimum, the following Passport resources will be assigned

Milestone	Resource
M01:Discovery, Planning, and Analysis	Solutions Engineer Sales Representative Technical Delivery Manager
M02: Design M03: Build and Configuration MO4: Data Migration	Project Manager Implementation Consultant Engineering Technical Delivery Manager
M05: Testing	Project Manager Implementation Consultant
M06: Pre-Deployment & Deployment	Project Manager Implementation Consultant
M07:Training and Documentation	Project Manager Implementation Consultant
M08:System Acceptance	Project Manager Client Success Executive Technical Delivery Manager
M09:Support, Maintenance, and Continuous Improvement	Project Manager Client Success Executive Technical Delivery Manager

3.0Milestones

M01: Discovery, Planning, and Analysis

Passport shall assign a Project Manager who shall be available to the City. Passport's Project Manager (PPM) is to provide direction and control of Passport's personnel and to establish a framework for communication, reporting, procedural and activities covered in this SOW. The PPM shall be responsible throughout the SOW for the following:

1) Review all SOW and associated documents with the CPM and CCM
2) Coordinate and manage the activities of Passport's SOW personnel
3) Maintain communications through the CPM and CCM
4) Develop documentation for this SOW
5) Provide weekly status reports

Planning Deliverables:

1) *Project Charter:* Passport, in coordination with the CPM and CCM, shall assist in creating Project Plans as needed to satisfy the City's documentation, reporting and oversight requirements. The items that follow are subsections within the Project Charter:
    a) Business Objectives – Shall list the high-level objectives.

b) Scope Overview – Shall list the high-level goals.
c) Integrated Business Solution – Shall detail how the high-level goals will be integrated to ensure a well-designed foundation for Passport and all integrated systems.
d) Integrated Governance and Structure – Shall detail the key resources, roles and responsibilities sufficient to support completion of project s within the SOW.
e) Critical Success Factors – Shall list the key factors that should be observed in order to deliver projects within the SOW on time and within budget.
f) Integrated Milestones – Shall list the high-level tasks necessary to fulfill the obligations of this SOW.
g) Risk Management Plan - Shall document and communicate known risks and evaluate potential risks in all phases of the SOW. The plan shall include mitigation strategies and establish the framework for identifying, managing and controlling risks. It shall also reflect how Passport defines risk, impact and probability.

2) Additionally, the following planning related artifacts shall be created by Passport:
a) The project plan will be prepared by the PPM in consultation with the CPM, CCM and team members.
b) The project planning phase will determine whether Passport Solution modules, features or integrations are to be implemented consecutively or concurrently and, if consecutively-, the order of implementation.
c) Integrated Project Plan (Work Breakdown Structure): Passport shall provide details on work that will be completed in each milestone, the amount of time expected to complete each task, and the staff or resources assigned to complete each task. At a minimum, this plan shall include an estimated but complete resource loaded schedule, including any constraints or assumptions. Passport shall employ professional project management software such as Microsoft Project.
d) Resource Directory: Passport and City shall list the resources and their contact information associated with the SOW.
e) Risk Register: Passport shall provide the format for recording risks. Risks will be discussed during weekly meetings (including PPM, CPM, CCM, etc.). A risk assessment meeting will be held monthly.
f) Quality Management Plan – Shall define the steps / processes to be used to ensure a sufficient level of quality is maintained throughout the life of the SOW.
g) Communication Plan – Passport shall assist in defining the steps / processes / tools available to communicate information to the CPM, CCM and City staff. Communication to City employees is the sole responsibility of the City.
h) Reports and Data Migration Methodologies - Passport shall describe the approach and define the details of the Software implementation as it pertains to required APIs, reports and data migration methodologies.

3) The City shall have the right to request new resources from Passport should the City deem they are not a good fit for the SOW, with the changes in resources being as immediate as possible.
4) Passport will work with the City to conduct discovery and analysis to determine what solution functionality best meets the City's requirements (as specified in the functional and technical requirements documents). This will be documented in the Solution Design Workbook (SDW) or other documents as agreed.
    a) Passport will assist with the gathering of the business requirements.
    b) Passport will be responsible for creating the final list of functional and technical requirements.
    c) Any gaps in functionality with the City's requirements and a solution to mitigate these gaps shall be mutually agreed upon before and documented before progressing to Milestone 02.
5) Develop detailed cutover plan including:
    a) Rollout plan including ordered, detailed tasks.
    b) Back-out plan including ordered, detailed tasks.
    c) Passport and City staff resource plan during cutover.
    d) Outage planning and communication.
    e) Adherence to all city technical change processes, procedures, and policies.
6) Change Management Plan - Passport shall help the City develop an appropriate change management strategy that at a minimum will:
    a) Identify and fully articulate the organizational changes that the initiative will bring.
    b) Develop specific transition and communication strategies for the various stakeholder groups.
    c) Develop strategies for mitigating and managing major barriers for implementation.
    d) Define how changes to the SOW and agreed requirements are to be evaluated, changed and coordinated within the SOW.
    e) Work with City counterpart(s) and communication support staff.
7) The implementation of each Passport solution module will involve the following stages:
    a) An overview of the module or functionality and the ways in which the module or functionality is operated.
    b) A determination of how best to configure and, if necessary, customize the module to meet the objectives of the City.
    c) An overview of the advantages and, if present, disadvantages of the proposed configuration and customizations, along with recommendations and assistance in developing or changing business processes if necessary.
    d) Documentation of the agreed configuration and customizations.
    e) The development by Passport of any required custom functionality or reports.
    f) The testing and acceptance by the City of configuration and custom functionality.
    g) The deployment of custom functionality or reports.

h) The development of a migration strategy for updating the Passport solution database with current and historical data from the incumbent system.
i) The development by the City of the integration components that are required to access data from the Passport system as outlined in the BRD.
j) The deployment of all integration components.
k) The testing and acceptance by the City of the integration components.

M02: Design

Passport shall be responsible for designing the Software to meet the agreed requirements.

Design Deliverables

Passport shall provide the City with the following:

1) Technical architecture design documentation.
2) Data migration design: Passport will perform an analysis of the data contained in the legacy systems to be migrated to the Software.
3) Integration requirements matrix. Source and Target integrations will be documented and will align to the City's integration standards
4) Reports Review requirement: Passport will verify that the standard reports available from Passport Solution meet City reporting requirements. If any requirements are not met Passport will work with City to define specific custom reporting needs.
5) Passport will be responsible for creating the configuration guide (detailing how to configure the system):
    a) Includes architecting workflows.
    b) Includes module configuration per the requirements document; and,
    c) Includes training around the same.
6) Passport will design historical data migration procedures.
7) Passport will assist in developing and documenting test plans and scripts for system and user acceptance testing.

M03: Build and Configuration

Passport shall be responsible for initial software configuration based upon the City's agreed requirements in preparation for initial user testing.

Configuration Deliverables

Passport shall:

1) Configure the Software to meet City agreed requirements as determined by the SDW or other Design documents. Create and configure users, groups, and roles.
2) Provide training on and assistance in creating and configuring user and role permissions.
3) Configure Software with Business Rules and workflows as determined during the Design phase and by using the SDW or other Design documents.
4) Create custom functionality or additional reports as needed and identified which fall into agreed deliverables or requirements, with change orders required for all others.
5) Provide required integrations based on the Business Requirements

6) Create and configure any City specific information as outlined in the requirements and SDW or other Design documents.
7) Preliminary testing of the Software configuration to ensure the Software functions accurately.
    a) Assist the City with the testing of the Software configuration.
8) Provide a configuration document detailing system interfaces.
9) Provide (and maintain) 4 environments (Development, Test, QA, and Production).

Environment Name	Definition	Refresh Cycle
Development	Configure, customize, and use source control to build an image of Passport PMIS to be promoted to another environment.	
Test	Environment to test new feature or upgrade procedure against controlled data and perform controlled testing of the resulting Passport PMIS.	Refresh as needed
Quality Assurance	Environment to test new feature or upgrade procedure against data, hardware, and software that closely simulate the Production environment and allow intended users to test the resulting Passport PMIS.	Parity with Production Refresh as needed
Production	Environment where the Passport PMIS is available for business use.	NA

10) Passport will be responsible for any custom development to meet requirements identified in the RFP and requirements referenced within this SOW:
    a) For any custom development, Passport will provide technical specifications.
11) Passport will work with the City to configure the system
12) Passport will work with the City to build data interface(s) to and from Passport.
13) Passport will be responsible for developing the interface(s) in/out of the Passport Solution system.
14) Passport will work with the City to connect and integrate with the ancillary technical systems (e.g., identity management, logging systems, support systems, etc.) as per technical requirements

MO4: Data Migration

1) Passport shall work with the City to map the City's historical information to the Software's data structure.
2) Passport shall work with the City to develop and document a strategy for mapping and migrating the City's historical data to the Software without damaging the integrity or stability of the Software or data.

3) Passport shall migrate the City's data into the Passport solution.
4) Passport shall work with the City to test the Software to ensure the migrated data displays as expected and the Software functions properly following the data migration.

M05: Testing

Passport shall include adequate provisions for system and user acceptance testing. This includes assistance in the development of a test plan that ensures the Software delivers the expected results the City identified in agreed requirements as described or clarified in the SDW or other Design documents. During the Testing phase Passport and the City will verify that the product meets the SDW and Design documents in M02 and M03.

1) For Testing that will be completed solely by Passport (Unit, System, Integration, Regression), testing certification will be provided to the City. User Acceptance Testing may not begin until Certification has been furnished. For Testing to be performed by both Passport and the City (UAT), Passport will prepare a detailed testing plan including executable test cases for all new features and functionality. Testing and defect resolution status will be provided to the City Project Manager and City Contract Manager according to the Project Plan and Passport must have a passing UAT score, as defined in testing deliverables 3.d, in order to deploy to production.
2) Defect Severity Scale: The following Defect Severity rating scale will be used to rate, track, score and address defects identified during testing.

S1 - Critical	The defect affects critical functionality or critical data. It does not have a workaround. Example: Unsuccessful installation, complete failure of a feature.
S2 - Major	The defect affects major functionality or major data. It has a workaround but is not obvious and is difficult. Example: A feature is not functional from one module, but the task is doable if 10 complicated indirect steps are followed.
S3 - Minor	The defect affects minor functionality or non-critical data. It has an easy workaround. Example: A minor feature that is not functional in one module, but the same task is easily doable from another module.

3) Testing Deliverables
   ~~a.~~ Test Certification - For Testing that will be completed solely by Passport (Unit, System, Integration, Regression), testing certification will be provided to the City that certifies each type of applicable testing has been completed, the test cases and methodology used to complete the testing, the outcome of the test, defects found including severity, root cause and resolutions for each defect. UAT will commence only when the Certification can attest that there are (1) Zero S1 defects (2) S2 defects on less than 15% of test cases (3) S3 defects on less than 20% of test cases.

b. Test Environment - Passport will prepare a Test Environment separate from the Development or Production environment in which to conduct UAT Testing. The test environment will be populated with a volume of relevant test data that will enable meaningful test case execution.
c. User Acceptance Test Plan - Passport will provide a User Acceptance Test Plan including testing strategy, testing environment, testing outline and test cases for new features and functionality as outlined in the SDW and Design documents from M02 and M03. Test cases shall also include demonstration that existing and related functionality remains operable. Passport will submit the User Acceptance Test Plan to the City Project Manager and City Contract Manager for Review and Acceptance according to the Project Plan.
d. Passport will maintain a User Acceptance Test Status Report during User Acceptance Testing. The UAT Test Status Report will indicate tests open, in progress and completed including the outcome of the test, defects found with severity, root cause, and resolution. The UAT Test Status report will be maintained and updated daily during UAT. Deployment to Production will be approved only when a passing score has been obtained; (1) Zero S1 defects (2) Zero S2 defects (3) S3 defects on less than 10% of test cases. Deployment to Production when the UAT score does not meet this criterion may only be completed upon Written approval of the City Project Manager and City Contract Manager.

M06: Pre-Deployment & Deployment

Passport shall address and fully test all City agreed requirements as documented, including SDW or other Design documents, prior to Software deployment. A Deployment Plan will be developed during the Configuration deliverable. This plan will be created and approved by the City. Therefore, this deliverable will be further defined once the Deployment Plan has been finalized.

Deployment Deliverables

1) Passport will provide architecture diagram, deployment document, and software configuration documentation around key and global settings specific to the City's configuration.
2) Participate in a go/no go decision with identified stakeholders from the City.
3) Implement cutover plan to deliver a configured budget management system.
4) Onsite or Dedicated virtual support for 30 business days after production deployment. Scheduling to be determined by City (based on Passport availability).
5) For 30 Days after Deployment Passport and the City will closely monitor, evaluate, and make modifications as warranted to address
    a. Technical issues
    b. Change Management issues
    c. Operational issues
6) Passport will maintain a Deployment report during that will list defects and issues reported with severity, root cause, and resolution. The Deployment Resolution Report will be maintained and updated daily.

7) System will be accepted upon completed of this 30 day period where the Deployment report contains (1) Zero S1 defects (2) Zero S2 defects (3) S3 defects on less than 5% of functionality (4) S4 defects on less than 10% of functionality.

M07: Training and Documentation

Passport shall provide virtual or on-site training. The training shall be designed and conducted to provide familiarization in all aspects of the Software by job function. The City will utilize train-the-trainer approach for end-user training. Training shall be scheduled by mutual agreement between Passport and the City.

Passport shall complete the following training:

1) Passport shall develop and provide user manuals to the City with specific training based on each module. Passport shall assist City trainers to develop training practice scenarios. Passport shall provide one (1) hard copy of each training manual and one (1) electronic copy of each training manual in the Microsoft Word format. The City may create as many copies of the training manuals as needed for its internal use.
2) All training shall be conducted against City-specific test environment.
3) All training shall be conducted on-site at the Wellington Webb Municipal Office Building in Denver, CO or remotely as agreed by City and Passport.
4) Training may be recorded by the City. The City may reuse these recordings without limitation.
5) The training approach shall be flexible, affording the City the flexibility to adjust participants or curriculum to achieve optimal training results.
6) Passport shall submit to the City for approval a class outline and training manual for all training, along with a time estimate to complete the sessions.
7) Passports learning program will address three knowledge areas
   a. Knowledge Readiness to perform User Acceptance Testing (UAT)
   b. Knowledge Readiness to Launch
   c. Knowledge Readiness to Support Business as Usual (BAU) operations such as new hires, functional roles changes, and/or promotions.

a. User Acceptance Testing (UAT)	b. Launch	d. Business as Usual (BAU)
Virtual Training led by passport for : ● Key City resources executing Test Cases for each functional area of City business	Virtual Training led by passport for : ● Specialty roles (audit, accounting, management, technical) ● Creating Passport Power Users	Passport Client Success Center for: ● Online procedure manual access

8) Passport shall provide training sessions that may include:

   a. Parking Management and Enforcement

Function	Program Description

Enforcement Officers (EO)	Provides officers with the knowledge and skills to issue citations and maintain their equipment.
Boot Enforcement Officers (BEO)	Provides boot enforcement officers with the knowledge and skills to issue warnings, immobilize vehicles, or initiate tow operations.
EO Leads & Supervisors	Provides supervisors with the knowledge and tools within Passport's system to improve daily operations.
Back Office	Provides all City staff (Management, Finance, Administrative Professionals, Customer Service, etc.) with the skill and knowledge to use the Passport system. Trainings include a range of topics including how to: ● Improve operations. ● Effectively and efficiently utilize Passport's system to support daily, weekly, monthly, and annual accounting routines. ● Accurately and efficiently support ticket questions from City constituents. ● Issue refunds, adjust payments, approve appeals, etc.

b. Permit Program

Function	Program Description
Permit Program Administrators	Provides employees with the knowledge and skills to ● Issue permits (including Meter Bags) and administer Permit Program ● Issue renewals ● Approve documentation ● Manage Waitlists
Other Back Office	Provides all City staff (Management, Finance, Administrative Professionals, Customer Service, etc.) with the skill and knowledge to use the Passport system. Trainings include a range of topics including how to: ● Improve operations. ● Effectively and efficiently utilize Passport's system to support daily, weekly, monthly, and annual accounting routines. ● Accurately and efficiently support permit questions from City constituents. ● Address verification data updates

9) Qualified technical experts shall conduct all training. The instructor(s) shall have a thorough mastery of the specific subject matter involved and shall have the ability to impart information to others in easily understood terms and with City-specific scenarios.
10) Passport shall provide Quick Reference Guides, including graphics. One (1) Quick Reference Guide per unique job function, up to a total of 15, shall be provided (e.g., entering a decision package).
11) Passport shall meet the following requirements for all training material:
    a) Shall be for the version of the software that is being deployed.
    b) Shall be customized to include functionality defined in the SOW.
12) Passport to provide training and documentation:
    a) Training for how to modify the configuration of the system in the future.
    b) Create User guide documentation.
    c) Assistance with creation of tutorials that will be used to train the agencies.

M08: System Acceptance

The final Acceptance will require a successful implementation of the system in all environments and successful User Acceptance Testing. Successful testing entails that the system performs as per the agreed requirements in the SDW and any other Design documents produced during the project. All Documentation shall be developed and provided to support the Software and the City's business processes. Any Software tools or utilities that are desirable to tune, test, maintain, or support the Software shall be specified by Passport. Any City-specific configuration or tailoring shall be documented and delivered to the City. Passport agrees to provide all documentation to include, but not limited to the following:

1) Technical administration
2) Software configuration
3) Interface(s)
4) Technical architecture diagram
5) Data dictionaries
6) Database setup and maintenance
7) Data model
8) Application Administration Guide
9) End-user day-to-day operation
10) Job function Quick Reference Guides
11) Disaster recovery plan and testing procedures

In addition, Passport will

- Finalize and deliver remaining documentation, recorded trainings, etc.
- Work with City to conduct Lessons Learned.
- Complete transition to Support and Maintenance and communicate support plan.
- Provide disaster recovery procedures, documentation of the testing of these processes, and a full data integrity test annually

M09: Support, Maintenance, and Continuous Improvement

Continuous Improvement

PMIS Products and Services will evolve and be supplemented, modified, enhanced, or replaced over time (1) to keep pace with technological advancements and improvements in the methods of delivering services (2) to respond to changes in Federal, State and Local laws or regulations, (3) improve the efficiency and effectiveness of the City Parking Management or Permit Programs and, (4) respond to industry trends and customer expectations. Passport and City acknowledge that these changes will improve the Products and Services and shall not result in new charges, unless the changed products or services meet the definition of a Change Order as stated in the Change Order Addendum.

The following deliverables are required to be created or maintained and updated as specified bellow.

Document	Delivery Schedule
1) Innovation Review	Bi-annually beginning Year 2
2) Compliance Review	Annually
3) PMIS Technology Roadmaps	Quarterly beginning Month 6
4) KPIs and PERFORMANCE REPORT CARD	Monthly

1) Innovation Review
A bi-annual Solution Refinement and Innovation Review will be conducted by Passport and be presented to the City. Passport will continue to refine the implemented solution and provide the City with the most innovative and current technologies available. On a bi-annual basis Passport will review the current solution and make recommendations to (1) improve efficiency of operational, administrative or management functions, (2) implement unused or enhanced features, (3) improve system performance and stability, (4) introduce new innovations for City constituents.

The review should contain a thorough analysis of each of the current software packages implemented and devices used, of all the functions that the City performs, of all Support issues such as help desk ticket analysis, outages and City requests, and the Vendors complete Parking Management, Enforcement, and Permitting software and hardware portfolio also taking into consideration innovations and implementations in other municipalities or locations.

The results of the analysis will be contained in the Innovation Review Document and presented to the City. The document must include:

- a description of each of the components analyzed
- recommendations or options for each component
- rationale and description of benefit/business case for each recommendation
- estimated timeline for implementation where applicable
- estimated cost where applicable
- new innovations or implementations in other municipalities in the past calendar year.

2) Compliance Review
Passport will ensure that the PMIS solution continues to meet all City Policies as well as Federal, State, and local laws and regulations. Passport will attest to adherence with the following City Policies annually. The City will make available all applicable City policies to Passport.

i) Data Retention Policy
ii) Department of Finance Cash City and County of Denver – Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds
iii) ADA policy and Compliance
iv) Branding and UX Standards
v) Security Policy
vi) TS Architecture Standards

vii) PCI/PII Compliance
viii) Internet of Things (IOT)

3) PMIS Technology Roadmap
PMIS Parking and Permit Program Roadmaps outlining current and future initiatives will be designed to meet the City's strategic goals and initiatives. The Roadmaps will be maintained and reviewed with the Vendor quarterly including:
   i) Goals: Both short-term and long-term achievements that the City Parking and Permit Programs and DOTI is hoping to achieve through the technology solution. Specifically, the goals will focus on the business capabilities that are enabled by the technology system, as well as what will be required to maintain the systems going forward.
   ii) New System Capabilities: High level description of what will be provided through the enhanced technology system.
   iii) Milestones: Key accomplishments achieved during the technology development process. Tracking milestones allow the stakeholders using the systems to understand the progress towards the long-term goals, at agreed upon points throughout the duration of the SOW.

4) KPIs and Passport Performance Report Card
Passport will develop an outcomes-based method to evaluate if the Passports and its subcontractor(s) are performing at or above agreed upon expectations. This program will be based on the City's stated goals. These will be reevaluated and updated as needed. During the initial Solution Delivery Phase, a meeting will be conducted with the City and Vendor to develop key performance metrics associated with the City's stated goals.
   i) Within 7 days of the initial meeting Passport will develop a draft of key performance indicators (KPIs) and distribute to the City for approval.
   ii) Within 30 days of final KPI approval, Passport will propose a data description and collection schedule to be provided to the City for approval. This will outline the specific data required, collection methods, reporting schedule and parties responsible for data collection and reporting.
   iii) No later than 30 days following the end of the first full quarter of operation, Passport will provide a draft report itemizing the results of each KPI.
   iv) Passport will present findings to the City.
   v) Passport will conduct strategy sessions and meetings to improve performance.
   vi) Passport will provide a monthly report.
   vii) Within 30 days of the end of the first full year of operations and annually thereafter, Passport will conduct a meeting between the City to review annual KPI objectives, revisions to existing KPIs, additional KPIs, any other changes necessary to promote continuous program improvement.
   viii) Within 14 days of this Annual review a new KPI agreement will be drafted for approval between the City and Passport.

4.0Compensation and Payment Terms

All compensation due to Passport shall be paid to Passport on a monthly basis by the City as specified in Attachment E - Pricing.

Payment Schedule

Upon System Acceptance as defined in Milestone M08. Passport will invoice the City by the 10th business day of each month for any Fees due for the prior month as itemized in Attachment E - Pricing.

All invoices will be paid in accordance with the City's Prompt Pay Ordinance.

Change Order

a. Change Orders

Any changes to the agreed specifications that meet the Change Order threshold as described by the Change Definition, including changes requested by the City within this project, shall be the subject of a new change order and the work to be carried out thereunder shall be mutually agreed upon, separately quoted, agreed, and billed as a part of this SOW.

b. Change Definition

The following definitions will be used to designate a request as a change order:

i. The request is a new feature that does not exist in the core product and requires significant custom development.
ii. The request is the addition of a new integration.
iii. The request will have a significant reduction or increase in scope.

c. Change Control Process

The change control process is required to: (i) assess and document the impact of scope changes on project schedules, resources, prices, payment schedule, deliverables, acceptance criteria, and other provisions of this SOW impacted by the proposed change, (ii) provide a formal vehicle for approval to proceed with any changes to this SOW and, (iii) provide a project audit record of all material changes to the original SOW.

i. Any changes, additions or deletions to the work effort hereunder including within the SOW and in in Attachments A, B, C, or D will be handled as follows:

1. In the case where the City or Vendor determine a change is required or desirable to the project, the requesting party will complete and sign a project change request form (a "Change Request" or "CR") and present the CR for countersignature by the other party;
2. Upon execution by both parties, a CR will become a "Change Order" and form part of this SOW; and
3. If the parties do not fully execute a Change Order, the prior obligations of each party under the SOW will remain unchanged.

ii. All changes to the SOW, pursuant to a Change Order, must be approved by the Project Sponsors and Project Managers from both Vendor and the City.

iii. In limited cases, a Change Order may need to operate as a separate and unique work assignment independent of the project schedules, resources, prices,

payment schedules, deliverables, milestones, acceptance criteria or other provisions of this SOW.

iv. When required, the City will ensure every Change Order will be accompanied by the appropriate pre-approved payment vehicle (e.g., purchase order, Agreement amendment or otherwise) to facilitate billing by Vendor.

d. Change Control Documentation Examples

i. Change Request Submission Example

Hello,

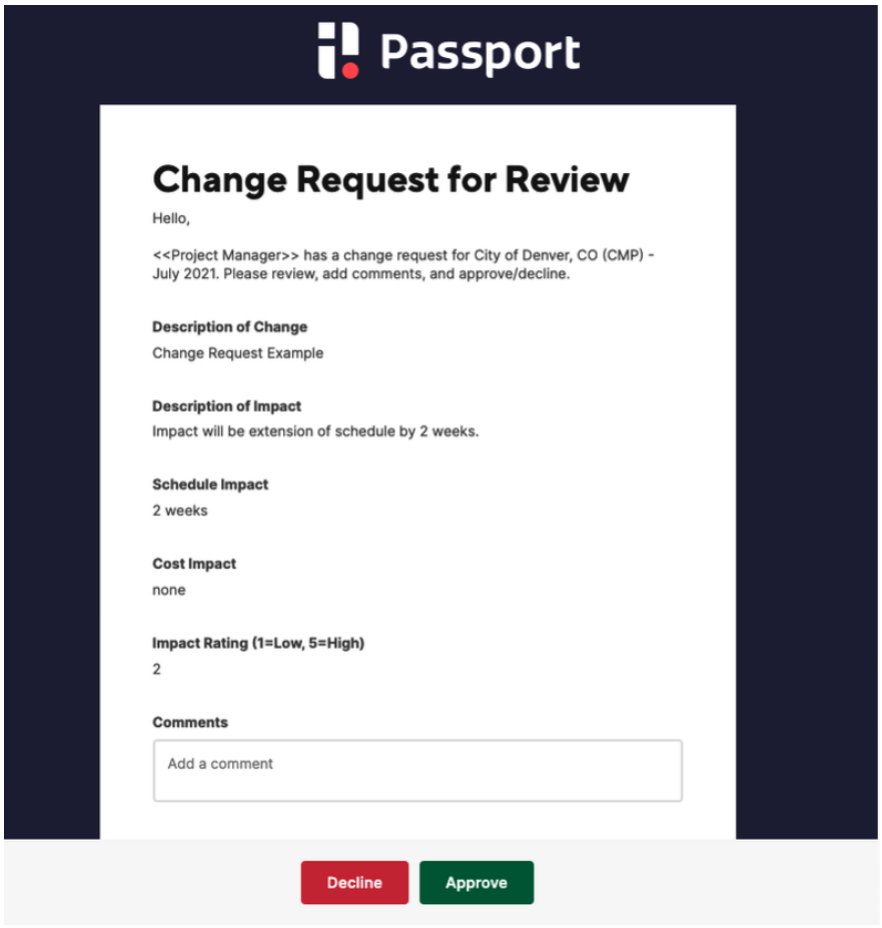
<<Project Manager>> has a change request for City of Denver, CO (CMP) - July 2021. Please review, add comments, and approve/decline.

View Request

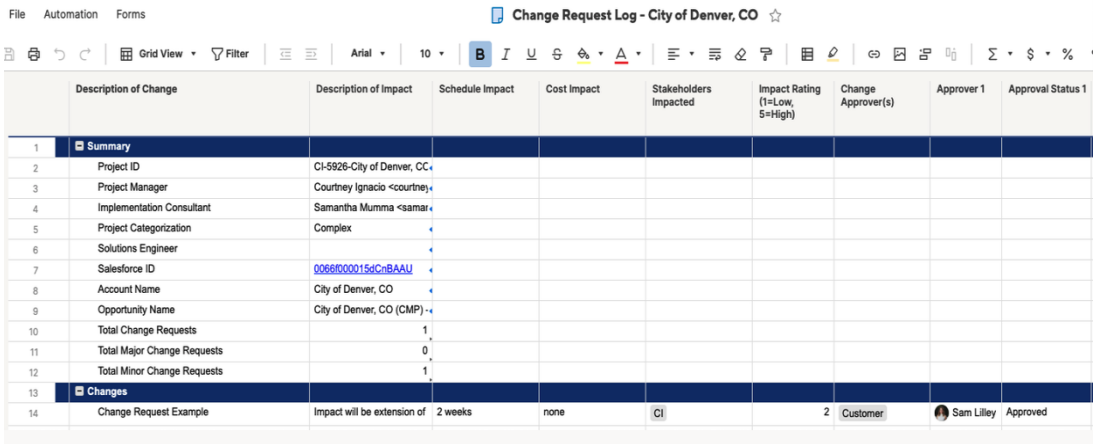
Row 14

Description of Change	Change Request Example
Description of Impact	Impact will be extension of schedule by 2 weeks.
Schedule Impact	2 weeks
Cost Impact	none
Impact Rating (1=Low, 5=High)	2

ii. Change Request Approval Example



iii. Change Request Log Example



5.0Glossary of Terms & Acronyms

Acronyms

Acronym	Definition
City	City and County of Denver
CPM	City Project Manager
CCM	City Contract Manager
SDW	Solution Design Workbook
PPM	Passport Project Manager
SOW	Scope of Work
BRD	Business Requirements Document
UAT	User Acceptance Testing
BAU	Business as Usual
PMIS	Parking Management Information System

Attachment A

City and County of Denver
201 W. Colfax Ave.
Department 304, 11th Floor
Denver, CO 80202

Parking Management Information System

Parking Management, Enforcement, and Professional Services

Business and Technical Requirements

Table of Contents

Goals and Objectives

I	Goals	Objectives
1	Future Proof	Able to incorporate future technology and mobility options Able to address unforeseen circumstances Able to address evolving and/or nontraditional business needs such as creating a new permit for outdoor dining or adding enforcement functions such as warnings Proactive in anticipating future needs in mobility, curbspace and the City's operational and policy changes State of the Art Technical Requirements: API Interoperability with any existing or future systems Fundamentally sound and reliable systems Industry standard cloud hosting
2	State of the Art Data Analytics Platform	Integrated with industry standard platforms and tools (Azure, AWS) Intuitive User Interface Dashboards/tables full flexibility Data validation/curation Responsive to data requests Proactive in anticipating future needs Machine Learning Predictive Analytics
3	Adaptable & Scalable	Technological capacity infrastructure growth built-in Ability to support large and complex data Ability to process Data at speed Nimble system e.g., ability to consolidate data with quality and stability
4	Ability to Control	Access to Settings – customizable user settings, administrator access level configurable, changes should be possible on a user setting level - no programming required Full access to data: Real time / Live Intuitive data transformation layer Timely and customer focused accessible data delivery
5	User Friendly – Internal & External	Internal Such as integrated with DMV Source of truth Robust customer service Intuitive workflows External One stop government compatible Streamlined service delivery for customers Modern functionality for customers Seamless customer experience for all things parking
6	Proactive, Future Oriented & Supportive Vendor Culture	Best in class culture Proactive in anticipating future needs Consulting Culture Increased efficiencies through continuous workflow / process improvement

Background

The City and County of Denver has a residential population of 727,211. The U.S. Department of Transportation's Smart City Challenge charged the City and County of Denver to think of transformative, multidisciplinary Smart City projects that could improve mobility. Denver was one of seven national finalists provided the opportunity to think beyond normal budget constraints, knowledge barriers and technological hurdles to identify a concrete path forward with a focus on innovative technologies, vehicle electrification and connected neighborhoods.

The City provides on-street paid parking with approximately 6,200 IPS single space meters with payment options ranging from cash to credit cards and Pay by App. Additionally, the City provides virtual and physical Parking and Occupancy Permits for Residential Parking, Official City Business, Emergency Trucks, Truck Loading, Food Trucks, and other specialty permits. City customers also can apply for Meter permits which block meter(s) for valid reasons such as construction or events.

Parking enforcement is managed by the Department of Transportation and Infrastructure (DOTI) Right of Way Enforcement Division. There are up to 80 Enforcement Agents and Boot Investigators that are responsible for enforcing parking codes by issuing notices, warnings and citations for parking violations and explain codes and regulations regarding parking violations to the public. The Agents also enforce ordinances, rules, and regulations relating to taxi hailing, vehicle towing and immobilization, expired/missing license plates, abandoned vehicles, street sweeping and valet operations. The City's Boot and Tow program, is executed by dispatchers and Boot crews who issue notifications, immobilize, tow or release vehicles. The Division is managed by a team of supervisors and managers that monitor enforcement personnel, duties and activities using the Parking Management Information System. The City is known for its innovative leadership in government transformation and strongly promotes data driven approaches. Using data to drive decisions is one of DOTI's focus areas. The PMIS data is a key component of the Department's and Division's Transportation, Mobility and Financial strategy.

Annual Transactions	
Transaction Type	Average per year (past 5 years)
Citations	400,000 – 650,000
Booted Vehicles	2,400 – 5,800

The City's omni channel approach to interact with its customers comprises of multiple interfaces that are provided to City customers that have been issued citations so that customers can resolve questions, pay citation(s), and adjudicate citation(s). To resolve questions customers can visit Denvergov.org or call a dedicated customer support line that is outsourced. To pay a citation, the City provides multiple options including an IVR system, mail-in payments, online payments and in-person payments. The City intends to reduce payment options in the future and to steer most payments to its online interface. Each of these payment interactions points to, is part of, or is integrated with the Parking Management Information System. In addition, the City provides customers the option to adjudicate citation(s) online.

Parking Management Information System (PMIS) Overview

The City's vision is a transformative and fully integrated Parking Management Information System (PMIS) consisting of 3 main functional components:

Parking-Related Systems	Technology/Service Provider	Included in this BRD
Parking Enforcement and Management	Passport	Yes
Professional Services	Passport	Yes
Permitting	Passport	No

The following systems constitute the main components of the current PMIS solution

Parking-Related Systems	Technology/Service Provider	To be retired or replaced	Retired by this BRD
Citation Issuance & Enforcement software	Conduent State & Local Solutions, Inc.	Yes	Yes
Citation Management System software	Conduent State & Local Solutions, Inc.	Yes	Yes
Business Intelligence software	Conduent State & Local Solutions, Inc.	Yes	Partial
Permit Management Solution software	Conduent State & Local Solutions, Inc.	No	No
Single Space Parking Meters	IPS Group, Inc.	No	No
Multi-Space Parking Pay Stations	IPS Group, Inc.	No	No
On-Street Mobile Payment	PayByPhone	No	No
Parking Access and Revenue Control Systems (PARCS)	SKIDATA Inc. & T2 pay stations	No	No
LPR	Genetec AutoVU*	No	No
Handheld Enforcement Devices	ZEBRA TC77, Zebra printer ZQ510, 3 IN BT4.0	No	No
Mobile Data Terminals (Ruggedized Laptops)	31 Vehicles, incl. 7 Boot Vans	No	No
*Genetec recurring annual software fee included in this SOW			

Out-of-Scope

Collections
First level collections, defined as any effort to collect on delinquent citation accounts during the first 365 days from date of citation issuance, is not in scope.
Second level collections, defined as any effort to collect on delinquent citation accounts on or after day 366 from date of citation issuance, is not in scope.

Functional Requirements

Note: Any requirements that are no longer required or have otherwise been removed from the scope of the initial implementation since RFP publication are indicated with a ~~strikethrough~~. Any requirements that will be met in a future release have been designated with the modifier Future/Roadmap. Any new requirements identified during Planning and Analysis shall follow the Change Order process as outlined in the Statement of Work.

1. Parking Management and Enforcement

Parking Enforcement Management and Customer Account Management will provide a comprehensive and consolidated overview of parking enforcement activities, parking program policies and configuration, and citation records. A consolidated interface will be implemented to manage and administer the City's PMIS program. While there may be multiple software components to execute the PMIS charges, there will be a single interface to manage the program and provide administrative processing for all products and services.

Citation Management/ Parking Enforcement Management

Back-office users may have specific functionality access assigned by a designated software administrator. Back-office users, based on the specific functionality access assigned, shall be able to perform the following citation management functions:

1) Citation Management
   Once a citation is issued or a customer interaction is created there should be a viewable audit trail of the event. Additionally, the citation record should be editable. The solution shall support these general citation management functions.
   a) Web-based software solution that provides citation-related data, accessible by City staff
   b) Integration of citation data in real-time
   c) Ability to View/Add/Edit citation data
   d) Ability to search for citations by customer name, business name, citation number, license plate, VIN.
   e) Ability to search for citations by address (Future/Roadmap)
   f) View files and documentation associated with a citation (photos, voice, correspondence, etc.)
   g) Ability to add specialized notes to the citation (both internal and external use)
   h) Ability to create fleet accounts for entities wanting to optimize citation payments for their fleet vehicles (e.g., rental car companies, deliver companies)
   ~~i) Integrated messaging and ability to send messages to other authorized users of the system~~
   j) Send physical letters to violators
   k) Send emails to violators for citation payment receipt and initial adjudication submission and adjudication decision.
   l) Send emails to violators for post-adjudication submission communication, such as request for further documentation and decision. (Future/Roadmap)

2) User Activity and Permissions
   a) Assign permissions to access certain features based on user ID
   b) Create an audit trail for user actions that result in a change to a record
   c) Review all user actions that result in a change to a record within the software

3) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
   i) Permit Management
   ii) Business Intelligence
   iii) Handheld Enforcement
   iv) Genetec LPR
   v) Scofflaw for ability to alert agents of boot eligible vehicles
   vi) Genetec LPR equipment
   vii) Pay-by-Phone and other Mobile Payment providers
   viii) Web/Mobile
   ix) Collection Agencies
   x) City Cashiering System
   xi) Others identified during Discovery with current vendor

4) General Citation
   Once a citation is issued there should be a viewable audit trail of the citation. Additionally, manual citations may be entered, and existing citation may require adjustments. The solution shall support these general citation functions.

   a) Query for citation data by any inputted field, including, but not limited to
      i) Date
      ii) Citation number
      iii) License plate number
      iv) Name (personal or business)
      v) Location

vi) VIN

b) View full history of citation including detailed audit trail
   i) Initial Issuance
   ii) Noticing and Correspondence
   iii) Customer Interactions (Outbound Calls, inbound calls, electronic or mailed communication)
   iv) Customer Activity (Online citation portal and back-office portal) including adjudication requests and associated documentation
   v) Notes
   vi) Boot Enforcement Activity
   vii) Violation Aging
   viii) Payment History and schedules
c) View current disposition in real-time
   i) Citation disposition
   ii) Boot disposition
   iii) Adjudication disposition
d) View a copy of a citation and images/photos taken during citation issuance (real-time or near real-time)
e) Attach voice recordings to citation records and listen to voice recordings.
   (a) Current voice recordings will be migrated such that the relationship to the Citation is preserved and the City can access and listen to the recordings.
f) Add or update the citation record
g) Add notes to citations, for both external and internal use only, and add notes to plate for internal use only.
h) Attach documents to citation records
i) Dismiss citations on one or multiple plates in one transaction.
j) Pay citations on one or multiple plates in one transaction
k) Disposition one or more citations in one transaction (e.g., one license plate may have multiple citations)
l) Place citations on hold to suspend penalty and notice activity
m) Void citations with custom City void codes
~~n) Cancel citations with custom City cancel codes~~
o) Support multiple vehicle owners on the same license plate
p) Support Colorado, out of state and non-US license plates
q) Edit tow information, including active and historical tows
r) Entry form for manually issued citations
s) Create a scofflaw list for boot eligible vehicles that is shared in real-time (or near real-time) with integrated enforcement such as Handheld, MDT and LPR
t) Validate vehicle owners and provide automated data validation of vehicle ownership leveraging both direct Validate vehicle owners and provide automated data validation of vehicle ownership
u) Acquire violator name and address information from both Colorado and out-of-state DMVs and obtain new names and addresses when notice mail is undeliverable leveraging both direct DMV and third-party integrations, such as but not limited to, NLETS.
v) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
   i) Permit Management
   ii) Business Intelligence
   iii) Handheld Enforcement
   iv) Genetec LPR
   v) Scofflaw for ability to alert agents of boot eligible vehicles
   vi) Genetec LPR equipment
   vii) Pay-by-Phone and other Mobile Payment providers
   viii) Web/Mobile
   ix) Collection Agencies
   x) City Cashiering System
   xi) Others identified during Discovery with current vendor

5) Parking Program Policies and Configuration

The City requires a solution that is configurable to meet City & County, State and Federal policies and laws. Where applicable and appropriate, City staff will have access to make configuration changes. Items that may be configured include but are not limited to:

a) Citation Record Configuration
   i) Data fields
   ii) Validation rules
b) Citation Lifecycle Configuration
   i) Violation aging
   ii) Suspension and Disposition rules including custom dispositions and void codes
   iii) Noticing Rules including multiple notification/ correspondence schedules
   iv) Citation Fee/Fine Schedule
c) Adjustment, Refund or Reduction rules
   i) Adjustment reasons/codes
   ii) Refund reasons/codes
   iii) Reduction reasons/codes
d) Payment Configuration including payment plans.
e) Workflow rules including automated actions, conditions, timing, and alerts
f) Geographic-based enforcement zones and beat designation
g) Communication templates both printed and electronic
h) User Access Configuration

6) Enforcement Management

The Right of Way Enforcement operation is managed by Managers and Supervisors in the field, in the office and remotely. Managers and Supervisors require tools to monitor real-time agent activity, evaluate performance over time, identify enforcement priorities, and review data to create and modify policy. Functions required to manage enforcement include:

a) Access to live citation issuance data, including ability to view access all fields of an issued citation, warning, or other actions
b) View GIS location of agent in real-time such as an accurate map view that displays active devices (HH) and breadcrumbs in near real-time with distinguishable icons for easy device/agent identification. The frequency of transmission of officer position information will be configurable, with a minimum transmission interval of thirty (30) seconds. The frequency of officer GPS capture will be configurable, with a minimum capture interval of one (1) minute.
c) View real-time citation issuance data visualized through density map and citation search
d) Reports for
   i) Performance evaluation
   ii) Hot List Identification and areas of investigation for increased compliance needs

7) Noticing and Correspondence

The City corresponds with customers and entities to resolve customer queries, provide customers with notification about violations, adjudication dispositions, or other account impacting activities. Electronic or hard copy correspondence may be generated and sent by City Staff or by Passport(s) or its professional services subcontractor(s). To effectively operate this portion of the parking program the following is required:

a) Create and configure templates for
   i) Mailed notifications and decision letters
   ii) Emails
   iii) Frequently used correspondence
b) Customize codes used in correspondence (liability reason codes, etc.)
c) Automatically send citations notifications and correspondence according to schedule
d) Manually create citation notification and correspondence
e) Issue reminder notices for unpaid citations
f) Issue delinquent notices to registered owners of vehicles with out-of-State license plates
~~g) Issue delinquent notices to registered owners of vehicles with non-US license plates~~

h) Issue notices to the lessee and/or secondary owner when delinquent following the lien process under state law
i) Issue notices to boot eligible vehicles prior to inclusion in the scofflaw list
j) Suspend noticing and penalty activities for bankruptcy notifications including identification of vehicle in PMIS based upon name, address, and or research of vehicle information through third party sources (e.g., Lexis Nexis)
k) Issue seizure notifications
l) Issue automatic notifications based on appeal and adjudication rules
m) Issue composite notices by license plate number, including noticing of partially paid parking citations
n) Process notifications issued to leased, rental and fleet vehicles, identifying responsible parties, and prepare specialized collection notice reports
o) Print one or more than one notification in one transaction
p) Create printer ready batch file of correspondence
q) Associate outgoing and incoming correspondence with violation record
r) Generate bar code, QR code and or numeric unique identifier for each piece of written communication to take the violator to the online payment portal
s) Mail notices according to City rules and schedules or ad hoc.
t) Maintain records of all notices issued including metadata and make these records viewable through Citation Management or Account Management software
u) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
    i) PMIS Citation Management and Account Management
    ii) Permitting
    iii) Mobile/Web
    iv) Business Intelligence
    v) Collection Agencies
    vi) Others identified during Discovery with current vendor

8) Handheld Citation Issuance

The City requires software for citation issuance to be deployed on its handheld devices. The City-owned hardware coupled with Passport provided software shall provide a comprehensive integrated System. Passport shall be required to support all software and hardware for the term of the agreement.

a) The following fields, at a minimum, must be available to generate, add and edit during citation issuance by enforcement software:
    i) Generate a Citation number (system generated)
    ii) Generate bar code (system generated)
    iii) License plate
    iv) State
    v) VIN or last six digits of VIN
    vi) One Violation code and description
    vii) More than one violation code and description
    viii) Location of violation, including program zone
    ix) Ability to recognize and auto populate location by GPS/Geofencing etc. (Future/Roadmap)
    x) Ability to scan Single Space Meter or Multi Space Pay station to populate unique meter identification number
    xi) Issue date
    xii) Issue time
    xiii) Officer ID and Agency ID
    xiv) Vehicle Make
    xv) Vehicle Color
    xvi) Officer Beat
    xvii) Officer signature for all issued citations with stylus or fingertip
    xviii) Notes to print on citation
    xix) Officer notes, not visible to the public
    xx) Fine and penalty schedules
    xxi) Appeal and payment instructions
    xxii) QR Code for Park Smart Denver

xxiii) Electronic marking
xxiv) Ability to take Photos (up to 10 per citation) and add to citation record
~~xxv) Ability to record Videos and add to citation record~~
~~xxvi) Ability to record Audio and add to citation record.~~
xxvii) Ability to issue a Warning with the same field definitions as for Citations
xxviii) Ability to utilize License Plate Recognition to automatically identify vehicle license plate, populate location, time mark, and pull data from vehicle based LPR use.
xxix) Ability to time mark (chalk) and upload time marks to the system for other agents to utilize on their HH devices.
xxx) Provision for operation and communication in low-bandwidth and no-bandwidth areas.
xxxi) Ability to issue Seizure Warnings
xxxii) Ability to enter Tow location information without citation or Warning issuance.
xxxiii) Ability to void citations in accordance with Business Rules. A valid void code must be entered for the voiding of any completed citation.
~~xxxiv) Ability to cancel a citation in accordance with Business Rules and ability to electronically request a cancellation of a citation by agent with a field for a cancellation code and notes.~~
xxxv) Support the reprinting of an issued citation, this reprinted citation must contain the same time as the original citation not simply the time it was reprinted.
xxxvi) Produce a voided ticket audit trail.
~~xxxvii) Produce a cancel ticket audit trail.~~
xxxviii) Ability to track and display agent location through HH device.
xxxix) Ability log agent activity.
xl) Provide Mobile device management (such as SOTI) software to manage business applications available on handheld devices
    1. Allow use of business-critical apps and software
    2. Prevent download of apps
    3. Prevent data download
    4. Provide remote device support/diagnostics
xli) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
    1. Scofflaw for ability to alert agents of boot eligible vehicles
    2. Genetec LPR equipment
    3. Pay-by-Phone and other Mobile Payment providers
    4. ~~Cartegraph~~
    5. PMIS Citation Management
    6. Samsara (Dispatch Tool/Telematics)
    7. Others identified during Discovery with current vendor

9) Boot Program

The City's operates a large fleet including a Vehicle Boot Team that consists of supervisors and investigators that execute and administer the field component the City's Boot Enforcement program. This includes issuing boot warnings, booting vehicles, releasing vehicles, readying vehicles to be impounded and managing boot inventory. The team currently has Mobile Data Terminals (ruggedized laptops) in vehicles with integrated software specific to managing their activity and operations. At a minimum the City desires the following software capabilities for the Vehicle Boot Team.

a) Provide a real-time interface/software between City-owned LPR equipment devices (ruggedized laptops equipped with Genetec LPR software) in all vehicles fitted with LPR systems and assigned to Boot Enforcement and PMIS to enable booting enforcement, update booted, towed, and released vehicle information using wireless communications. Tows processed on MDT will usually be to the City's Impound lot.
b) Ability to provide a 'local mode' to allow Vehicle Boot Investigators (VBI) to continue booting activities if Wireless communication is unavailable. All activity updates shall remain locally on the above identified device for update once the wireless communication becomes available.
c) The daily scofflaw file shall be available on the above identified devices using wireless technology.
d) The following minimum data shall be available on the above identified devices:

i) License Plate and State
ii) Total Amount due
iii) VIN (Last 6)
iv) Citation number
v) Vehicle Make
vi) Vehicle Color
vii) Location
viii) Boot Device number
ix) Reason Code
x) Reason Code Comment
xi) Notes
xii) Alerts
xiii) Escape Boot Fee

e) The following shall be editable by VBI
   i) Vehicle Color
   ii) Vehicle Make
   iii) Vehicle Location
f) Ability for the VBI to add notes to boot record. Notes should include:
   i) agent ID
   ii) time/date stamp
   iii) note details
g) Ability for high alert warnings to be presented to the VBI for safety awareness
h) Real-time boot release data from PMIS shall be available on the above identified devices using wireless technology
i) Ability to configure and display escape fees in accordance with Business Rules
j) Ability for the VBI to maintain and update a digital log of activities
k) Ability to attach LPR vehicle images to the Boot Record
l) Ability to 'accept' or 'reject' a boot identified by LPR. Rejecting a boot identified by LPR will require the VBI to specify a rejection reason/reason code
m) Ability to enter a reason/reason code when a Boot is identified as Gone on Arrival (GOA)
n) Ability to enter seizure warning notice issuance information
o) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
   i) Scofflaw for ability to alert agents of boot eligible vehicles
   ii) Genetec LPR equipment
   iii) PMIS Citation Management
   iv) Samsara (Dispatch Tool)
   v) Others identified during Discovery with current vendor

10) Dispatching

Dispatchers receive, route, and track the disposition of resident requests from 311 (Denver's Contact Center for help and assistance with City Services) and directly from residents and other stakeholders. They also dispatch the Boot team. The City requires an integrated system to facilitate and manage this process including but not limited to the functions described below:

a) Provide a real-time GIS interface to track vehicles and dispatch cases to agents via wireless communication to HH devices.
b) Ability to view the location of LPR vehicles and vans, walkers, and the scofflaw hit list on a real-time GIS display to dispatch the closest available vehicle
c) Receive case requests from 311 (currently Salesforce) including the following data points:
   i) Case Origin, Type, Priority, Status, Assigned Agency, Assigned Department
d) Provide case updates to 311 originated requests including the following data points
   i) Case Creation Date/Time, Case Closure Status, Case Closure Date/Time, Comments/Notes, Description, Status, Contact Information
e) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:

i) Scofflaw for ability to alert agents of boot eligible vehicles
ii) Genetec LPR equipment
iii) PMIS Citation Management
iv) Samsara (Dispatch Tool/Telematics)
v) Salesforce (311 Tickets)
vi) Business Intelligence
vii) Others identified during Discovery with current vendor

11) Adjudication

City magistrates process and adjudicate citation appeals with support from Professional Services. This City requires PMIS components to process and facilitate the adjudication of these citations. The following functions are required to support the City's adjudication procedures and policies:

a) Ability to automate and apply suspend rules while appeals are under investigation.
b) Sort appeals/citations by type of violation and/or defense
c) Record case decisions
d) Modify, edit, and cancel appeal/adjudication requests
e) Ability to schedule a hearing according to City rules
f) Enter notes on individual or multiple citations
g) Allow both Internal and External notes
h) Upload documents to support appeal/adjudication requests
i) Display disposition status (Paid, Convicted, Dismissed, Recipient Not Responsible per Valid Meter Claim, etc.)
j) Display reasons for adjudication (if dismissed)
k) Display notes or hearing minutes
l) Place individual citations, or multiple citations assigned to one license plate, on hold to suspend penalties and noticing for a specified timeframe
m) Automatically remove the hold once a specified date/event has passed
n) Adjust fines (reduce, add additional fines, fees, court costs, etc.)
o) Send correspondence via mail and email regarding hearings, Court appearances and dispositions
p) Provide notification to Court to proceed with default judgements
q) Track payment of citations
    i) prior to a hearing date
    ii) after customer fails to appear or fails to make payment
r) Enter a disposition that places vehicles on tow eligibility list when an end user fails to appear or fails to make payment.
s) Ability to receive notifications or alerts for events such as when a customer makes a payment or a customer submits an appeal.
t) Ability to define user-specific notifications or alerts for events that require a citation to be in a specific status before the notification or alert is delivered. (Future/Roadmap)
u) Ability to receive notifications or alerts for events such as when a customer submits additional appeal documentation. (Future/Roadmap)
v) Ability to configure notification and alert events.
w) Ability to queue appeals for processing with and without priority selection
x) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
    i) THEMIS, City's Court software
    ii) PMIS Citation Management and account Management
    iii) City Cashiering System
    iv) Business Intelligence
    v) Others identified during Discovery with current vendor

12) Payments

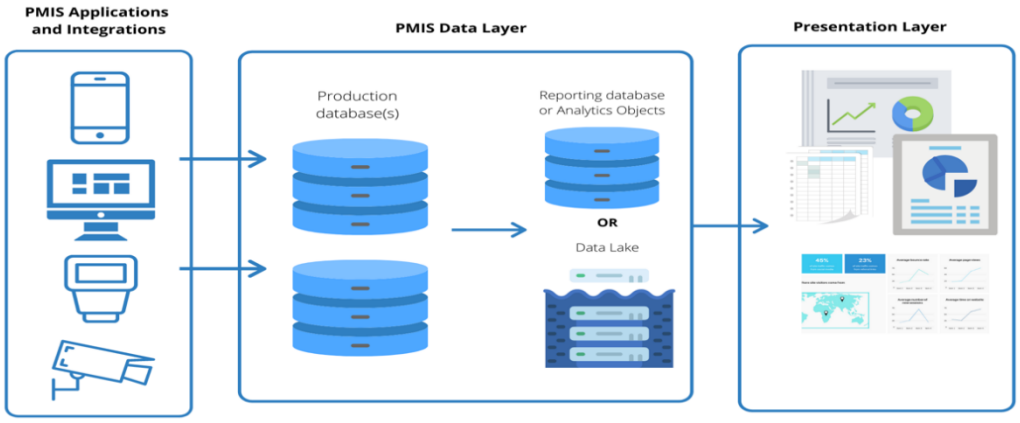
Ability to utilize the service, functions, and components of the City's Cashiering system to process payments.

a) PMIS shall support the ability to view payment plans, split payments, auto payments, partial payments, and deferred payments as required by the City's Cashiering system.
b) PMIS shall support the ability to apply and view non-standard transactions, including but not limited to refunds, transfers to another citation, adjustments, and other non-standard transactions.
c) PMIS shall reflect the payments made and current citation status in real-time when payments are made.
d) Integrations
   i) City Cashiering System
   ii) Workday for DOTI Finance
   iii) PMIS Citation Management an Account Management
   iv) Permitting
   v) Mobile/Web
   vi) Business Intelligence
   vii) Others identified during Discovery with current vendor

2. Reporting

The City needs to aggregate, analyze, and report on the data collected from all PMIS related solutions for a centralized view of the entire City Parking Program. A consolidated data view is required to provide executive insight into the City's Parking Programs' performance, as well as provide insight for both tactical and strategic decision support. The Business Intelligence solution will streamline the City's efforts to search for data and transform it into actionable intelligence. The Business Intelligence solution will provide easy to-use interfaces, easily accessed and combined data sources, and built-in visual best practices. In addition, the Business Intelligence solution will be scalable, allowing the City to scale its Business Intelligence needs over time.

Additionally, the City will be able to view and run operational, analytical, and financial reports for agents, administrators, magistrates, controllers, supervisors, and managers to perform their daily functions and reconciliation, keep apprised of operations, identify areas to improve operational efficiency and locate trends. Daily, weekly, and monthly operational and financial reports should be available to users.



1) Centralize all Parking Data in a Data Layer
   a) Adhere to standards for data completeness, accuracy, and timeliness (live data where applicable)
   b) Organize data within the centralized system into logical, flexible configurations in which individual elements and tables can be linked to each other across conformed dimensions for multiple business uses
   c) The City must have access to all tables, data sets, and schemas through modern data transmission methods including APIs that do not require Passport intervention
   d) All structured and unstructured data shall be available to the City and provided upon request in an industry standard format (e.g., doc., xls, .pdf, logs, and flat files)
   e) Entity relationship diagram(s) and data dictionaries to support development of end-user reports will be provided.

2) Provide a Presentation Layer that contains
   a) Dashboards
   b) Heat Maps and GIS Presentation
   c) Reporting assets/objects (static, standard, custom, variable)

3) Presentation Layer Functions
   a) The solution will provide capability to copy and modify existing reports and dashboards to create new reports/dashboards (Future/Roadmap)
   b) The solution will provide authorized users the ability to configure new reports and templates. (Future/Roadmap)
   c) The solution will allow a user to save a personal copy for later execution of a pre-defined report with a set of specific selection criteria
   d) The solution will provide functionality for the user to incorporate formulas, functions, and mathematical calculations into reports (Future/Roadmap)
   e) The solution will provide the ability to easily create and configure dashboards that show different analyses in visualizations that are comparable to modern data visualization programs (e.g., SAP Crystal Reports, Tableau, PowerBI, etc.) (Future/Roadmap)
   f) The solution will provide the ability to add data points and fields to a report, provide slicing and parsing abilities to isolate data points by different variables, identify trends, conduct data range analyses, etc. (Future/Roadmap)
   g) The solution will provide the ability to sort reports by predefined data fields
   h) The solution will provide pre-defined reports that support day-to-day PMIS business functions that are automatically generated and distributed (pushed to the user) by the PMIS at a user defined time for publication
   i) The solution will provide the ability to export presentation layer assets (CSV, Excel, PDF) (Future/Roadmap)

4) Integrations
   a) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
      i) Permit Management
      ii) Business Intelligence
      iii) Handheld Enforcement
      iv) Genetec LPR
      v) Scofflaw for ability to alert agents of boot eligible vehicles
      vi) Genetec LPR equipment
      vii) PayByPhone and other Mobile Payment providers
      viii) Web/Mobile
      ix) Collection Agency
      x) City Cashiering System
      xi) Others identified during Discovery with current vendor

3. Web/Mobile

Passport will provide online and mobile service applications to service City customers. The goals are to provide streamlined service delivery for residents/customers, improve public perception through better branding, boost community engagement, meet the unique needs of the Department of Transportation & Infrastructure. The Web/Mobile solution to serve the City's customer consists of three components described below. This Business Requirements Document includes the Citation and Adjudication components of the solution as well as redirects to and from the additional components listed.

Web Mobile Components	Technology/Service Provider	Included in this BRD
Citations and Adjudication	Passport	Yes
Permits	Passport	No
Park Smart Denver (Denver.Gov)	CCD	No

Passport will provide a portal that enables customers to pay for citations, the ability to receive reminder notices for citations (when available), and the ability to adjudicate citations. The interfaces must be PC, tablet, and mobile device-friendly, with support for Windows, Android, and iOS operating systems.

The City has developed the ParkSmartDenver website which serves as a landing point to service City customer parking needs; https://www.denvergov.org/Government/Departments/Parking-Division. The requested online and mobile service applications will be integrated with this landing point and other points of entry on Denver websites.

Passport's online and mobile service applications will be "private label," designed to meet the City of Denver's branding and marketing standards and shall be designed in a manner consistent with City's existing style guide. The online and mobile service applications will be hosted externally.

Passport will update content as required in a timely manner, such as changes to parking rules, fines and penalties. The City will forward website traffic to Passport-hosted online and mobile service applications portal using forward URL links on the City's website, and Passport online and mobile service applications will include links to send users back to the City of Denver website.

Passport's online and mobile service applications must be accessible on multiple browser platforms, including MS Edge, Google Chrome, Safari, and Firefox. The online and mobile service applications experience for the user shall provide device detection and content displayed according to device type, including desktop computers, laptops, mobile devices, and tablets.

Below is a list of functions that will be provided to our City Customers.

a) Ability to make parking citation inquiries by citation number and License Plate
b) Ability to hide Personal Identifiable Information (PII) such as customer name and address while performing an inquiry/search
c) Ability to send email to permit holder when a new citation is issued to permitted license plate number

2) Citations and Adjudication
   a) Ability to view a copy of a citation and related customer-facing approved documentation such as photos and notes
   b) Ability to add/view the appeal/adjudication of parking citations
   c) Ability to edit/update the appeal/adjudication of parking citations such as uploading additional documentation (Future/Roadmap)
   d) Ability to upload supporting documentation to the appeal/adjudication of parking citations.
   e) Ability to identify and locate towed vehicles

3) Payments
   a) Ability to pay by
      i) Credit card
      ii) Debit card
      iii) Electronic check (Future/Roadmap)

b) Ability to process payment for citations or any other configurable fee type such as escaped boot fee, short check fee etc.
c) Ability to identify, isolate and pay for boot eligible citations only

4) FAQs and Content
   a) Provide FAQs for citation payment and appeal/adjudication features.
   b) Provide inline/on-page content to guide the user experience.
   c) Passport is expected to create a guide on how to view, pay and appeal/adjudicate citations which must be available on the web/mobile
   d) Ability to accept redirects from Denver.gov and redirect customers back to Denver.gov upon completion of a user flow

5) Compliance
   a) All Passport managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines (collectively, "Guidelines") 3-20.

6) Integrate with existing City systems and Passport applications. Integrations needed will depend upon the final solution architecture and configuration and may include:
   i) Permit Management
   ii) Business Intelligence
   iii) City Cashiering System
   iv) Others identified during Discovery with current vendor

4. Professional Services

Additional professional services may be provided to complete the operation of the City's Parking Program. Included in these offerings is live telephonic support to resolve City customer citation queries, mail and email support to resolve ad hoc citation queries, IVR/ automated telephonic support, noticing, lockbox processing, and general administrative support.

The duties and tasks of the Customer Service Call Center would include both parking program support and shall support the following:

1) Non-automated communication via phone, internet/email, and mail
   a) Provide a customer service support center for the City's parking program, at a minimum, from Monday through Friday and 8:00 AM to 5:00 PM MDT/MST, and subject to modification. Staff must be well trained, professional, and courteous customer service personnel equipped to handle clerical, customer service, supervisory, and managerial tasks in compliance with the approved operations and quality assurance plan. Callers seeking a live Customer Service Representative (CSR) must be serviced with an average Speed of Answer (ASA) of 60 seconds and an average abandon rate of under 5% per week.
   b) Staff and/or reroute calls in the event the connection to the computer network is disrupted
   c) Call scripts shall be developed by Passport, with City approval, for response to inquiries by customers
   d) Follow established business processing rules
   e) Monitor and record calls for quality assurance for a term of 90 days, subject to the same terms for English or Spanish speaking customers. Monitor the call acceptance rate, call completion rate, and longest and shortest call wait time. An incomplete telephone call is defined as a call terminated after 30 seconds have elapsed from the time an individual's call is received in Passport's (or its subcontractor's) system.
   f) Log all interactions with end users, including interaction type (phone/email/mail), name, inquiry date/ time, issue type, notes, resolution, closed date/time in the subcontractors end user CRM system. An audio recording of all telephone calls with end users will be delivered to the PMIS system and attached to either a citation or permit record. City may request the specific logs of the call details using a defined process in an ad hoc manner.
   g) All events resulting in changes to a citation record or permit record will be logged in the PMIS system and viewable in the citation or permit trail.
   h) Complaints made by end users regarding Vendor service must be logged and reported to the City within twenty-four (24) hours of complaint.
   i) Receive and scan appeal/adjudication requests via US mail
   j) Appeal/adjudication preparation to include processing for initial hearing reviews

2) IVR
   a) Operate a customized Interactive Voice Response (IVR) System in English and Spanish to accept payments and provide information. The interactive system must provide real-time information on each citation, including issue date, delinquent date, amount owed, and open citations by license plate number.
   b) The IVR system must recognize user inputs by touch tones and speech; include language support options to accept payments and provide information.
   c) The IVR system shall offer the caller the option of a live CSR during operating hours and the CSR option must be provided early in the phone script.
   d) Provide the City with a toll-free telephone line that accepts global payments by Interactive Voice Response (IVR) 24 hours a day, 7 days a week. City's current provider will transfer the existing phone number to the new provider as part of the implementation.; must be Payment Card Industry (PCI) compliant.
      i) Payment types
         (1) Credit card
         (2) Debit card
         (3) Electronic check (Future/)
      ii) Credit card payments shall be processed through a City-owned Merchant Identification (MID) code approved and issued by the Cash Managements Section under the existing merchant services agreement managed therein. Passport must certify to process with the City's existing merchant services provider prior to implementation

e) The assessment of credit card convenience fees to customers is not part of the City's current receipting business model. Any proposal to assess fees beyond the cost of City services shall be submitted to the Cash Management Section for review and submission to the Manager of Finance for approval.
f) Ability to comply with Department of Finance (DoF) payment processing, deposits, reconciliation, and compliance rules.

3) Lockbox Payment Processing
The City is currently contracting out a Lockbox Payment Processing feature but is evaluating if such service should continue to be offered to City customers.

a) Accept mail-in citation payments (lockbox) preferably to a Denver mailing address. Existing mailing address will be transferred from existing Vendor to Passport during implementation.
~~b) Establish a Lockbox processing center location(s), including address(es) and a unique zip code, where applicable, and employees to support this function.~~
~~c) Provide support personnel (include resume).~~
d) Process mailed payments via lockbox processing, in-house remittance processing, third party remittance processing, or another process identified by Passport
e) Perform post office pickups daily (on days that the post office is in operation).
f) Provide Item scanning technology (Bar Code, Optical Character Recognition (OCR), Scan Line, etc.). Scan and handle non payment information based on routing rules defined between Vendor and City.
g) Establish and comply with payment processing timelines; citations are time sensitive and must be processed within City established timeframes (currently 1-3 days of time of receipt at processing center), and in order of first received.
h) Comply with quality controls performed for the City of Denver.
i) Establish a data transmission process (both for incoming and outgoing files).
j) Establish an exception handling process to be approved by the City prior to implementation.
k) Establish an error resolution process/plan to be approved by the City prior to implementation.
l) Establish and provide Check conversion (Accounts Receivable Conversion (ARC)), Image Replacement Document (IRD), ACH, etc.) and float schedule.
m) Provide document archival and disposal.
n) Provide a daily and monthly reports of operational effectiveness
o) Deposit funds daily by either electronic or physical delivery into a city owned bank account approved by the City's Cash Management Section.
~~p) Make physical bank deliveries; City preferred method is armored car.~~
q) Make ACH, wire, or other means of electronic depositing.
r) Process credit card transactions and any associated fees. Note: Credit card payments shall be processed through a City-owned Merchant Identification (MID) code approved and issued by the Cash Managements Section under the existing merchant services agreement managed therein. Passport must certify to process with the City's existing merchant services provider prior to implementation.
s) Comply with charge back quality controls/reconciliation performed for the City of Denver.
t) Comply with short check quality controls/reconciliation performed for the City of Denver.
u) Handle uncollected returned checks as follows: All returned checks received by Passport that are not successfully collected within one hundred twenty (120) days of their receipt shall be sent to the City and County of Denver, Treasury Division – Asset Recovery Service to be sent for collection to the contracted collection attorneys.
v) Handle overpayments as follows: Overpayments shall be reviewed monthly and refunds issued accordingly for any citation overpayment that is more than 365 days from payment date.
w) Handle batch processing: the processing of multiple payments identified by a unique batch number.
x) Procedures and systems must prove certified Payment Card Industry Data Security Standard (PCI DSS) compliant and/or identified as out of scope by the City’s PCI Committee prior to selection. All credit card processing solutions must comply with PCI DSS rules and regulations as specified by the City’s Cash, Risk and Capital Funding group.

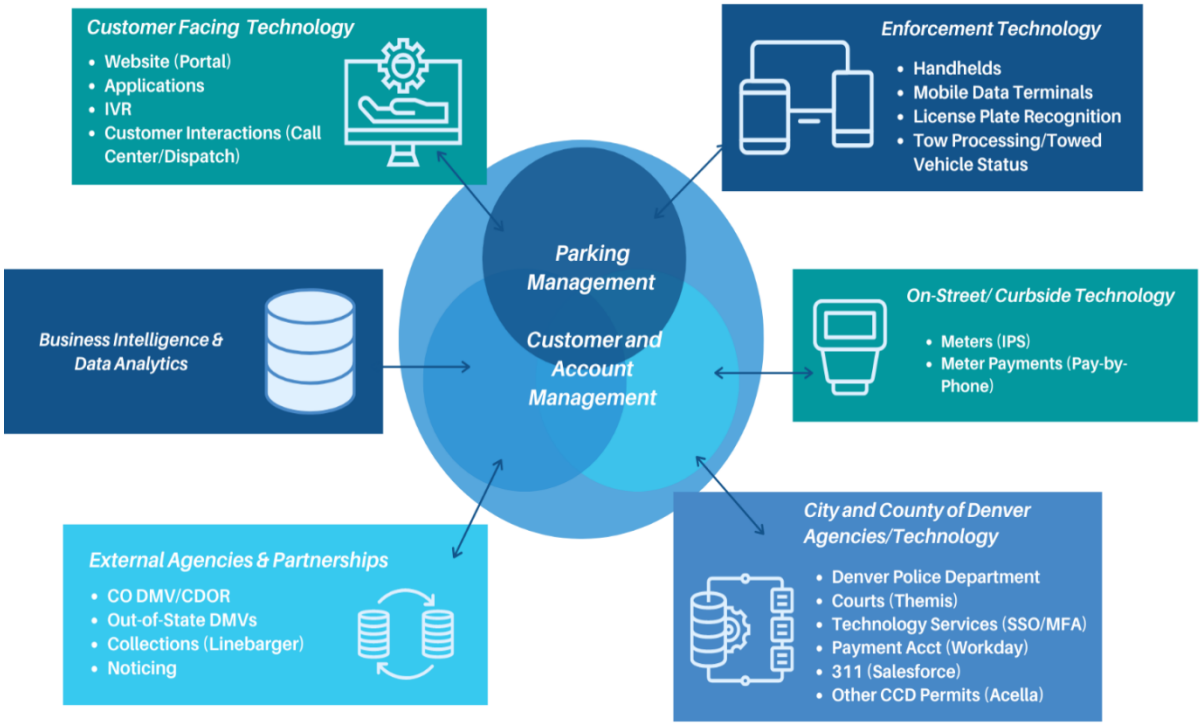
y) Systems and procedures must comply with the National Automated Clearing House Association and applicable rules and regulations surrounding Fed wires when processing ACH or wire payments, to be approved by the City's Cash Management Unit prior to implementation.
z) Passport must comply with all cash handling requirements specified by the City's Cash, Risk and Capital Funding group, as outlined in the attached Cash Handling Guidelines.
aa) Passport shall provide the City with any information requested as pertains to the audit of a specific revenue stream or function to verify completeness of records, identify balancing issues, and fully reconcile all payments.
bb) Open, Review, Sort, and Index incoming correspondence which may include digital records
cc) Transform written correspondence into electronic form and handle based on routing rules provided by the City.
dd) Associate or append correspondence with record or citation in PMIS
ee) Apply all payments received
ff) Generate the appropriate responses and respond in kind to citizen inquires within timeframes established by the City.
gg) Provided City capability to search and retrieve correspondence upon request
hh) Integrations
    i) Business Intelligence
    ii) PMIS Citation Management
    iii) PMIS Account Management
    iv) Others identified during Discovery with current vendor

5. Integrations

The solution will require integration within the solution itself, with internal City Systems, and with third party vendors. The integrations support City functions, city policies, data consistency, and ease of operations.

Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Application architecture and number of integrations will depend upon the final solution configuration. The high-level diagram below illustrates some of the existing integrations in our current architecture and integrations that may be required.



6. Non-Functional Requirements

The City requires a PMIS System that meets the City's Technical standards for operational maturity, information security maturity and technical compatibility. Passport will operate a mature IT organization following best practices. Expected areas of maturity and requirements therein are described below. Passport will be required to pass the City's Technical Security Questionnaire and present their strategy, architecture roadmap, transition strategy, architecture standards and principles to the City's Technical Architecture Review Board prior to proceeding with implementation.

1) Identity Management
   a) Ability to integrate with the City's multifactor authentication (MFA) and single sign-on (SSO) solution DUO Security (Mandatory).
   b) Ability to comply with the City's Identity Management protocols. Internal corporate or customer (tenant) user account credentials shall be restricted ensuring appropriate identity, entitlement, and access management and in accordance with the following established policies and procedures (Mandatory):
      i) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)
      ii) Account credential lifecycle management from instantiation through revocation
      iii) Account credential and/or identity store minimization or re-use when feasible
      iv) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)
   c) Role based security where access to data, screens, and critical functions can be limited based on roles or groups
   d) Audit logging where user activity is recorded for security and auditing

2) End-User Device Compatibility
   a) All web applications that will be accessed by the public must be compatible with current versions of Microsoft Edge and Google Chrome.
   b) Compatibility with current desktop, laptop, or tablet computing environments.
   c) Any software that is intended to run on mobile devices should support the current release of iPhone, iPad, Android, and Window devices.

3) Usability and Accessibility
   a) Images are properly described (using alt text) and provide readable color contrast
   b) Text and images are large and/or enlargeable
   c) Headers are used in a logical order of hierarchy
   d) Link and button text are descriptive with underline and properly contrasted color
   e) Videos are closed captioned
   f) Web pages do not contain anything that flashes more than three times in any one second period
   g) Content is written in plain language and illustrated with instructional diagrams (when applicable)
   h) Documents are fully accessible and converted to PDF format for best use
   i) Use City Brand standards for white label portions of the solution. White label designs will be subject to City approval

4) Application and Interface Security
   a) Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
   b) Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
   c) Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration, or destruction. These policies and procedures shall be in accordance with known legal, statutory, and regulatory compliance obligations.
   d) All credentials required for communication with external systems shall be encrypted.

e) Ability to utilize the City's centralized system for security information and event management.

5) Interoperability and Portability
   a) The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.
   b) The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data.

6) Deployment Model
   a) Use one of the following deployment models:
      i) Cloud hosting
      ii) Managed hosting
      iii) Hybrid cloud and managed hosting

7) Policy Compliance
   a) Passport will ensure that the PMIS solution meet all City Policies as well as Federal, State, and local laws and regulations and will attest to adherence with City Policies at the beginning of the contract and annually thereafter.
      i) Data Retention Policy
      ii) Department of Finance Cash City and County of Denver – Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds
      iii) ADA policy
      iv) Branding and UX Standards
      v) Security Policy
      vi) TS Architecture Standards
      vii) PCI/PII Compliance
      viii) Internet of Things (IOT)

8) Data Migration
   The City's current PMIS system provided by Conduent, maintains City of Denver records including but not limited to:
   - Citation records
   - Boot &Tow records
   - Appeal/Adjudication records
   - Collections records
   - Payment records
   - Data transformation records (business intelligence)

   Passport shall work with our existing PMIS vendor to migrate data to the new PMIS System in mutually agreed-upon formats. Passport will also work with City staff to migrate data fields from City and other third-party vendor systems that currently house parking related data. Passport will be responsible for defining a comprehensive data migration strategy for migrating Citation, Issuance and Enforcement data from existing systems to the new proposed solution. The migration strategy will identify data extraction and transformation methods, data validation and data clean-up measures and a testing plan to ensure migration quality, integrity, and completeness.

   a) Ability to provide a comprehensive migration strategy to migrate all data from existing permit, citation, and issuance/enforcement, boot &, customer contact, and collections systems to new solution. This includes but is not limited to eTIMs General Processing, eTIMs Workflow, City Sight Enforcement, Tableau, Merge, Scofflaw, and operational spreadsheets.
   b) Ability to extract data; capture all data in scope for migration.
   c) Ability to transform data as required for input into new solution.
   d) Ability to perform data validation/data clean up on migrated and transformed data.
   e) Ability to perform comprehensive testing to ensure migration quality, integrity, and completeness.

9) Operational Hours and Availability

The City requires the PMIS components to be fully operational and available according to times specified by the City excluding maintenance or planned outages. Operational availability will be tracked and measured and subject to Service Level Agreements.

a) Ability to comply with the City's Operational Hours. The PMIS components shall be operational 24 hours per day, Monday through Sunday.
b) Maintenance to the online environment shall not be performed by Passport between 6:00 AM and 11:00 PM, Monday through Sunday without the express permission of the City.
c) Schedule PMIS System maintenance between the hours of 12:00AM and 4:00AM with notification to City staff one (1) week in advance.
d) 99.9% Availability for hosted/cloud services. Availability that does not meet this standard will be subject to penalties that will be defined in the Statement of Work (SOW).
e) 99.9% Availability for software applications. Availability that does not meet this standard will be subject to penalties that will be defined in the Statement of Work (SOW).
f) 99.9% Availability for software application integrations and interfaces. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).

10) Capacity and Performance

The City requires the PMIS components to meet capacity requirements for City use and meet benchmark performance standards to ensure operational effectiveness.

a) Minimum of 150 total and concurrent users for Parking Account Management
b) Minimum of 200 total and concurrent users for Handheld Enforcement
c) Minimum of 20 total concurrent users for Boot
d) Support 5,000 visits per day for Web and Mobile
    i) Support a minimum of 5000 Citation payments per day
    ii) Support a minimum 1000 Adjudication requests per day
e) Meet benchmark application page load under 3 seconds
f) Meet benchmark TTFB (Time-to-First-Byte) under 1.5 seconds
g) Meet benchmark TTD (Time-to-Display) for standard reports and dashboards 3 seconds
h) Meet benchmark TTD (Time-to-Display) for interactive queries 3 seconds
i) Meet benchmark TTD (Time-to-Display) for deep analytics 60 minutes

Exhibit B

S1-PME-Citation Management

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Citation Management/ Parking Enforcement Management**	**This section describes the functional requirements for the Citation Management/ Parking Enforcement Management for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Citation Management	Web-based software solution that provides citation-related data, accessible by City staff	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *#4. Section 1 Parking Management and Enforcement* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Citation data integration	Integration of citation data in real-time	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	View Edit Citation Data	Ability to View/Add/Edit citation data	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Search Citation data	Ability to search for citations by customer name, business name, citation number, license plate, VIN.	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5.1	Search Citation data by address	Ability to search for citations by address	**Future Release**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	View documentation	View files and documentation associated with a citation (photos, voice, correspondence, etc.)	**Out-of-the-Box**	Manage Citations; Citation Details	Passport's system does not currently support the attachment of digital voice recordings or videos, but could link to external files using the "Add Notes" feature in the citation record. Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.7	Notes	Ability to add specialized notes to the citation (both internal and external use)	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.8	Business (Fleet) Account	Ability to create fleet accounts for entities wanting to optimize citation payments for their fleet vehicles (e.g., rental car companies, delivery companies)	**Out-of-the-Box**	Fleet Management	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
~~1.9~~	~~Messaging~~	~~Integrated messaging and ability to send messages to other authorized users of the system~~	**~~Cannot Meet~~**	~~User Management~~	~~Passport's back-end system, Client Portal, has the ability to identify users of the system and extrapolate their email addresses from their profile to message them outside of the PMIS platform.~~
1.10	Letters	Send physical letters to violators	**Out-of-the-Box**	Letter Template Setup; Customer Portal	Passport's platform can currently identify lingering citations associated to a user's account if they have a permit associated to the citation. Additionally, the team intends to iterate to add the ability to send notifications via multiple communication methods.
1.10.1	Email	Send emails to violators for citation payment receipt and adjudication submission communication such as request for further documentation and decision.	**Out-of-the-Box**	Letter Template Setup; Customer Portal	Passport's platform can currently identify lingering citations associated to a user's account if they have a permit associated to the citation. Additionally, the team intends to iterate to add the ability to send notifications via multiple communication methods.
1.10.2	Post-adjudication initial Adjudication communication	Send emails to violators for post-adjudication submission communication, such as request for further documentation and decision. (Future/Roadmap)	**Future Release**		
1.11	User Permissions	User Activity and Permissions - Assign permissions to access certain features based on user ID - Create an audit trail for user actions that result in a change to a record	**Out-of-the-Box**	User Management	Please see *User Activity and Permissions* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Activity Logs	Review all user actions that result in a change to a record within the software	**Out-of-the-Box**	Citation Detail Trail; Reporting	Please see *User Activity and Permissions* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: ii) Permit Management iii) Business Intelligence iv) Handheld Enforcement v) Genetec LPR vi) Scofflaw for ability to alert agents of boot eligible vehicles vii) Genetec LPR equipment viii) Pay-by-Phone and other Mobile Payment providers ix) Web/Mobile x) Collection Agencies xi) City Cashiering System	**With Configuration**	Client Portal	Passport intends to integrate with all of the listed City systems.

S1-PME-Policy and Configuration

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Policy and Configuration**	**This section describes the functional requirements for thePolicy and Configuration functions for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Citation Record Confirguration	a) Citaton Record Configuration i) Data fields ii) Validation rules	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Parking Program Policies and Configuration* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Citation Lifecycle	Citation Lifecycle Configuration i) Violation aging ii) Suspension and Disposition rules including custom dispositions and void codes iii) Noticing Rules including multiple notification/ correspondence schedules iv) Citation Fee/Fine Schedule	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Parking Program Policies and Configuration* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Adjustment and Refund	Adjustment, Refund or Reduction rules v) Adjustment reasons/codes vi) Refund reasons/codes vii) Reduction reasons/codes	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Parking Program Policies and Configuration* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Payment	Payment Configuration including and payment plans.	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Parking Program Policies and Configuration* as well as *Payments* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Adjustment and Refund	Workflow rules including automated actions, conditions, timing, and alerts	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Parking Program Policies and Configuration* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Enforcement	Geographical-based enforcement zones and beat designation	**Out-of-the-Box**	Settings; Enforcement Settings	Passport's platform can currently track the location and activity of parking officers in the field. The information can be displayed on a GIS interactive map which will display breadcrumb trails. The beats of the officer can also be inputted during the citation issuance process. Passport intends to iterate on the beat feature to enable the City to overlay beats, zones, and other geographical data for officers in the field.
1.7	Communication	Communication templates both printed and electronic	**Out-of-the-Box**	Settings; Enforcement Settings; Letter Template Setup	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.8	User Access	User Access Configuration	**Out-of-the-Box**	User Management	Please see *User Activity and Permissions* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.

S1-PME-General Citation

ID	Requirement Name	Requirement Description	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - General Citation**	**This section describes the functional requirements for the General Citation management functions for the PMIS.**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Query	Query for citation data by any inputted field, including, but not limited to i) Date ii) Citation number iii) License plate number iv) Name (personal or business) v) Location vi) VIN	Manage Citations	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	History	View full history of citation including detailed audit trail i) Initial Issuance ii) Noticing and Correspondence iii) Customer Interactions (Outbound Calls, inbound calls, electronic or mailed communication) iv) Customer Activity (Online citation portal and back-office portal) including adjudication requests and associated documentation v) Notes vi) Boot Enforcement Activity vii) Violation Aging viii) Payment History and schedules	Manage Citations; Citation Details	Calls are not tracked in automated fashion as they are received, however, users can add notes to a citation record via the "Add Note" feature. This can be used for documenting call conversations with a timestamp and the attributing user ID. Please also see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for additional details.
1.3	Dispositions	View current disposition in real-time i) Citation disposition ii). Boot disposition iii) Adjudication disposition	Boot and Tow	Please see *General Citation* as well as *Boot Program* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Images/Photos	View a copy of a citation and images/photos taken during citation issuance (real-time or near real-time)	Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Voice recordings	Attach voice recordings to citation records and listen to voice recordings. - Current voice recordings will be migrated such that the relationship to the Citation is preserved and the City can access and listen to the recordings.	Citation Details	Passport's issuance software includes a voice-to-text feature for a hands-free method of dictating notes to be added to the citation. Within Client Portal, Passport's system does not currently support the attachment of digital voice recordings but could link to an external audio file using the "Add Note" feature in the citation record. Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Update record	Add or update the citation record	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.7	Notes	Add notes to citations, for both external and internal use only, and add notes to plate for internal use only.	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.8	Documents	Attach documents to citation records	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.9	Dismiss	Dismiss citations on one or multiple plates in one transaction.	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.10	Pay	Pay citations on one or multiple plates in one transaction	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.11	Disposition	Disposition one or more citations in one transaction (e.g., one license plate may have multiple citations)	Manage Citations; Citation Details; Process Appeals	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Hold/Suspend	Place citations on hold to suspend penalty and notice activity	Manage Citations; Citation Details; Process Appeals	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	Void	Void citations with custom City void codes	Manage Citations; Citation Details; Process Appeals	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
~~1.14~~	~~Cancel~~	~~Cancel citations with custom City cancel codes~~	~~Manage Citations; Citation Details; Process Appeals~~	~~Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.~~
1.15	Multiple Owners	Support multiple vehicle owners on the same license plate	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.16	License Plates	Support Colorado, out of state and non-US license plates	Manage Citations; Citation Details	Please see *Account Management* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.17	Tow	Edit tow information, including active and historical tows	Boot and Tow	Please see *Boot Program* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.18	Manual Citation	Entry form for manually issued citations	Write Citation	Please see *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.19	Scofflaw	Create a scofflaw list for boot eligible vehicles that is shared in real-time (or near real-time) with integrated enforcement such as Handheld, MDT and LPR	Boot and Tow	Please see *Boot Program* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.20	Vehicle ownership	Validate vehicle owners and provide automated data validation of vehicle ownership	Registered Owner Data Retrievals	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.21	Violator address	Acquire violator name and address information from both Colorado and out-of-state DMVs and obtain new names and addresses when notice mail is undeliverable leveraging both direct DMV and third-party integrations, such as but not limited to, NLETS.	Registered Owner Data Retrievals	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.22	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Permit Management ii) Business Intelligence iii) Handheld Enforcement iv) Genetec LPR v) Scofflaw for ability to alert agents of boot eligible vehicles vi) Genetec LPR equipment vii) Pay-by-Phone and other Mobile Payment providers viii) Web/Mobile ix) Collections x) City Cashiering System iv) Others identified during Discovery with current vendor	Client Portal	Passport intends to integrate with all of the listed City systems.

S1-PME-Enforcement Management

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Enforcement Management**	**This section describes the functional requirements for Enforcement Management for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Live Citation Data	Access to live citation issuance data, including ability to view access all fields of an issued citation, warning, or other actions	**Out-of-the-Box**	Manage Citation; Reporting	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Agent location	View GIS location of agent in real-time such as an accurate map view that displays active devices (HH) and breadcrumbs in near real-time with distinguishable icons for easy device/agent identification. a) The frequency of transmission of officer position information will be configurable, with a minimum transmission interval of thirty (30) seconds. The frequency of officer GPS capture will be configurable, with a minimum capture interval of one (1) minute.	**Out-of-the-Box**	Reporting	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Citation Issuance Data Visualization	View real-time citation issuance data visualized through density map and citation search	**Out-of-the-Box**	Manage Citations; Reporting; Citation Density	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Performance and Hot List reports	Dashboard and Reports for i) Performance evaluation ii) Hot List Identification and areas of investigation for increased compliance needs	**Out-of-the-Box**	Reporting; Citation Density	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: (1) PMIS Citation Management an Account Management (2) Business Intelligence (3) Dispatch (Beat boundaries) iv) Others identified during Discovery with current vendor	**With Configuration**	Client Portal; OpsMan Mobile Enforcement Software	Passport intends to integrate with all of the listed City systems.

S1-PME-Noticing Correspondence

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Noticing**	**This section describes the functional requirements for the Noticing functions for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Configuration	Create and configure templates for i) Mailed notifications and decision letters ii) Emails iii) Frequently used correspondence	**Out-of-the-Box**	Letter Template Setup	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Codes	Customize codes used in correspondence (liability reason codes, etc.)	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Noticing and Correspondence* as well as *Parking Program Policies and Configuration* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Automatic notifications	Automatically send citations notifications and correspondence according to schedule	**Out-of-the-Box**	Settings; Enforcement Settings	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Manual notifications	Manually create citation notification and correspondence	**Out-of-the-Box**	Settings; Enforcement Settings; Citation Details	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Reminders	Issue reminder notices for unpaid citations	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Out-of-state	Issue delinquent notices to registered owners of vehicles with out-of-State license plates	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
~~1.7~~	~~Non-US~~	~~Issue delinquent notices to registered owners of vehicles with non-US license plates~~	**~~Cannot Meet~~**	~~Delinquent Noticing/Correspondence~~	~~Passport's solution allows citation issuance to non-US license plates, however, delinquent notices are only able to be mailed to US-based plates at this time. Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.~~
1.8	Lessee/Secondary owner	Issue notices to the lessee and/or secondary owner when delinquent following the lien process under state law	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.9	Boot Eligible	Issue notices to boot eligible vehicles prior to inclusion in the scofflaw list	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.10	Suspend noticing	Suspend noticing and penalty activities for bankruptcy notifications including identification of vehicle in PMIS based upon name, address, and or research of vehicle information through third party sources (e.g., Lexis Nexis)	**With Custom Programming**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.11	Seizure Notification	Issue seizure notifications	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Automatic notifications (Adjudication)	Issue automatic notifications based on appeal and adjudication rules	**Out-of-the-Box**	Process Appeals	Please see *Noticing and Correspondence* as well as *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	Composite notices	Issue composite notices by license plate number, including noticing of partially paid parking citations	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.14	Leased, Rental or Fleet	Process notifications issued to leased, rental and fleet vehicles, identifying responsible parties, and prepare specialized collection notice reports	**Out-of-the-Box**	Fleet Management Module; Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.15	Print	Print one or more than one notification in one transaction	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.16	Batch	Create printer ready batch file of correspondence	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.17	Associate with records	Associate outgoing and incoming correspondence with violation, account record	**Out-of-the-Box**	Citation Details	Please see *Noticing and Correspondence* as well as *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.18	Bar code/QR code	Generate bar code, QR code and or numeric unique identifier for each piece of written communication to take the violator to the online payment portal	**Out-of-the-Box**	Citation Details	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.18	Mail notices	Mail notices according to City rules and schedules or ad hoc.	**Out-of-the-Box**	Delinquent Noticing/Correspondence	Please see *Noticing and Correspondence* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.19	Records	Maintain records of all notices issued including metadata and make these records viewable through Citation Management or Account Management software	**Out-of-the-Box**	Citation Details	Please see *Noticing and Correspondence* as well as *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.20	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: (1) PMIS Citation Management an Account Management (2) Permitting (3) Mobile/Web (4) Business Intelligence (5) Collection iv) Others identified during Discovery with current vendor	**Out-of-the-Box**	Client Portal	Passport intends to integrate with all of the listed City systems.

S1-PME-Handheld Citation Issuance

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Handheld Citations**	**This section describes the functional requirements for the Handheld Citations functions that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Citation Number	Generate a Citation number (system generated)	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Bar Code	Generate bar code (system generated)	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	License	Add/Update/Display License plate	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	State	Add/Update/Display State	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	VIN	Add/Update/Display VIN or last six digits of VIN	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Violation Code	Add/Update/Display violation code and description (up to two)	**Out-of-the-Box**	Issue Ticket	Currently, Passport's ticket issuance process will only allow parking enforcement officers to issue one ticket/violation at a time. Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.7	Location	Add/Update/Display location of violation, including program zone	**Out-of-the-Box**	Issue Ticket	Passport will need to work with the City to fully understand and support program zones. Please also see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for details.
1.8	GPS/Geofencing	Ability to recognize and auto populate location by GPS/Geofencing etc.	**Future Release**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.9	Populate location	Ability to scan Single Space Meter or Multi Space Pay station to populate unique meter identification number	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.10	Issue Date	Add/Update/Display issue date	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.11	Issue time	Add/Update/Display issue time	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Officer ID and Agency ID	Add/Update/Display Officer ID and Agency ID	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	Vehicle Make	Add/Update/Display Vehicle Make	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.14	Vehicle Color	Add/Update/Display Vehicle Color	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.15	Officer Beat	Add/Update/Display Officer Beat	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.16	Signature	Officer signature for all issued citations with stylus or fingertip	**Out-of-the-Box**	Issue Ticket	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.17	Notes (Citation)	Add/Update/Display Notes to print on citation	**Out-of-the-Box**	Notes	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.18	Notes (Internal)	Officer notes, not visible to the public	**Out-of-the-Box**	Notes	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.19	Fines	Fine and penalty schedules	**Out-of-the-Box**	Issue Ticket; Settings; Enforcement Settings	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.20	Instructions	Appeal and payment instructions	**Out-of-the-Box**	Notes; Predefined Fields	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.21	QR Code	QR Code for Park Smart Denver	**Out-of-the-Box**		

1.22	Time Mark	Electronic marking	**Out-of-the-Box**	Notes; Predefined Fields	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.23	Photos	Ability to take Photos (up to 10 per citation) and add to citation record	**Out-of-the-Box**	Notes; Predefined Fields	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.24	Videos	~~Ability to record Videos and add to citation record~~	**Cannot Meet**		
1.25	~~Audio~~	~~Ability to record Audio and add to citation record~~	**~~Cannot Meet~~**		
1.26	Warning	Ability to issue a Warning with the same field definitions as for Citations	**Out-of-the-Box**	Warning Tickets	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.27	LPR	Ability to utilize License Plate Recognition to automatically identify vehicle license plate, populate location, time mark, and pull data from vehicle based LPR use.	**Out-of-the-Box**	Violations from LPR	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.28	Time Mark	Ability to time mark (chalk) and upload time marks to the system for other agents to utilize on their HH devices.	**Out-of-the-Box**	Digital Chalking	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.29	Low/No Bandwidth	Provision for operation and communication in low-bandwidth and no-bandwidth areas.	**Out-of-the-Box**	Offline Mode	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.30	Seizure Warning	Ability to issue Seizure Warnings through the HH device.	**Out-of-the-Box**	Issue Ticket	Passport can configure a violation type for "seizure warning" that can be issued from the handheld device. Passport will work with the City to define any additional data points or attributes that need to be included in the seizure warning.
1.31	Tow Location	Ability to enter Tow location information without citation or Warning issuance.	**Future Release**	Issue Ticket	Passport currently does not have the ability to enter tow information with the issuance of a boot "ticket" which does not need to have a dollar amount associated to it. In the future Passport will have an ingrained functionality to simply mark the vehicle as towed from the handheld device.
1.32	Void	Ability to void citations in accordance with Business Rules. A valid void code must be entered for the voiding of any completed citation.	**Out-of-the-Box**	OpsMan Mobile Enforcement Software	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.33	~~Cancel~~	~~Ability to cancel a citation in accordance with Business Rules and ability to electronically request a cancellation of a citation by agent with a field for a cancellation code and notes.~~	**~~Out-of-the-Box~~**	Issue Ticket; Void Queue	Please see *Handheld Citation Issuance* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.34	Reprint	Support the reprinting of an issued citation, this reprinted citation must contain the same time as the original citation not simply the time it was reprinted.	**Out-of-the-Box**	Previous Tickets	Please see *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.35	Void Audit Trail	Produce a voided ticket audit trail.	**Out-of-the-Box**	Reporting	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.36	~~Cancel Audit Trail~~	~~Produce a cancel ticket audit trail.~~	**~~Out-of-the-Box~~**	~~Reporting~~	~~Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.~~
1.37	Agent Location	Ability to track and display agent location through HH device.	**Out-of-the-Box**	Reporting	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.38	Agent activity	Ability to log agent activity.	**Out-of-the-Box**	Reporting	Please see *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.39	Mobile Device Management	Provide Mobile device management (such as SOTI) software to manage business applications available on handheld devices: (1) Allow use of business critical apps and software (2) Prevent download of apps (3) Prevent data download (4) Provide remote device support/diagnostics	**With Configuration**		
1.40	Integration	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Scofflaw for ability to alert agents of boot eligible vehicles ii) Genetec LPR equipment iii) Pay-by-Phone and other Mobile Payment providers iv) Cartegraph (strikethrough) v) PMIS Citation Management vi) Samsara (Dispatch Tool/Telematics) iv) Others identified during Discovery with current vendor	**With Configuration**	Client Portal; OpsMan Mobile Enforcement Software	Passport intends to integrate with all of the listed City systems.

S1-PME-Boot

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Boot**	**This section describes the functional requirements for the Boot functions that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Software for Boot Vehicles	Provide a real-time interface/software between City-owned LPR equipment devices (ruggedized laptops equipped with Genetec LPR software) in all vehicles fitted with LPR systems and assigned to booting and towing and PMIS to enable booting and towing enforcement, update booted, towed, and released vehicle information using wireless communications. Tows processed on MDT will usually be to the City's Impound lot.	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Local mode	Ability to provide a 'local mode' to allow Vehicle Boot Investigators (VBI) to continue booting activities if Wireless communication is unavailable. All activity updates shall remain locally on the above identified device for update once the wireless communication becomes available.	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Scofflaw	The daily scofflaw file shall be available on the above identified devices using wireless technology.	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Data Points	The following minimum data shall be available on the above identified devices: i) License Plate and State ii) Total Amount due iii) VIN (Last 6) iv) Citation number v) Vehicle Make vi) Vehicle Color vii) Location viii) Boot Device number ix) Reason Code x) Reason Code Comment xi) Notes xii) Alerts xiii) Escape Boot Fee	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Editable Data	The following shall be editable by VBI i) Vehicle Color ii) Vehicle Make iii) Vehicle Location	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Notes	Ability for the VBI to add notes to boot record. Note should include: i) agent ID ii) time/date stamp iii) note details	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.7	Alert Warning	Ability for high alert warnings to be presented to the VBI for safety awareness	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.8	Real-time	Real-time boot release data from PMIS shall be available on the above identified devices using wireless technology	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.9	Configuration	Ability to configure and display escape fees in accordance with Business Rules	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program*, *Dispatching*, and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.10	Activity log	Ability for the VBI to maintain and update a digital log of activities	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.11	Attach LPR images	Ability to attach LPR vehicle images to the Boot Record	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Accept/Reject Boot	Ability to 'accept' or 'reject' a boot identified by LPR. Rejecting a boot identified by LPR will require the VBI to specify a rejection reason/reason code	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	GOA reason codes	Ability to enter a reason/reason code when a Boot is identified as Gone on Arrival (GOA)	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.14	Seizure information	Ability to enter seizure warning notice issuance information	**Out-of-the-Box**	Boot and Tow	Please see *Boot Program* and *Handheld Citation Issuance* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.15	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Scofflaw for ability to alert agents of boot eligible vehicles ii) Genetec LPR equipment iii) PMIS Citation Management iv) Samsara (Dispatch Tool) iv) Others identified during Discovery with current vendor	**Out-of-the-Box**	Client Portal; OpsMan Mobile Enforcement Software	Passport intends to integrate with all of the listed City systems.

S1-PME-Dispatching

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Dispatching**	**This section describes the functional requirements for the Dispatching functions for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	GIS Vehicle/Agent tracking	Provide a real-time GIS interface to track vehicles and dispatch cases to agents via wireless communication on to HH devices.	**Out-of-the-Box**	AutoReturn ARIES	Please see *Dispatching* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	GIS with Scofflaw	Ability to view the location of LPR vehicles and vans, walkers, and the scofflaw hit list on a real-time GIS display to dispatch the closest available vehicle.	**Out-of-the-Box**	AutoReturn ARIES	Please see *Dispatching* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Case Request	Receive case requests from 311 (currently Salesforce) including the following data points: i) Case Origin, Type, Priority, Status, Assigned Agency, Assigned Department	**Out-of-the-Box**	AutoReturn ARIES	Please see *Dispatching* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Case Update	Provide case updates to 311 originated requests including the following data points i) Case Creation Date/Time, Case Closure Status, Case Closure Date/Time, Comments/Notes, Description, Status, Contact Information	**Out-of-the-Box**	AutoReturn ARIES	Please see *Dispatching* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Scofflaw for ability to alert agents of boot eligible vehicles ii) Genetec LPR equipment iii) PMIS Citation Management iv) Samsara (Dispatch Tool/Telematics) v) Salesforce (311 Tickets) vi) Business Intelligence iv) Others identified during Discovery with current vendor	**Out-of-the-Box**	Client Portal; AutoReturn ARIES	Passport intends to integrate with all of the listed City systems.

S1-PME-Adjudication

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Adjudication**	**This section describes the functional requirements for the Adjudication functions for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Suspend rules	Ability to automate and apply suspend rules while appeals are under investigation.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	Sort	Sort appeals/citations by type of violation and/or defense.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Record Decision	Record case decisions.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Modify, Edit, Cancel	Modify, edit, and cancel appeal/adjudication requests.	**Out-of-the-Box**	Process Appeals; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.5	Schedule hearing	Ability to schedule a hearing according to City rules.	**Out-of-the-Box**	Schedule Hearings; Customer Portal	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.6	Notes (one or multiple)	Enter notes on individual or multiple citations	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.7	Notes (internal or external)	Allow both Internal and External notes	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.8	Documents	Upload documents to support appeal/adjudication requests.	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.9	Disposition Status	Display disposition status (Paid, Convicted, Dismissed, Recipient Not Responsible per Valid Meter Claim, etc.).	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.10	Reason	Display reasons for adjudication (if dismissed).	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.11	Notes and minutes	Display notes or hearing minutes.	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.12	Specify suspend	Place individual citations, or multiple citations assigned to one license plate, on hold to suspend penalties and noticing for a specified timeframe.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.13	Remove hold	Automatically remove the hold once a specified date/event has passed.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.14	Adjust fines and fees	Adjust fines (reduce, add additional fines, fees, court costs, etc.).	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* as well as *General Citation* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.15	Correspondence	Send correspondence via mail and email regarding hearings, Court appearances and dispositions.	**Out-of-the-Box**	Process Appeals; Schedule Hearings	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.16	Notify Court	Provide notification to Court to proceed with default judgements.	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.17	Payment Tracking	Track payment of citations -prior to a hearing date -after customer fails to appear or fails to make payment	**Out-of-the-Box**	Batch Payment Report; Reporting	Please see *Adjudication* as well as *Enforcement Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.18	Tow Eligibility	Enter a disposition that places vehicles on tow eligibility list when an end user fails to appear or fails to make payment.	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.19	Alerts	Ability to receive notifications or alerts for events such as when a customer makes a payment or a customer submits an appeal.	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.20	Alerts	Ability to define user-specific notifications or alerts for events that require a citation to be in a specific status before the notification or alert is delivered. (Roadmap)	**Future Release**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.21	Alerts	Ability to receive notifications or alerts for events such as when a customer submits additional appeal documentation. (Roadmap)	**Future Release**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.22	Alerts	Ability to configure notification and alert events	**Out-of-the-Box**	Process Appeals; Manage Citations; Citation Details	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.23	Processing workflow/queue	Ability to queue appeals for processing with and without priority selection	**Out-of-the-Box**	Process Appeals	Please see *Adjudication* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.24	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) THEMIS, City's Court software ii) PMIS Citation Management and account Management iii) City Cashiering System iv) Business Intelligence iv) Others identified during Discovery with current vendor	**With Configuration**	Client Portal	Passport intends to integrate with all of the listed City systems.

S1-PME-Payments

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Parking Management and Enforcement - Payments**	**This section describes the functional requirements for Payment functions for the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	View payments	PMIS shall support the ability to view payment plans, split payments, auto payments, partial payments, and deferred payments as required by the City's Cashiering system.	**Out-of-the-Box**	Manage Payment Plans	Please see *Payments* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.2	View non-standard transactions	PMIS shall support the ability apply and view non-standard transactions, including but not limited to refunds, transfers to another citation, adjustments, and other non-standard transactions.	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Payments* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.3	Payment status	PMIS shall reflect the payments made and current citation status in real-time when payments are made.	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *Payments* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
1.4	Integrations	Integrations (1) City Cashiering System (2) Workday for DOTI Finance (3) PMIS Citation Management an Account Management (4) Permitting (5) Mobile/Web (6) Business Intelligence iv) Others identified during Discovery with current vendor	**With Configuration**	Client Portal	Passport intends to integrate with all of the listed City systems.

S3-Reporting

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Business Intelligence - Data Layer**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Standards	Adhere to standards for data completeness, accuracy, and timeliness (live data where applicable)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.2	Centralized	Organize data within the centralized system into logical, flexible configurations in which individual elements and tables can be linked to each other across conformed dimensions for multiple business uses	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	Access	The City must have access to all tables, data sets, and schemas through modern data transmission methods including APIs that do not require Contractor intervention	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	Structure	All structured and unstructured data shall be available to the City and provided upon request in an industry standard format (e.g., doc., xls, .pdf, logs, and flat files)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	ERD	The vendor will provide an entity relationship diagram(s) and data dictionaries to support development of end-user reports	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2	**Presentation Layer Components**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
2.1	Dashboards	Dashboards	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2.2	Heatmaps/GIS	Heat Maps and GIS Presentation	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2.3	Reports	Reporting assets/objects (static, standard, custom, variable)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3	**Presentation Layer Functions**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
3.1	Copy, Modify and Create	The solution will provide capability to copy and modify existing reports and dashboards to create new reports/dashboards	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.2	New Report configuration/build	The solution will provide authorized users the ability to configure or build new reports and templates.	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.3	Pre-defined	The solution will allow a user to save a personal copy for later execution of a pre-defined report with a set of specific selection criteria	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.4	Formulas and functions	The solution will provide functionality for the user to incorporate formulas, functions, and mathematical calculations into reports	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.5	Dashboard visualization	The solution will provide the ability to easily create and configure dashboards that show different analyses in visualizations that are comparable to modern data visualization programs (e.g., SAP Crystal Reports, Tableau, PowerBI, etc.)	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.6	Data points and analyses	The solution will provide the ability to add data points and fields to a report, provide slicing and parsing abilities to isolate data points by different variables, identify trends, conduct data range analyses, etc.	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.7	Sort and filter	The solution will provide the ability to sort and filter reports by predefined data fields	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.8	Operational reports	The solution will provide pre-defined reports that support day-to-day PMIS business functions that are automatically generated and distributed (pushed to the user) by the PMIS at a user defined time for publication	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.9	Export	The solution will provide the ability to export presentation layer assets (CSV, Excel, PDF)	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
4	**Integrations**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.1	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Permit Management ii) Business Intelligence iii) Handheld Enforcement iv) Genetec LPR v) Scofflaw for ability to alert agents of boot eligible vehicles vi) Genetec LPR equipment vii) PayByPhone and other Mobile Payment providers viii) Web/Mobile ix) Collections x) City Cashiering System iv) Others identified during Discovery with current vendor	**With Custom Programming**	Client Portal	Passport intends to integrate with all of the listed City systems.

S4-Web Mobile

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Web / Mobile**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Citation Inquiry	Ability to make parking citation inquiries by citation number and License Plate	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
1.2	PPI	Ability to hide Personal Identifiable Information (PII) such as customer name and address while performing an inquiry/search	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
1.3	Notifications/Reminders/Alerts	Ability to send email to permit holder when a new citation is issued to permitted license plate number	**With Custom Programming**	Customer Portal	If the customer holds an active permit, Passport can provide notification in that permit holder's account of any newly issued citations. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for details.
2	**Citations and Adjudication**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
2.1	View Citation and documentation	Ability to view a copy of a citation and related customer-facing approved documentation such as photos and notes	**Out-of-the-Box**	Customer Portal	Users will not be able to view videos attached to citations within Client Portal, however, a link could be added to a citation record via the "Add Note" feature. Users can then click the link and view a video in an external application. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
2.2	Adjudicate Citation	Ability to add/view the appeal/adjudication of parking citations	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.2.1	Adjudication documentation	Ability to edit/update the appeal/adjudication of parking citations such as uploading additional documentation	**Future Release**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.3	Adjudication documentation	Ability to upload supporting documentation to the appeal/adjudication of parking citations.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.4	Locate Towed Vehicles	Ability to identify and locate towed vehicles	**Out-of-the-Box**	Customer Portal	The Customer Portal can be configured to display a status indicating that a vehicle has been towed and can provide instructions to the customer that they will need to contact the City for further details.
3	**Payments**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
3.1	Payment Types	Ability to process parking citations i) credit card ii) debit card	**Out-of-the-Box**	Customer Portal	Passport's Customer Portal accepts all major credit/debit cards (Visa, Mastercard, Discover, and AMEX) as well as credit-card issuer-backed debit cards (i.e. the Visa/MasterCard logo is present on the card)
3.1.1	Payment Types	Ability to process parking citations i) electronic check	**Future Release**	Customer Portal	Passport's Customer Portal accepts all major credit/debit cards (Visa, Mastercard, Discover, and AMEX) as well as credit-card issuer-backed debit cards (i.e. the Visa/MasterCard logo is present on the card)
3.2	Citation Payments	Ability to process payment for citations or any other configurable fee type such as escaped boot fee, short check fee etc.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.3	Boot Eligible citations payment	Ability to identify, isolate and pay for boot eligible citations only	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.4	~~Permit Payment~~	~~Ability to process permit payments~~	~~**Out-of-the-Box**~~	~~Customer Portal~~	~~Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.~~
4	**FAQs and Content**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.1	FAQs	Provide FAQs for citation payment, appeal/adjudication, or other features.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
4.2	In-line and on-page content	Provide inline/on-page content to guide the user experience.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details
4.3	Guide	Vendor is expected to create a guide on how to view, pay and appeal/adjudicate citations, which must be available on the web/mobile platform	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
4.4	Redirects	Ability to accept redirects from Denver.gov and redirect customers back to Denver.gov upon completion of a user flow	**With Configuration**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
~~**5**~~	~~**Credentials**~~	~~**This section describes Web Mobile requirements that are required as part of the PMIS.**~~	~~**VENDOR RESPONSE REQUIRED**~~		
~~5.1~~	~~Credentials~~	~~Establish account credentials following City security protocols~~	~~**Out-of-the-Box**~~	~~Customer Portal~~	~~Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.~~
~~5.2~~	~~Username and password reset~~	~~Ability for customer to request forgotten username and/or request password reset from the Customer Portal and receive support/reset instructions/links through customer authorized channels including email~~	~~**Out-of-the-Box**~~	~~Customer Portal~~	~~Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.~~
6	**Compliance**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
6.1	Compliance	All Contractor managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines (collectively, "Guidelines") 3-20.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
7	**Integrations**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
7.1	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Permit Management ii) Business Intelligence iii) City Cashiering System iv) Others identified during Discovery with current vendor	**With Configuration**	Customer Portal	Passport intends to integrate with all of the listed City systems.

S5-Professional Services

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Non-automated communication via phone, internet/email, and mail**	**This section describes the functional requirements Professional Services**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Operational Hours	Provide a customer service support center for the City's parking program, at a minimum, from Monday through Friday and 8:00 AM to 5:00 PM MDT/MST, and subject to modification. Staff must be well trained, professional, and courteous customer service personnel equipped to handle clerical, customer service, supervisory, and managerial tasks in compliance with the approved operations and quality assurance plan. Callers seeking a live Customer Service Representative (CSR) must be serviced with an average Speed of Answer (ASA) of 60 seconds and an average abandon rate of under 5% per week.	**With Configuration**	A virtual cloud-based platform provided by Five9 will manage incoming and outbound calls using "Automatic Call Distribution" ("ACD") from Monday through Friday 8:00 AM to 5:00 PM MDT/MST. PRWT	PRWT recognizes that each live call interaction must be handled in a timely, courteous, efficient, and knowledgeable fashion and provide resolution consistent with the City's policies and guidelines, such as not placing any citizens calling for a live CSR on hold for longer than (2) minutes. In addition, PRWT will monitor and record all English and Spanish speaking customers calls for quality assurances purposes with call acceptance rates, call completion rates, and longest and shortest call wait time, captured by our virtual cloud-based call center platform.
1.2	Route Calls	Staff and/or reroute calls in the event the connection to the computer network is disrupted.	**With Configuration**	Data centers are geographically distributed in North America and Europe, The data centers currently process over 3 billion customer interactions per year, operate 24/7 and provide customers an option to choose geo- redundancy – the ability to route traffic to an alternate facility.	The virtual cloud-based call center architecture is deployed using hardened and secure data centers, which are designed to host mission-critical applications and databases. These data centers include fully redundant subsystems and compartmentalized security zones controlled by biometric access control methods. Data centers are regularly audited under AICPA AT 101 or SSAE 16 standards demonstrating robust data protection controls.
1.3	Call Scripts	Call scripts shall be developed by the Vendor, with City approval, for response to inquiries by customers.	**With Configuration**	PRWT will work with the City to develop a comprehensive knowledge base for customer service staff utilization. The City will approve telephone scripts and standards for telephone interactions.	PRWT looks forward to continuously working directly with designated City staff on policies and procedures as well as creating/adjusting call center scripts.
1.4	Business Processing Rules	Follow established business processing rules.	**With Configuration**	PRWT will configure primary functions as required to adhere to the City's business processing rules. If there is an inherent conflict based on functionality, PRWT will work with the City for resolution.	If there is a third-party provider that is integral to the service being provided, PRWT shall also work with that provider to align with the City's business processing rules.
1.5	Quality	Monitor and record calls for quality assurance for a term of 90 days, subject to the same terms for English or Spanish speaking customers. Monitor the call acceptance rate, call completion rate, and longest and shortest call wait time. An incomplete telephone call is defined as a call terminated after 30 seconds have elapsed from the time an individual's call is received in Passport's (or its subcontractor's) system.	**With Configuration**	PRWT understands that quality assurance is critical to the overall success in providing superior call center customer service. PRWT uses a comprehensive quality assurance program that supports the business operation and will establish a quality score card that reflects the measuring and monitoring of agreed upon call center and customer services metrics. Currently, PRWT monitors and measures key components of call handling by our CSR's.	PRWT has configured call recordings of inbound calls to capture CSR conversations during call sessions. Call recording allows PRWT to monitor and manage the quality of our Customer Support Service operations and ensure a positive citizen experience, reduce liability, resolve citizen issues, and comply with any regulatory and legal requirements.
1.6	Record Interactions	Log all interactions with end users, including interaction type (phone/email/mail), name, inquiry date/ time, issue type, notes, resolution, closed date/time in the subcontractors end user CRM system. An audio recording of all telephone calls with end users will be delivered to the PMIS system and attached to either a citation or permit record. City may request the specific logs of the call details using a defined process in an ad hoc manner.	**With Configuration**	Our CSR's will log and track all interactions with callers including interaction type (phone/email/mail), name, inquiry date/ time, issue type, notes, resolution, closed date/time.	PRWT will work with City to automate the logging of information process into acceptable reporting.
1.6a	Change Recording	All events resulting in changes to a citation record or permit record will be logged in the PMIS system and viewable in the citation or permit trail.	**Out-of-the-Box**		
1.7	Complaints	Complaints made by end users regarding Vendor service must be logged and reported to the City within twenty-four (24) hours of complaint.	**With Configuration**	Any complaints made by the public regarding PRWT's customer service will be logged and reported to the City within twenty-four (24) hours of the complaint.	PRWT will work with City to determine the reporting tool and format of the reporting.
1.8	Adjudication Request	Receive and process appeal/adjudication requests via web portal and US mail	**With Configuration**	PRWT's Call Center staffing will be trained initially by the City to receive and process parking appeals and adjudication request.	PRWT will establish formal training program to service citizen appeals and adjudication upon review and approval of the City.

1.9	Adjudication Hearing Prep	Appeal/adjudication preparation to include processing for initial hearing reviews	**With Configuration**	PRWT's Call Center staffing will be trained initially by the City to include processing for initial hearing reviews with appeals/adjudication preparation.	Initial hearing reviews will be included in the formal training for appeals/adjudication.
2	**IVR**	**This section describes the functional requirements Professional Services**	**VENDOR RESPONSE REQUIRED**		
2.1	IVR General	Operate a customized Interactive Voice Response (IVR) System in English and Spanish to accept payments and provide information. The interactive system must provide real-time information on each citation, including issue date, delinquent date, amount owed, and open citations by license plate number.	**With Configuration**	PRWT's IVR solution is a cloud-based platform with 100% up time or data center availability. In addition to the 100% up time, the platform is PCI, SSAE and HIPAA certified. Our solution provides a secure payment gateway that controls payment data collection by interacting with the City of Denver's Parking Citation Management System's interface while customers obtain payment authorization after posting credit and debit card payment information.	PRWT's solution provides robust reports (50+ standard and custom reports) which capture the number and types of calls that the IVR has handled such as call flow exit points, transfer status, inbound calls by DNIS, call volumes etc.- reports that can be exported by the City of Denver for internal use.
2.2	Inputs	The IVR system must recognize user inputs by touch tones and speech; include language support options to accept payments and provide information.	**With Configuration**	The IVR is a speech enabled system that will present menu options for both speech and DTMF (Dual-tone multi-frequency signaling entered values) and allow callers to return to the main menu and prior menus by entering the menu selection numbers. Menu selections items are usually between 1 to 5 items, so citizens are not overwhelmed.	The "Adaptive Personalization" feature can automatically push specific menu options to the front of the call flow. The IVR will play all voice prompts in the languages that customers prefer.
2.3	Live CSR Option	The IVR system shall offer the caller the option of a live CSR during operating hours and the CSR option must be provided early in the phone script.	**With Configuration**	The IVR system shall offer callers the option of a live CSR during operating hours and the CSR option will be provided early in the IVR script tree.	With configuration, citizens can prompt for CSR during any time of the IVR script.
2.4	IVR Operations	Provide the City with a toll-free telephone line that accepts global payments by Interactive Voice Response (IVR) 24 hours a day, 7 days a week. City's current provider will transfer the existing phone number to the new provider as part of the implementation.; must be Payment Card Industry (PCI) compliant.	**With Configuration**	PRWT's IVR solution will provide the City of Denver's Parking Citation Management initiative with a 24-hour, 7 days a week, 365 days per year automated telephone answering system.	The "Adaptive Personalization" feature can automatically push specific menu options to the front of the call flow. The IVR will play all voice prompts in the languages that customers prefer.
2.5	Payment Methods	Must be Payment Card Industry (PCI) compliant. i) Payment types (1) Credit card (2) Debit card (3) Electronic Check (Roadmap) ii) Credit card payments shall be processed through a City-owned Merchant Identification (MID) code approved and issued by the Cash Managements Section under the existing merchant services agreement managed therein. Vendor must certify to process with the City's existing merchant services provider prior to implementation	**With Configuration**	The intelligent self-service IVR delivers services that includes providing citizens with parking enforcement violations specific payment options in a fully compliant PCI DSS environment	The IVR prompts the caller to enter their card number using DTMF and to press the pound (#) key when complete. The DTMF collection will allow up to 19 digits to be entered to account for various payment options. Credit cards will be processed through the City's MID code. PRWT will comply with certification requirements prior to implementation.
2.6	No Convenience Fees	The assessment of credit card convenience fees to customers is not part of the City's current receipting business model. Any proposal to assess fees beyond the cost of City services shall be submitted to the Cash Management Section for review and submission to the Manager of Finance for approval.	**With Configuration**	Any convenience fee assessment shall be reviewed that is beyond the City's current parameters and approved by the Manager of Finance	PRWT needs to understand the City's cost of services receipting business model.
2.7	DoF Compliance	Ability to comply with Department of Finance (DoF) payment processing, deposits, reconciliation, and compliance rules.	**Out-of-the-Box**	PRWT will comply with Department of Finance (DoF) payment processing, deposits, reconciliation, and compliance rules.	City must provide guidelines for compliance.
3	**Lockbox Processing**	**This section describes the functional requirements Professional Services**	**VENDOR RESPONSE REQUIRED**		
3.1	Accept mail-in citation payment	Accept mail-in citation payments (lockbox) preferably to a Denver mailing address. Existing mailing address will be transferred from existing Vendor to Passport during implementation.	**Out-of-the-Box**	PRWT will secure a P.O. Box at the local Post Office. Mail will be handled via courier to our physical Lockbox with a Denver address.	All mail-in citation payments and correspondence will reference the designated Denver P.O. box address for processing.
~~3.2~~	~~Lockbox processing center~~	~~Establish a Lockbox processing center location(s), including address(es) and a unique zip code, where applicable, and employees to support this function.~~	**~~With Configuration~~**	~~PRWT has established physical space for the location of the lockbox processing center within Denver city limits to house operations and staffing for processing of all mail intake that includes payments and correspondence.~~	
~~3.3~~	~~Support personnel~~	~~Provide support personnel (include resume).~~	**~~With Configuration~~**	~~Operational support Staffing will be local to the Denver area. Staffing will be selected upon award.~~	

3.4	Process payments	Process mailed payments via lockbox processing, in-house remittance processing, third party remittance processing, or another process identified by Passport	**With Configuration**	PRWT will provide a fast and efficient processing solution for payments and correspondence for the City of Denver's Parking Citation Management initiative. PRWT offers state of the art image capture based remittance processing that can electronically deposit checks (EFT) of all sizes with superior back-end processing software. PRWT is committed to processing payments by the fastest, most cost-effective means possible. We constantly evaluate and utilize the clearing methods that are best for our customers to ensure timely and accurate application of payments which is a critical component of excellent customer service.	PRWT will provide reliable, accurate lockbox services utilizing advanced remittance processing technology along with full control measures ensuring client compliance in our lockbox processing centers for parking citation payments, notice payments, and citizen correspondence.
3.5	Pickups	Perform post office pickups daily (on days that the post office is in operation).	**Out-of-the-Box**	PRWT will use a bonded courier for daily pickup from Post Office P.O. box.	
3.6	Scanning	Provide Item scanning technology (Bar Code, Optical Character Recognition (OCR), Scan Line, etc.). Scan and handle non payment information based on routing rules defined between Vendor and City.	**With Custom Programming**	PRWT's image capture Check 21 processing solution utilizes an extensive set of features. Standard features include Optical Character Recognition (OCR), an auto-feeder with an open feeder design for improved productivity, industry-leading Magnetic Ink Character Recognition (MICR) reader, high-quality image with 300 dpi image cameras, and endorsement decisions based on MICR and/or front image content such as optical character recognition, bar code recognition, or image quality results.	Custom programming is required for the image capture and reading of Denver's current payment processing coupons and notices scanlines for accurate reading of payment information.
3.7	Processing timelines	Establish and comply with payment processing timelines; citations are time sensitive and must be processed within City established timeframes (currently 1-3 days of time of receipt at processing center), and in order of first received.	**Out-of-the-Box**	PRWT will comply with all payment processing timelines and timeframes.	Current compliance is 1-3 days in order of receipt.
3.8	Quality	Comply with quality controls performed for the City of Denver.	**With Configuration**	PRWT will comply with quality control established by the City of Denver.	PRWT will meet with City to review current quality controls and suggest our quality control best practices as well.
3.9	Data Transmission	Establish a data transmission process (both for incoming and outgoing files).	**With Custom Programming**	The data transmission process will be in conjunction with the established parameters in use by the City.	PRWT must review current transmission process to understand it's strengths and weaknesses to provide the most secure method for payment file data.
3.10	Exception Handling	Establish an exception handling process to be approved by the City prior to implementation.	**With Configuration**	PRWT will work with City to establish an exception handling process.	PRWT will use City's approved exception process.
3.11	Error Resolution	Establish an error resolution process/plan to be approved by the City prior to implementation.	**With Configuration**	PRWT will establish an error resolution process/plan in conjunctions with the City	PRWT will utilize City's approved process/plan.
3.12	Conversion and Float Schedule	Establish and provide Check conversion (Accounts Receivable Conversion (ARC)), Image Replacement Document (IRD), ACH, etc.) and float schedule.	**With Custom Programming**	PRWT will establish and provide a fast and efficient processing solution Check conversion (Accounts Receivable Conversion (ARC)), Image Replacement Document (IRD), ACH, etc.) and float schedule.	PRWT will need to review City's specifications prior to custom programming
3.13	Document Archival and Disposal	Provide document archival and disposal.	**Out-of-the-Box**	PRWT will provide archival and disposal.	PRWT will meet with City to determine retention/disposal timelines.
3.14	Operational Reports	Provide a daily and monthly reports of operational effectiveness	**With Custom Programming**	PRWT will develop robust reporting to capture operational KPI's.	PRWT will work with City to determine reporting metrics.
3.15	Deposits	Deposit funds daily by either electronic or physical delivery into a city owned bank account approved by the City's Cash Management Section.	**With Configuration**	PRWT will deposit funds daily in target banks approved by the City's Cash Management .	Check 21 will deposit all funds daily by EFT.
~~3.16~~	~~Bank Delivery~~	~~Make physical bank deliveries; City preferred method is armored car.~~	~~**Out-of-the-Box**~~	~~PRWT will use armored car for all cash deposits.~~	~~Bonded armored courier will be utilized.~~
3.17	Electronic Deposits	Make ACH, wire, or other means of electronic depositing.	**With Custom Programming**	PRWT will use ACH and Check 21 as methods of EFT depositing.	Custom programming is required.
3.18	MID	Process credit card transactions and any associated fees. Note: Credit card payments shall be processed through a City-owned Merchant Identification (MID) code approved and issued by the Cash Managements Section under the existing merchant services agreement managed therein. Vendor must certify to process with the City's existing merchant services provider prior to implementation.	**With Configuration**	PRWT will process credit card transactions with associated fees. Processing will be through a City-owned Merchant Identification (MID) code approved and issued by the Cash Managements Section under the existing merchant services agreement managed therein. PRWT will certify to process with the City's existing merchant services provider prior to implementation.	PRWT will meet with City to review.

3.19	Charge Back Controls	Comply with charge back quality controls/reconciliation performed for the City of Denver.	**With Configuration**	PRWT will comply with charge back quality controls/reconciliation performed for the City of Denver.	PRWT will meet with City to review.
3.20	Short Check Controls	Comply with short check quality controls/reconciliation performed for the City of Denver.	**Out-of-the-Box**	PRWT will comply with short check quality controls/reconciliation performed for the City of Denver.	PRWT will meet with City to review.

3.21	Returned checks	Handle uncollected returned checks as follows: All returned checks received by the Vendor that are not successfully collected within one hundred twenty (120) days of their receipt shall be sent to the City and County of Denver, Treasury Division – Asset Recovery Service to be sent for collection to the contracted collection attorneys	**Out-of-the-Box**	PRWT will review uncollected returned checks within 120 days of receipt with the City for review and determination	PRWT will meet with City to review.
3.23	Overpayments	Handle overpayments as follows: Overpayments shall be reviewed monthly and refunds issued accordingly for any citation overpayment that is more than 365 days from payment date.	**Out-of-the-Box**	PRWT will review Overpayments monthly and refunds issued accordingly for any citation overpayment that is more than 365 days from payment date.	PRWT will meet with City to review.
3.24	Batch Processing	Handle batch processing: the processing of multiple payments identified by a unique batch number.	**With Configuration**	PRWT currently processes payment with batching and each batch has a unique identifier.	PRWT's best practices for payment processing.
3.25	PCI Compliance	Procedures and systems must prove certified Payment Card Industry Data Security Standard (PCI DSS) compliant and/or identified as out of scope by the City's PCI Committee prior to selection. All credit card processing solutions must comply with PCI DSS rules and regulations as specified by the City's Cash, Risk and Capital Funding group.	**With Configuration**	PRWT's procedures and systems are certified PCI DSS for credit card processing. New lockbox environment in Denver will need to be reviewed and approved PCI DSS internally.	PRWT will review with the City's PCI Committee prior to selection.to ensure that processing solutions comply with PCI DSS rules and regulations as specified by the City's Cash, Risk and Capital Funding group.
3.26	ACH Compliance	Systems and procedures must comply with the National Automated Clearing House Association and applicable rules and regulations surrounding Fed wires when processing ACH or wire payments, to be approved by the City's Cash Management Unit prior to implementation.	**Out-of-the-Box**	PRWT's systems and procedures comply with the National Automated Clearing House Association and applicable rules and regulations surrounding Fed wires when processing ACH or wire payments.	PRWT will await approval by the City's Cash Management Unit prior to implementation.
3.27	Cash Handling Compliance	Vendor must comply with all cash handling requirements specified by the City's Cash, Risk and Capital Funding group, as outlined in the attached Cash Handling Guidelines.	**Out-of-the-Box**	PRWT will comply with all cash handling requirements guidelines.	PRWT will comply with City's Cash, Risk and Capital Funding group, as outlined in the Cash Handling Guidelines.
3.28	Audit	Vendor shall provide the City with any information requested as pertains to the audit of a specific revenue stream or function to verify completeness of records, identify balancing issues, and fully reconcile all payments.	**With Configuration**	PRWT will provide all information to the City's request for the audit of a specific revenue stream or function to verify completeness of records, identify balancing issues, and fully reconcile all payments.	PRWT will meet with City to determine policies and procedures as required.
3.29	Process correspondence	Open, Review, Sort, and Index incoming correspondence which may include digital records	**With Configuration**	All received correspondence will be processed.	As per City's specifications.
3.30	Transform correspondence	Transform written correspondence into electronic form and handle based on routing rules provided by the City.	**With Configuration**	PRWT will image capture all correspondence received.	PRWT's intelligent remittance software captures, processes and applies business rules to full-page correspondence documents, checks, payment stubs through forms recognition technology.
3.31	Associate with record	Associate or append correspondence with record or citation in PMIS	**With Configuration**	PRWT will link any correspondence received with payment to the citation record within the PMIS.	Any orphan correspondence will be researched to connect to citation record through a unique identifier if possible.
3.32	Apply Payments	Apply all payments received	**With Configuration**	All payments received, processed and applied.	PRWT is committed to processing payments by the fastest, most cost-effective means possible. We constantly evaluate and utilize the clearing methods to ensure timely and accurate application of payments which is a critical component of excellent customer service.
3.33	Response Timeframe	Generate the appropriate responses and respond in kind to citizen inquires within timeframes established by the City.	**Out-of-the-Box**	PRWT will comply to respond to citizens inquiries within timelines established by the City.	PRWT will meet with City to determine timelines for responding.
3.34	Search and Retrieval	Provided City capability to search and retrieve correspondence upon request	**With Configuration**	PRWT will provide correspondence images through image capture functionality .	City can review with notification to PRWT prior to viewing.
4	**Integrations**	**This section describes the functional requirements Professional Services**	**VENDOR RESPONSE REQUIRED**		
4.1	Integrations	Integrations i) Business Intelligence ii) PMIS Citation Management iii) PMIS Account Management iV) City Cashiering System iv) Others identified during Discovery with current vendor	**With Custom Programming**	All integrations must be reviewed to determine the methodology with other platforms	PRWT will work with City and other vendor platforms to determine level or usefulness of potential integrations once all specifications are reviewed for each platform

All Sections-Non-functional Requirements

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Identity Management and Security**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**		**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Identity Management	**This is a mandatory requirement** Ability to integrate with the City's multifactor authentication (MFA) and single sign-on (SSO) solution DUO Security.	**With Custom Programming**	User Management	**This is a mandatory requirement** Passport does not support single-sign-on capability in its system. Passport does employ 2FA within its back-end system via Google Authenticator. After inputting their user ID/password credentials, users must enter a 6-digit validation code that is generated from the Google Authenticator app in order to log in.
1.2	Credentials	This is a mandatory requirement Ability to comply with the City's Identity Management protocols. Internal corporate or customer (tenant) user account credentials shall be restricted ensuring appropriate identity, entitlement, and access management and in accordance with the following established policies and procedures: a) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) b) Account credential lifecycle management from instantiation through revocation c) Account credential and/or identity store minimization or re-use when feasible d) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)	**With Custom Programming**	User Management	**This Is a mandatory requirement** Passport is unable to comply with management protocols listed here such as single-sign-on. As stated in 1.1, Passport does employ the use of multi-factor authentication via Google Authenticator in order to access the system.
1.3	Role-Based Security	Role based security where access to data, screens, and critical functions can be limited based on roles or groups	**Out-of-the-Box**	User Management	Please see *User Activity and Permissions* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
1.4	Audit Logging	Audit logging where user activity is recorded for security and auditing	**Out-of-the-Box**	User Management; Reporting	Please see *User Activity and Permissions* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
2	**End User and Device Compatibility**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
2.1	Web Browsers	All web applications that will be accessed by the public must be compatible with current versions of Microsoft Edge and Google Chrome.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.2	Computing Environment	Compatibility with current desktop, laptop or tablet computing environments. Computing environment specifications and additional written responses will be required if the vendor is shortlisted.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.3	Mobile Devices	Any software that is intended to run on mobile devices should support the current release of iPhone, iPad, Android and Windows Phone.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.

3	**Usability and Accessibility**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
3.1	Image Alt text and Color Contrast	Images are properly described (using alt text) and provide readable color contrast	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.2	Image enlargement	Text and images are large and/or enlargeable	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.3	Logical order	Headers are used in a logical order of hierarchy	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.4	Contact and Contrast	Link and button text are descriptive with underline and properly contrasted color	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.5	Video	Videos are closed captioned	**Cannot Meet**	N/A	While Passport plans to build out video functionality in its system, the availability of closed captioning on those videos has not yet been determined.
3.6	Web Flash	Web pages do not contain anything that flashes more than three times in any one second period	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.7	Content	Content is written in plain language and illustrated with instructional diagrams (when applicable)	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.8	Document accessibility	Documents are fully accessible and converted to PDF format for best use	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.9	White Label	Use City Brand standards for white label portions of the solution. White label designs will be subject to City approval	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.10	**Application and Interface Security**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
3.11	Application Security	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements - Connectivity* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
3.12	Data Integrity	Data input and output integrity routines (i.e. reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.

3.13	Data Integrity and Security	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration or destruction. These policies and procedures shall be in accordance with known legal, statutory and regulatory compliance obligations.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
3.14	Connections to External Systems	All credentials required for communication with external systems shall be encrypted.	**Out-of-the-Box**	Client Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
3.15	System and Application logging	Ability to utilize the City's centralized system for security information and event management.	**Cannot Meet**	Client Portal	Passport would need more information on what the City is looking for in order to scope and commit to this requirement. Passport welcomes discussions to better understand the City's intention and use case(s).
4	**Interoperability**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.1	APIs	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements - Connectivity* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
4.2	Standardized Network Protocols	The provider shall use secure (e.g. non-clear text and authenticated) standardized network protocols for the import and export of data.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
5	**Deployment Model**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
5.1	Hosted or Hybrid Model	a) Use one of the following deployment models: i) Cloud hosting ii) Managed hosting iii) Hybrid cloud and managed hosting	**Out-of-the-Box**	Client Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.

6	**Policy Compliance**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
6.1	Policies	Vendor will ensure that the PMIS solution meet all City Policies as well as Federal, State, and local laws and regulations and will attest to adherence with City Policies at the beginning of the contract and annually thereafter. i. Data Retention Policy ii. Department of Finance Cash City and County of Denver – Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds iii. ADA policy iv. Branding and UX Standards v. Security Policy vi. TS Architecture Standards vii. PCI/PII Compliance viii. Internet of Things (IOT)	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
7	**Data Migration**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
7.1	Migration Strategy	Ability to provide a comprehensive migration strategy to migrate all data from existing permit, citation and issuance/enforcement, boot &, customer contact, and collections systems to new solution. This includes but is not limited to eTIMs General Processing, eTIMs Workflow, ReportWeb, City Sight Enforcement, Tableau, Merge, Scofflaw and operational spreadsheets.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.2	Extract data	Ability to extract data; capture all data in scope for migration.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.3	Transform data	Ability to transform data as required for input into new solution.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.4	Data Validation	Ability to perform data validation/data clean up on migrated and transformed data.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.5	Data Testing	Ability to perform comprehensive testing to ensure migration quality, integrity and completeness.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.

8	**Operational Service Level Agreements**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
8.1	Operational Hours	Ability to comply with the City's Operational Hours. The PMIS components shall be operational 24 hours per day, Monday through Sunday.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.2	Maintenance Window	Maintenance to the online environment shall not be performed by the Vendor between 6:00 AM and 11:00 PM, Monday through Sunday without the express permission of the City.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.3	Maintenance Window	Schedule PMIS System maintenance between the hours of 12:00AM and 4:00AM with notification to City staff one (1) week in advance.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.4	Hosted/Cloud Availability %	99.9% Availability for hosted/cloud services. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.5	Application Availability %	99.9% Availability for software applications. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.6	Integration/Interface Availability %	99.9% Availability for software applications. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.

9	Capacity	This section describes the technical/non-functional requirements required for all systems and components of the PMIS.			
9.1	Number of Users Parking Account Management	Minimum of 150 total and concurrent users.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
9.2	Handheld Enforcement	Minimum of 200 total and concurrent users.	**Out-of-the-Box**	OpsMan Mobile Enforcement Software	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
9.4	Number of Users Reporting	Minimum of 50 total and concurrent users.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
9.5	Number of Users Boot	Minimum of 20 total concurrent users.	**Out-of-the-Box**	Boot and Tow; AutoReturn ARIES	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
9.6	Web Mobile - Number of Visits City Customers	Ability to support 5,000 visits per day.	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.7	Web Mobile - Number of Visits City Customers	Support a minimum of 5000 Citation payments per day	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
9.8	Web Mobile - Number of Visits City Customers	Support a minimum 1000 Adjudication requests per day	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.10	Web Mobile - Number of Visits City Customers	Meet benchmark application page load under 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.

9.11	Web Mobile - Number of Visits City Customers	Meet benchmark TTFB (Time-to-First-Byte) under 1.5 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.12	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for standard reports and dashboards 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.13	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for interactive queries 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.14	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for deep analytics 60 minutes	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.

Vendor Response Lookup

RequirementCompliance	Description
Cannot Meet	The product cannot meet the requirement “Out-of-the-Box”, “With Configuration”, “With Custom Programming” or with a “Future Release”.
Future Release	The current version of the solution cannot meet the requirement “Out of the Box” or “With Configuration” but will be able to with a scheduled, future release of the product. The scheduled release must be within 4 months from date of final RPF response. Vendors may be asked to provide a current roadmap, requirements or user stories to validate this claim.
With Custom Programming	The solution can meet the requirement only by modifying the product’s source code (changing or adding new code) to enable it to do what it was not originally able to do. This custom programming is expected to be completed upon transition to the City. Vendors may be asked to provide evidence of similar custom programming provided to other clients including overall time for completion or a demonstration of its completion.
With Configuration	The solution can meet the requirement by arranging the functional parameters that are already inherent in the product – and not by changing the product’s source code – so that it functions in a way that meets the City’s specific business needs. The vendor may be asked to provide a demonstration of this configuration or provide evidence of similar configuration provided to other clients.
Out-of-the-Box	The solution meets the requirement as is, “out-of-the-box” functionality with no configuration or custom programming/coding. The City expects any functionality with this designation to be available for live demonstration. An inability to provide a live demonstration will be considered non-responsive or 'cannot meet'.
Prioritization Type	Prioritization Description
Must Have	Requirements labeled as "Must Have" are critical to the current delivery timebox in order for it to be a success. If even one "Must Have" requirement is not included, the project delivery should be considered a failure (note: requirements can be downgraded from "Must Have", by agreement with all relevant stakeholders; for example, when new requirements are deemed more important).
Should Have	Requirements labeled as "Should Have" are important but not necessary for delivery in the current delivery timebox. While "Should Have" requirements can be as important as "Must Have", they are often not as time-critical or there may be another way to satisfy the requirement, so that it can be held back until a future delivery timebox.
Could Have	Requirements labeled as "Could Have" are desirable but not necessary, and could improve user experience or customer satisfaction for little development cost. These will typically be included if time and resources permit.
Won't Have	Requirements labeled as "Won't Have" have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time. As a result, "Won't Have" requirements are not planned into the schedule for the next delivery timebox. "Won't Have" requirements are either dropped or reconsidered for inclusion in a later timebox. (Note: occasionally the term Would like to have is used; however, that usage is incorrect, as this last priority is clearly stating something is outside the scope of delivery).

Attachment C

City and County of Denver
201 W. Colfax Ave.
Department 304, 11th Floor
Denver, CO 80202

Parking Management Information System

Permitting

Business and Technical Requirements

Table of Contents

Goals and Objectives

ID	Goals	Objectives
1	Future Proof	Able to incorporate future technology and mobility options Able to address unforeseen circumstances Able to address evolving and/or nontraditional business needs such as creating a new permit for outdoor Proactive in anticipating future needs in mobility, curbspace and the City's operational and policy changes State of the Art Technical Requirements: API Interoperability with any existing or future systems Fundamentally sound and reliable systems Industry standard cloud hosting
2	State of the Art Data Analytics Platform	Integrated with industry standard platforms and tools (Azure, AWS) Intuitive User Interface Dashboards/tables full flexibility Data validation/curation Responsive to data requests Proactive in anticipating future needs Machine Learning Predictive Analytics
3	Adaptable & Scalable	Technological capacity infrastructure growth built-in Ability to support large and complex data Ability to process Data at speed Nimble system e.g., ability to consolidate data with quality and stability
4	Ability to Control	Access to Settings – customizable user settings, administrator access level configurable, changes should be possible on a user setting level - no programming required Full access to data: Real time / Live Intuitive data transformation layer Timely and customer focused accessible data delivery
5	User Friendly – Internal & External	Internal Such as integrated with DMV Source of truth Robust customer service Intuitive workflows External One stop government compatible Streamlined service delivery for customers Modern functionality for customers Seamless customer experience for all things parking
6	Proactive, Future Oriented & Supportive Vendor Culture	Best in class culture Proactive in anticipating future needs Consulting Culture Increased efficiencies through continuous workflow / process improvement

Background

The City and County of Denver has a residential population of 727,211. The U.S. Department of Transportation's Smart City Challenge charged the City and County of Denver to think of transformative, multidisciplinary Smart City projects that could improve mobility. Denver was one of seven national finalists provided the opportunity to think beyond normal budget constraints, knowledge barriers and technological hurdles to identify a concrete path forward with a focus on innovative technologies, vehicle electrification and connected neighborhoods.

The City provides on-street paid parking with approximately 6,200 IPS single space meters and starting in March 2022 with an increasing number of IPS multi space meters with payment options ranging from cash to credit cards and Pay by App. Additionally, the City provides virtual and physical Parking and Occupancy Permits for Residential Parking, Official City Business, Emergency Trucks, Truck Loading, Food Trucks, and other specialty permits. City customers also can apply for Meter permits which block meter(s) for valid reasons such as construction or events.

Multiple Permit programs are managed by the Department of Transportation and Infrastructure through its Transportation Operations Division and Right of Way Services Division. The teams process new and renewal permit applications (Residential Parking permits, Official City Business permits, Food Trucks permits, Meter permits). The City will use both physical and virtual permits (license plate-based and location based). The City seeks to bring more permits from physical to virtual and is actively working on improving the online offering for multiple permit types as well as exploring new permit programs such as managed loading zones.

Annual Permit Transactions

Transaction Type	Average per year (past 5 years)
Permits (all categories)	40,000 – 75,000

Customer interfaces are provided to City customers to initiate new and renewal permit applications and establish accounts to manage these permits.

Parking Management Information System (PMIS) Overview

The City's vision is a transformative and fully integrated the Parking Management Information System (PMIS) consisting of 3 main functional components:

Parking-Related Systems	**Technology/Service Provider**	**Included in this BRD**
Parking Enforcement and Management	Passport	No
Professional Services	Passport	No
Permitting	Passport	Yes

The following systems constitute the main components of the current PMIS solution

Parking-Related Systems	Technology/Service Provider	To be retired or replaced	Retired by this BRD
Citation Issuance & Enforcement software	Conduent State & Local Solutions, Inc.	Yes	No
Citation Management System software	Conduent State & Local Solutions, Inc.	Yes	No
Business Intelligence software	Conduent State & Local Solutions, Inc.	Yes	Partial
Permit Management Solution software	Conduent State & Local Solutions, Inc.	Yes	Yes
Single Space Parking Meters	IPS Group, Inc.	No	No
Multi-Space Parking Pay Stations	IPS Group, Inc.	No	No
On-Street Mobile Payment	PayByPhone	No	No
Parking Access and Revenue Control Systems (PARCS)	SKIDATA Inc. & T2 pay stations	No	No
LPR	Genetec AutoVU*	No	No
Handheld Enforcement Devices	ZEBRA TC77, Zebra printer ZQ510, 3 IN BT4.0	No	No
Mobile Data Terminals (Ruggedized Laptops)	31 Vehicles, incl. 7 Boot Vans	No	No

Functional Requirements

Note: Any requirements that are no longer required or have otherwise been removed from the scope of the initial implementation since RFP publication are indicated with a ~~strikethrough~~. Any requirements that will be met in a future release have been designated with the modifier Roadmap. Any new requirements identified during Planning and Analysis shall follow the Change Order process as outlined in the Statement of Work.

1. Permit Program

The Permit Management component of the PMIS system is the software and support solution that will supply the City with all parking permit processing functions. Such functions are outlined below. The core functionality must include the option for City staff and customers to search by permit number, license plate number, account number, permit holder name, permit type, and location/address, apply, renew, and pay for permits.

Additional functionality will include the support of waitlists by permit type and location, the ability to process payments, and manage all permit types - amounts, exemptions, and locations. Users may have specific functionality access assigned by a designated software administrator. Software shall limit permit eligibility by the city defined rules.

Permit Management will support the validation of documentation to establish that a customer is eligible to purchase a permit. For example, residents must provide a valid driver's license, current vehicle registration and proof of residency (utility bill, telephone bill, TV, or internet bill, auto or home insurance document) in a designated residential zone or area. In the future, validation may also be completed through integrations with DMV or other services to verify customer eligibility and address. The City currently operates physical permits as well as license plate and location based virtual parking permits. Passport will support both physical and virtual parking permit programs.

Permit Management Software Specifications

1) Permits General (includes Meter Bagging permits)
   a) Support both physical and virtual permit programs utilizing LPR technology
   b) Support both annual and temporary time-limited permits
   c) Generate unique permit numbers
      i) Unique parking permit numbers per city defined criteria (including pending or pre-issued permits) such as License plate number, type of Permit code, other indicators. Permit numbers should allow both numbers and letters
   d) Accommodate requests for multiple permit types
   e) Physical permit stock to be supplied by the Vendor, optional
   f) Ability to support the printing of QR permits for temporary or regularly issued permits
   g) Ability to print permit information through template files, as necessary
   h) Permit query results shall display in logical order including the number of accounts and number of active permits associated with accounts
   i) Support rolling expiration dates (e.g., daily, weekly, monthly, annually)
   j) Support guest permits with physical and/or virtual permits

2) Permit Account Management

   The solution shall support these general account management and customer relationship management functions. Once a customer account, permit record or customer interaction is created there should be a viewable audit trail of the event. The following account management and customer relationship management functions will be available:

   a) Web-based software solution that provides permit-related data, accessible by City staff
   b) Integration of permit data in real-time

c) Permit Account attributes include:
   i) Name (First, Last or Business)
   ii) Account Type
   iii) Account Number
   iv) Contact information (phone, email, preferred contact method)
   v) Address
   vi) Vehicle(s)/Plates(s)
   vii) Any additional custom data field for each permit, as defined by City
d) Create, edit, or update permit record
e) Ability to create permit records based on different attributes such as license plate, location, person, or company/fleet
f) Inactivate permit records with optional reason code in accordance with Business Rules
g) Retain inactivated permit and account information
h) Add notes to permit records
i) Ability to View permit customer account data and View/Add/Edit permit record data.
j) Ability to search for permits by customer name, business name, license plate, permit number, address.
k) View files and documentation associated with a permit record (photos, voice, correspondence, etc.)
l) Ability to add specialized notes to the permit record
~~m) Integrated messaging and ability to send messages to other authorized users of the system~~
n) Send physical letters to permit holders
o) Send emails to permit holders when account changes are made including permit application submission, permit application approval, permit payment receipt, and renewal notices.
p) Send email to permit holder when a new citation is issued to permitted license plate number.

3) Permit Applications and Permit Waitlists
   a) Accept web/mobile applications for Permits
   b) Autofill and standardize address entries, during permit application and editing of permit addresses, utilizing Denver Address Database
   c) Limit permit availability based on geographical location (address validation) of requested permit or other City-determined factors in accordance with Business Rules
   d) Limit issuance of permits (i.e. Residential Parking Permits) by License Plate, Entity/Business or Person (Driver's License) in accordance with Business Rules
   e) Prevent parking violators with open citations from obtaining certain permit types such as residential parking permits
   f) Ability to search for meter permits based on meter ID and permit holder
   g) Ability to manage inventory of meters and their status (Available, Pending Permit, Approved Permit, Unavailable)
   h) Ability to see current and future meter bag requests to manage operations
   i) Support varying exception permit processes and quantity limitations by a designated period for both daytime and overnight permits
   j) Restrict or allow multiple permit purchases for the same plate number depending on Business Rules
   k) Validate permit program eligibility based upon supporting documentation
   l) Support waitlists, by permit type and location

4) Process Permit Applications (Automatic or Manual)
   a) Establish permit processing work queues/workflow and rules for permit processing work queues/workflow including establishing different queues for different permit types and priority routing in accordance with Business Rules
   b) View permit applications and attached documents
   c) Process payment for permits
   d) Process multiple permit requests in one transaction
   e) Edit any permit field (based upon user-assigned privileges)
   f) Provide bulk permit purchases for group accounts
   g) Refund a permit
   h) Cancel a permit

5) Issue Notifications
   a) Automatically send permit renewal notices by mail and email in accordance with Business Rules
   b) Configure multiple notification schedules
   c) Print and email correspondence letters to permit holders in accordance with Business Rules
   d) Ability to support multiple notification types (mail and email)
   e) Issue permit renewal notices by batch or individually

6) Configure Permits
   a) Create/modify/delete permit zones
   b) Create/modify/delete permit eligibility rules by permit type
   c) Create/modify/delete permit eligibility rules by geographical zones
   d) Create/modify/delete permit fee schedules by permit type, zone, and other eligibility criteria
   e) Provide a variable rate fee structure based on permit type
   f) Create/modify/delete permit application rules
   g) Allow for ongoing configuration to meet changing City business needs, or changes to local, State, or Federal laws

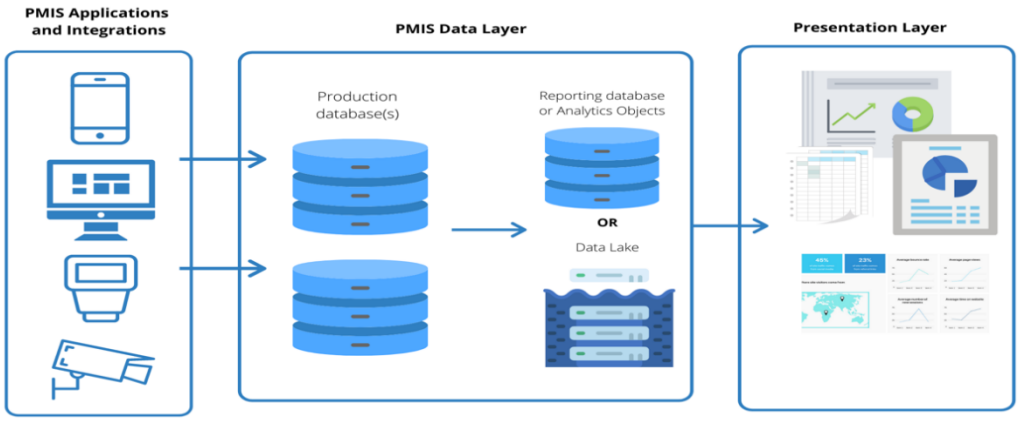
7) User Activity and Permissions
   a) Assign permissions to access certain features based on user ID
   b) Create an audit trail for all user actions that result in a change to a record
   c) Review all user actions that result in a change to a record within the software

8) Integrations
   a) Integration with City Cashiering System
   b) PMIS Citation Management an Account Management
   c) Mobile/Web
   d) Business Intelligence
   e) Accela
   f) Single Space and Multi Space hardware infrastructure
   g) Third Party Integrations for eligibility validation

2. Reporting

The City has a need to be able to aggregate, analyze and report on the data collected from all PMIS related solutions for a centralized view of the entire City Parking Program, A consolidated data view is required to provide executive insight into the City's Parking Programs' performance, as well as provide insight for both tactical and strategic decision support. The Business Intelligence solution will streamline the City's efforts to search for data and transform it into actionable intelligence. The Business Intelligence solution will provide easy to-use interfaces, easily accessed and combined data sources, and built-in visual best practices. In addition, the Business Intelligence solution will be scalable, allowing the City to scale its Business Intelligence needs over time.

Additionally, the City will be able to view and run operational, analytical, and financial reports for administrators, supervisors, and managers to perform their daily functions and reconciliation, keep apprised of operations, identify areas to improve operational efficiency and locate trends. Daily, weekly, and monthly operational and financial reports will be available to users.



1) Centralize all Parking Data in a Data Layer
    a) Adhere to standards for data completeness, accuracy, and timeliness (live data where applicable)
    b) Organize data within the centralized system into logical, flexible configurations in which individual elements and tables can be linked to each other across conformed dimensions for multiple business uses
    c) The City must have access to all tables, data sets, and schemas through modern data transmission methods including APIs that do not require Passport intervention
    d) All structured and unstructured data shall be available to the City and provided upon request in an industry standard format (e.g., doc., xls, .pdf, logs, and flat files)
    e) Entity relationship diagram(s) and data dictionaries to support development of end-user reports will be provided.

2) Provide a Presentation Layer that contains
    a) Dashboards
    b) Heat Maps and GIS Presentation
    c) Reporting assets/objects (static, standard, custom, variable)

3) Presentation Layer Functions
    a) The solution will provide capability to copy and modify existing reports and dashboards to create new reports/dashboards (Future/Roadmap)
    b) The solution will provide authorized users the ability to configure new reports and templates. (Future/Roadmap)
    c) The solution will allow a user to save a personal copy for later execution of a pre-defined report with a set of specific selection criteria
    d) The solution will provide functionality for the user to incorporate formulas, functions, and mathematical calculations into reports (Future/Roadmap)
    e) The solution will provide the ability to easily create and configure dashboards that show different analyses in visualizations that are comparable to modern data visualization programs (e.g., SAP Crystal Reports, Tableau, PowerBI, etc.) (Future/Roadmap)
    f) The solution will provide the ability to add data points and fields to a report, provide slicing and parsing abilities to isolate data points by different variables, identify trends, conduct data range analyses, etc. (Future/Roadmap)
    g) The solution will provide the ability to sort and reports by predefined data fields
    h) The solution will provide pre-defined reports that support day-to-day PMIS business functions that are automatically generated and distributed (pushed to the user) by the PMIS at a user defined time for publication
    i) The solution will provide the ability to export presentation layer assets (CSV, Excel, PDF) (Future/Roadmap)
    j) Integrations
        i) Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include:

1. Enforcement Management
2. Citation Management
3. Business Intelligence
4. Permit Management
5. Handheld Enforcement
6. Genetec LPR
7. Scofflaw for ability to alert agents of boot eligible vehicles
8. Genetec LPR equipment
9. PayByPhone and other Mobile Payment providers
10. Web/Mobile
11. Collections
12. City Cashiering System
13. Others identified during Discovery with current vendor

3. Web/Mobile

Passport will provide online and mobile service applications to service City customers that are both innovative and customer oriented. The goals are to provide streamlined service delivery for residents/customers, improve public perception through better branding, boost community engagement, meet the unique needs of the Department of Transportation & Infrastructure.

Web Mobile Components	Technology/Service Provider	Included in this BRD
Citations and Adjudication	Passport	No
Permits	Passport	Yes
Park Smart Denver (Denver.Gov)	CCD	No

Passport will provide a portal that enables account creation, application for permits (multiple types to be defined), permit renewal, permit payment, and the ability to manage wait-list positions. The interfaces must be PC, tablet, and mobile device-friendly, with support for Windows, Android, and iOS operating systems.

The City has developed the ParkSmartDenver website which serves as a landing point to service City customer parking needs; https://www.denvergov.org/Government/Departments/Parking-Division. The requested online and mobile service applications will be integrated with this landing point and other points of entry on Denver websites.

Passport's online and mobile service applications will be "private label," designed to meet the City of Denver's branding and marketing standards and shall be designed in a manner consistent with City's existing style guide. The online and mobile service applications will be hosted externally.

Passport will update content as required in a timely manner, such as changes to existing permits, waitlists new permit types for sale. The City will forward website traffic to the Passport-hosted online and mobile service applications portal using forward URL links on the City's website, and Passport's online and mobile service applications shall include links to send users back to the City of Denver website.

Passport's online and mobile service applications must be accessible on multiple browser platforms, including MS Edge, Google Chrome, Safari, and Firefox. The online and mobile service applications experience for the user shall provide device detection and content displayed according to device type, including desktop computers, laptops, mobile devices, and tablets.

Below is a list of functions that will be provided to our City Customers.

1) Account

a) Ability to create a customer account
b) Ability to access permit information associated with a customer account
c) Ability to hide Personal Identifiable Information (PII) such as customer name and address while performing an inquiry/search
d) Ability to provide reminders and alerts for account activity

2) Permit Application and Status
   a) Ability to request new permits and include supporting documentation
   b) Ability to verify eligibility for permit application submittal based on documentation supplied by the end user
   c) Ability to display the appropriate permit type based on the selection of account type (employee/resident/visitor/City official) and address
   d) Autofill and standardize address entries
   e) Ability to view the status of permit requests, including wait-list positions.
   f) Ability to purchase more than one permit in a single transaction
   g) Ability to renew existing permits
   h) Ability to modify existing permit (e.g., Vehicle or License Plate update)
   i) Ability to cancel permits (Roadmap)
   j) Ability to request placement on multiple waitlists
   k) Ability to remove names from waitlists
   l) Ability to view wait-list positions
   m) Accept payment for a waitlist position and later apply that payment to the permit (Roadmap)
   n) Ability to restrict permit application eligibility
      i) Outstanding citations or other unpaid violations
      ii) Maximum number of permits met
      iii) Other

3) Meter Bagging
   a) Ability to request a meter bag permit through responsive web application
   b) Ability to see which meters are available to be bagged by date
   c) Ability to receive email notification when meter bag has been approved

4) Payments
   a) Ability to process payments by
      i) Credit card
      ii) Debit card
      iii) Electronic check (Roadmap)
   b) Ability to process permits
   c) Ability to process payments for wait-list positions

5) FAQs and Content
   a) Provide FAQs for permit application, renewal, waitlist, and other online features.
   b) Provide inline/on-page content to guide the user experience.
   c) Vendor is expected to create a guide about the permit application, renewal, and waitlist process which must be available on the web/mobile
   d) Ability to accept redirects from Denver.gov and redirect customers back to Denver.gov upon completion of a user flow

6) Credentials
   a) Establish account credentials following City security protocols
   b) Ability for customer to request forgotten username and/or request password reset from the Customer Portal and receive support/reset instructions/links through customer authorized channels including email

7) Compliance

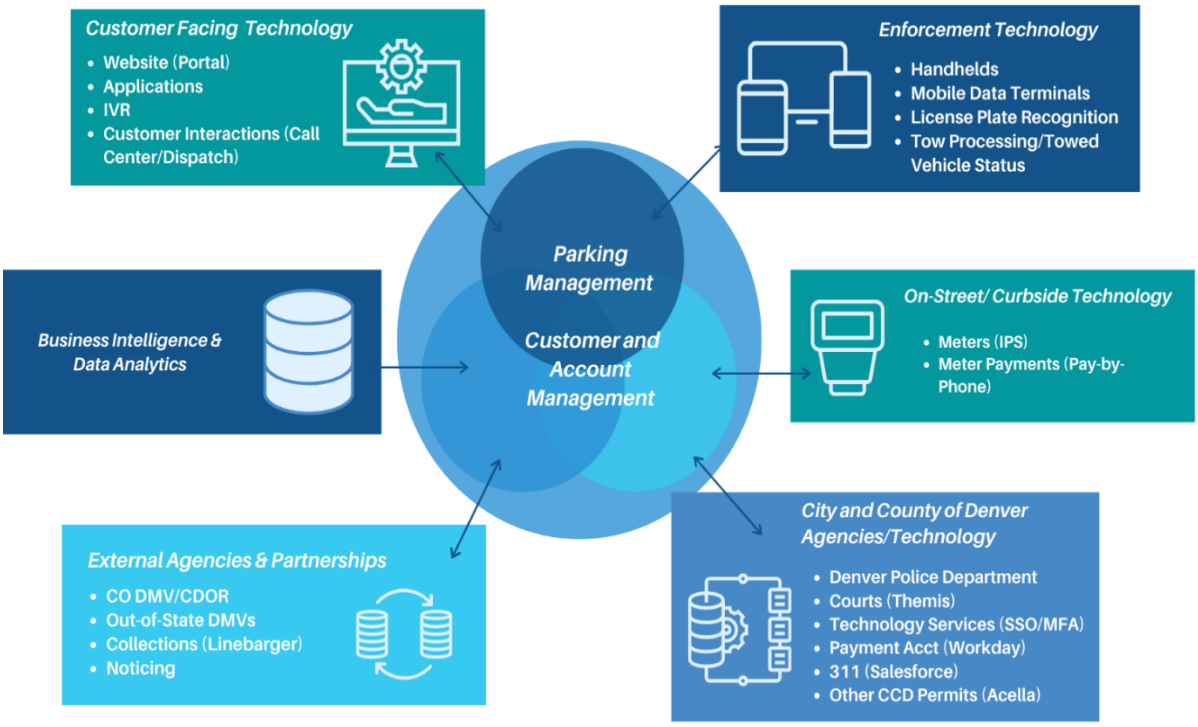
a) All Vendor managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines (collectively, "Guidelines") 3-20.

4. Integrations

The solution will require integration within the solution itself, with internal City Systems, and with third party vendors. The integrations support City functions, city policies, data consistency, and ease of operations.

Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Application architecture and number of integrations will depend upon the final solution configuration and design. The table below illustrates some of the existing integrations in our current architecture and integrations that may be required.



5. Non-Functional Requirements

The City requires a PMIS System that meets the City's Technical standards for operational maturity, information security maturity and technical compatibility. The vendor will operate a mature IT organization following best practices. Expected areas of maturity and requirements therein are described below. Vendors will be required to pass the City's Technical Security Questionnaire and present their strategy, architecture roadmap, transition strategy, architecture standards and principles to the City's Technical Architecture Review Board prior to proceeding with implementation.

1) Identity Management
   a) Ability to integrate with the City's multifactor authentication (MFA) and single sign-on (SSO) solution DUO Security. (Mandatory)
   b) Ability to comply with the City's Identity Management protocols. Internal corporate or customer (tenant) user account credentials shall be restricted ensuring appropriate identity, entitlement, and access management and in accordance with the following established policies and procedures: (Mandatory)
      i) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)
      ii) Account credential lifecycle management from instantiation through revocation
      iii) Account credential and/or identity store minimization or re-use when feasible
      iv) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)
   c) Role based security where access to data, screens, and critical functions can be limited based on roles or groups
   d) Audit logging where user activity is recorded for security and auditing

2) End-User Device Compatibility
   a) All web applications that will be accessed by the public must be compatible with current versions of Microsoft Edge and Google Chrome.
   b) Compatibility with current desktop, laptop, or tablet computing environments. Computing environment specifications and additional written responses will be required if the vendor is shortlisted.
   c) Any software that is intended to run on mobile devices should support the current release of iPhone, iPad, Android, and Window devices.

3) Usability and Accessibility
   a) Images are properly described (using alt text) and provide readable color contrast
   b) Text and images are large and/or enlargeable
   c) Headers are used in a logical order of hierarchy
   d) Link and button text are descriptive with underline and properly contrasted color
   e) Videos are closed captioned
   f) Web pages do not contain anything that flashes more than three times in any one second period
   g) Content is written in plain language and illustrated with instructional diagrams (when applicable)
   h) Documents are fully accessible and converted to PDF format for best use
   i) Use City Brand standards for white label portions of the solution. White label designs will be subject to City approval

4) Application and Interface Security
   a) Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
   b) Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
   c) Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure,

alteration, or destruction. These policies and procedures shall be in accordance with known legal, statutory, and regulatory compliance obligations.
d) All credentials required for communication with external systems shall be encrypted.
e) Ability to utilize the City's centralized system for security information and event management.

5) Interoperability and Portability
   a) The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.
   b) The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data.

6) Deployment Model
   a) Use one of the following deployment models:
      i) Cloud hosting
      ii) Managed hosting
      iii) Hybrid cloud and managed hosting

7) Policy Compliance
   a) Vendor will ensure that the PMIS solution meet all City Policies as well as Federal, State, and local laws and regulations and will attest to adherence with City Policies at the beginning of the contract and annually thereafter.
      i) Data Retention Policy
      ii) Department of Finance Cash City and County of Denver – Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds
      iii) ADA policy
      iv) Branding and UX Standards
      v) Security Policy
      vi) TS Architecture Standards
      vii) PCI/PII Compliance
      viii) Internet of Things (IOT)

8) Data Migration

The City's current Vendor, Conduent, maintains City of Denver records including but not limited to:

- Permit Records
- Payment records
- Data transformation records (business intelligence)

Passport will work with our existing PMIS vendor to migrate data to the new PMIS System in mutually agreed-upon formats. Passport will also work with City staff to migrate data fields from City and other third-party vendor systems that currently house permit related data. Passport will be responsible for defining a comprehensive data migration strategy for migrating the Permit data from existing systems to the new proposed solution. The migration strategy will identify data extraction and transformation methods, data validation and data clean-up measures and a testing plan to ensure migration quality, integrity, and completeness.

   a) Ability to provide a comprehensive migration strategy to migrate all data from existing permit systems to new solution. This includes but is not limited to eTIMs General Processing, eTIMs Workflow, Tableau, Merge, and operational spreadsheets.
   b) Ability to extract data; capture all data in scope for migration.
   c) Ability to transform data as required for input into new solution.
   d) Ability to perform data validation/data clean up on migrated and transformed data.
   e) Ability to perform comprehensive testing to ensure migration quality, integrity, and completeness.

9) Operational Hours and Availability

The City requires the PMIS components to be fully operational and available according to times specified by the City excluding maintenance or planned outages. Operational availability will be tracked and measured and subject to Service Level Agreements.

a) Ability to comply with the City's Operational Hours. The PMIS components shall be operational 24 hours per day, Monday through Sunday.
b) Maintenance to the online environment shall not be performed by the Vendor between 6:00 AM and 11:00 PM, Monday through Sunday without the express permission of the City.
c) Schedule PMIS System maintenance between the hours of 12:00AM and 4:00AM with notification to City staff one (1) week in advance.
d) 99.9% Availability for hosted/cloud services. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).
e) 99.9% Availability for software applications. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).
f) 99.9% Availability for software application integrations and interfaces. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).

10) Capacity and Performance

The City requires the PMIS components to meet capacity requirements for City use and meet benchmark performance standards to ensure operational effectiveness.

a) Minimum of 50 total and concurrent users for Permitting
b) Support 5,000 visits per day for Web and Mobile
    i) Support a minimum 1000 Permit Applications per day
c) Meet benchmark application page load under 3 seconds
d) Meet benchmark TTFB (Time-to-First-Byte) under 1.5 seconds
e) Meet benchmark TTD (Time-to-Display) for standard reports and dashboards 3 seconds
f) Meet benchmark TTD (Time-to-Display) for interactive queries 3 seconds
g) Meet benchmark TTD (Time-to-Display) for deep analytics 60 minutes

Attachment D

S2-Permit Program

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Permit Management Software Specifications - General**	**This section describes the requirements for the Permitting component of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Physical and Virtual Permits	Support both physical and virtual permit programs utilizing LPR technology	**Out-of-the-Box**	Permits Module, Customer Portal	Please see *#5. Section 2 Permit Program* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.2	Permit Length/Time	Support both annual and temporary time-limited permits	**Out-of-the-Box**	Permits Module, Customer Portal	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.3	Permit Numbers	Generate unique permit numbers i. Unique parking permit numbers per city defined criteria (including pending or pre-issued permits) such as License plate number, type of Permit code, other indicators. Permit numbers should allow both numbers and letters	**Future Release**	Manage Permits, Customer Portal	Passport can accommodate the creation of unique permit numbers based on City defined criteria via custom programming. Please also see *Process Permit Applications (Automatic or Manual)* in the Passport Labs, Inc. – Section 2 Permit Program document for additional details.
1.5	Permit Request(s)	Accommodate requests for multiple permit types	**Out-of-the-Box**	Manage Permits; Permit Settings	Please see *Accounts* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.6	Permit stock	Physical permit stock to be supplied by the Vendor, optional	**Out-of-the-Box**	Permits Module	Please see *Permits General (includes Meter Bagging permits)* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.7	Barcode/QR Code	Ability to support the printing of QR permits for temporary or regularly issued permits	**With Configuration**	Manage Permits, Customer Portal	Please see *Permits General (includes Meter Bagging permits)* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.8	Print	Ability to print permit information through template files, as necessary	**With Configuration**	Manage Permits, Customer Portal	Please see *Permits General (includes Meter Bagging permits)* as well as *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.9	Query results	Permit query results shall display in logical order including the number of accounts and number of active permits associated with accounts	**Out-of-the-Box**	Manage Permits	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.10	Rolling Expiration Dates	Support rolling expiration dates (e.g., daily, weekly, monthly, annually)	**Out-of-the-Box**	Manage Permits	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
1.11	Guest Permits	Support guest permits with physical and/or virtual permits	**Out-of-the-Box**	Manage Permits	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2	**Permit Management Software Specifications - Permit Account Management**	**This section describes the requirements for the Permitting component of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
2.1	Account integration	Web-based software solution that provides permit-related data, accessible by City staff	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *#4. Section 1 Parking Management and Enforcement* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.2	Account data	Integration of permit data in real-time	**Out-of-the-Box**	Client Portal; Customer Portal	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.3	Permit account attributes	Permit account attributes include i) Name (First, Last or Business) ii) Account Type iii) Account Number iv) Contact information (phone, email, preferred contact method) v) Address vi) Vehicle(s)/Plates(s) vii) Any additional custom data field for each permit, as defined by City	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.4	View/Edit Permit Accounts	Create, edit, or update permit record	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.

2.5	Permit Record Attributes	Ability to create permit records based on different attributes such as license plate, location, person, or company/fleet	**Out-of-the-Box**	Manage Permits, Groups	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2.6	Inactivate Permit	Inactivate permit records with optional reason code in accordance with Business Rules	**Out-of-the-Box**	Manage Permits	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2.7	Retain Data	Retain inactivated permit and account information	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2.8	Notes	Add notes to permit records	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2.9	View records	Ability to View permit customer account data and View/Add/Edit permit record data.	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
2.10	Search Accounts	Ability to search for permits by customer name, business name, license plate, permit number, address.	**Out-of-the-Box**	Manage Citations; Citation Details	Passport's system does not currently support the attachment of digital voice recordings or videos, but could link to external files using the "Add Notes" feature in the citation record. Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.11	View documentation	View files and documentation associated with a permit record (photos, voice, correspondence, etc.)	**Out-of-the-Box**	Manage Citations; Citation Details	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.12	Notes	Ability to add specialized notes to the permit record	**Out-of-the-Box**	Fleet Management	Please see *Account Management* in the Passport Labs, Inc. – Section 1 Parking Management and Enforcement document for full details.
2.13	~~Messaging~~	~~Integrated messaging and ability to send messages to other authorized users of the system~~	**~~Cannot Meet~~**	~~User Management~~	~~Passport's back-end system, Client Portal, has the ability to identify users of the system and extrapolate their email addresses from their profile to message them outside of the PMIS platform.~~
2.14	Physical letters	Send physical letters to permit holders	**Out-of-the-Box**	Letter Template Setup; Customer Portal	Passport's platform can currently identify lingering citations associated to a user's account if they have a permit associated to the citation. Additionally, the team intends to iterate to add the ability to send notifications via multiple communication methods.
2.15	Email Notifications Permits	Send emails to permit holders when account changes are made including permit application submission, permit application approval, permit payment receipt, and renewal notices.	**Out-of-the-Box**	Letter Template Setup; Customer Portal	Passport's platform can currently identify lingering citations associated to a user's account if they have a permit associated to the citation. Additionally, the team intends to iterate to add the ability to send notifications via multiple communication methods.
2.16	Email Notifications Citations	Send email to permit holder when a new citation is issued to permitted license plate number.	**Future Release**	Letter Template Setup; Customer Portal	Passport's platform can currently identify lingering citations associated to a user's account if they have a permit associated to the citation. Additionally, the team intends to iterate to add the ability to send notifications via multiple communication methods.
3	**Permit Application and Waitlists**	**This section describes the requirements for the Permitting component of the PMIS.**			
3.1	Accept Applications	Accept web/mobile applications for Permits (refer to Web/Mobile Section 4)	**Out-of-the-Box**	Customer Portal	Passport does not offer an application to purchase permits, however, the Customer Portal website is mobile-optimized to be accessed seamlessly from any mobile device. Please see *Permit Applications and Permit Waitlists* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.2	Normalize addresses	Autofill and standardize address entries, during permit application and editing of permit addresses, utilizing Denver Address Database	**Out-of-the-Box**	Customer Portal	Please see *Permit Applications and Permit Waitlists* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.3	Permit Availability	Limit permit availability based on geographical location (address validation) of requested permit or other City-determined factors in accordance with Business Rules	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.4	Permit Limits	Limit issuance of permits (i.e. Residential Parking Permits) by License Plate, Entity/Business or Person (Driver's License) in accordance with Business Rules	**Out-of-the-Box**	Customer Portal; Permit Settings	Passport can limit the issuance of permits by LPN, but not according to driver's license number. Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for additional details.
3.5	Permit Restriction	Prevent parking violators with open citations from obtaining certain permit types such as residential parking permits	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.

3.6	Meter Availability	Ability to search for meter permits based on meter ID and permit holder	**Out-of-the-Box**	Customer Portal; Permit Settings	Passport has a phased approach for implementing this functionality on its Customer Portal. Please see *Permit Applications and Permit Waitlists* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.7	Real-time Validation	Ability to manage inventory of meters and their status (Available, Pending Permit, Approved Permit, Unavailable)	**Out-of-the-Box**	Customer Portal; Permit Settings	Passport has a phased approach for implementing this functionality on its Customer Portal. Please see *Permit Applications and Permit Waitlists* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.8	Meter Bag List	Ability to see current and future meter bag requests to manage operations	**Out-of-the-Box**		
3.9	Exceptions	Support varying exception permit processes and quantity limitations by a designated period for both daytime and overnight permits	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.10	Multiple Purchase	Restrict or allow multiple permit purchases for the same plate number depending on Business Rules	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.11	Eligibility	Validate permit program eligibility based upon supporting documentation	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
3.12	Waitlists	Support waitlists, by permit type and location	**Out-of-the-Box**	Customer Portal; Permit Settings	Please see *Permit Applications and Permit Waitlists* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4	**Permit Application Processing**	**This section describes the requirements for the Permitting component of the PMIS.**			
4.1	Workflow	Establish permit processing work queues/workflow and rules for permit processing work queues/workflow including establishing different queues for different permit types and priority routing in accordance with Business Rules	**Out-of-the-Box**	Approval Queue; Permit Settings	Please see *Process Permit Applications (Automatic or Manual)* as well as *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.2	Applications	View permit applications and attached documents	**Out-of-the-Box**	Approval Queue	Please see *Process Permit Applications (Automatic or Manual)* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.3	Payments	Process payment for permits	**Out-of-the-Box**	Manage Permits; Approval Queue	Please see *Process Permit Applications (Automatic or Manual)* as well as *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.4	Multiple Permits	Process multiple permit requests in one transaction	**Out-of-the-Box**	Manage Permits; Approval Queue	Please see *Process Permit Applications (Automatic or Manual)* as well as *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.5	Edit	Edit any permit field (based upon user-assigned privileges)	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.6	Clone	Provide bulk permit purchases for group accounts	**Out-of-the-Box**	Manage Permits; Permit Details	Passport believes its Group Management functionality will accommodate this requirement. Passport will work with the City to understand the use cases for cloning permit purchases.
4.7	Refund	Refund a permit	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Process Permit Applications (Automatic or Manual)* as well as *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
4.8	Cancel	Cancel a permit	**Out-of-the-Box**	Manage Permits; Permit Details	Please see *Process Permit Applications (Automatic or Manual)* as well as *Accounts* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.

5	**Issue Notifications**	**This section describes the requirements for the Permitting component of the PMIS.**			
5.1	Automatic notices	Automatically send permit renewal notices by mail and email in accordance with Business Rules	**Out-of-the-Box**	Message Permit Holders	Please see *Issue Notifications* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
5.2	Schedule	Configure multiple notification schedules	**With Configuration**	Message Permit Holders	Please see *Issue Notifications* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
5.3	Print	Print, mail and email correspondence letters to permit holders in accordance with Business Rules	**Out-of-the-Box**	Message Permit Holders; Letter Template Setup	Please see *Issue Notifications* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
5.4	Types	Ability to support multiple notification types (mail and email)	**Out-of-the-Box**	Message Permit Holders; Letter Template Setup	Please see *Issue Notifications* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
5.5	Types	Issue permit renewal notices by batch or individually	**Out-of-the-Box**	Message Permit Holders; Letter Template Setup	Please see *Issue Notifications* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6	**Configure Permits**	**This section describes the requirements for the Permitting component of the PMIS.**			
6.1	Zones	Create/modify/delete permit zones	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.2	Permit Types	Create/modify/delete permit eligibility rules by permit type	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.3	Geographical Zone Eligibility	Create/modify/delete permit eligibility rules by geographical zones	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.4	Fee Schedule	Create/modify/delete permit fee schedules by permit type, zone, and other eligibility criteria	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.5	Variable Rate	Provide a variable rate fee structure based on permit type	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.6	Application Rules	Create/modify/delete permit application rules	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
6.7	Ongoing Configuration	Allow for ongoing configuration to meet changing City business needs, or changes to local, State, or Federal laws	**Out-of-the-Box**	Permit Settings	Please see *Configure Permits* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
7	**User Activity and Permissions**	**This section describes the requirements for the Permitting component of the PMIS.**			
7.1	Permissions	Assign permissions to access certain features based on user ID	**Out-of-the-Box**	User Management	Please see *User Activity and Permissions* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
7.2	Audit Trail	Create an audit trail for all user actions that result in a change to a	**Out-of-the-Box**	Manage Permits; Reporting	Please see *User Activity and Permissions* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
7.3	User Activity	Review all user actions that result in a change to a record within the software	**Out-of-the-Box**	Manage Permits; Reporting	Please see *User Activity and Permissions* and *Operational Reporting* in the Passport Labs, Inc. – Section 2 Permit Program document for full details.
8	**Integrations**	**This section describes the requirements for the Permitting component of the PMIS.**			
8.1	Integrations	a. Integration with City Cashiering System b. PMIS Citation Management an Account Management c. Mobile/Web d. Business Intelligence e. Accela f. Single Space and Multi Space hardware infrastructure g. Third Party Integrations for eligibility validation	**With Custom Programming**	Client Portal	Passport intends to integrate with all of the listed City systems.

S3-Reporting

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Business Intelligence - Data Layer**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.>**
1.1	Standards	Adhere to standards for data completeness, accuracy, and timeliness (live data where applicable)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.2	Centralized	Organize data within the centralized system into logical, flexible configurations in which individual elements and tables can be linked to each	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	Access	The City must have access to all tables, data sets, and schemas through modern data transmission methods including APIs that do not require	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	Structure	All structured and unstructured data shall be available to the City and provided upon request in an industry standard format (e.g., doc., xls, .pdf, logs, and flat files)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
1.3	ERD	Entity relationship diagram(s) and data dictionaries to support development of end-user reports will be provided.	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2	**Presentation Layer Components**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
2.1	Dashboards	Dashboards	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2.2	Heatmaps/GIS	Heat Maps and GIS Presentation	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
2.3	Reports	Reporting assets/objects (static, standard, custom, variable)	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3	**Presentation Layer Functions**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
3.1	Copy, Modify and Create	The solution will provide capability to copy and modify existing reports and dashboards to create new reports/dashboards	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.2	New Report configuration/build	The solution will provide authorized users the ability to configure or build new reports and templates.	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.3	Pre-defined	The solution will allow a user to save a personal copy for later execution of a pre-defined report with a set of specific selection criteria	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.4	Formulas and functions	The solution will provide functionality for the user to incorporate formulas, functions, and mathematical calculations into reports	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.5	Dashboard visualization	The solution will provide the ability to easily create and configure dashboards that show different analyses in visualizations that are comparable to modern data visualization programs (e.g., SAP Crystal Reports, Tableau, PowerBI, etc.)	**Future Release**	BI/Reporting Module	Passport is actively building out its business intelligence tools and is happy to discuss a mutually agreeable solution with the City.
3.6	Data points and analyses	The solution will provide the ability to add data points and fields to a report, provide slicing and parsing abilities to isolate data points by different variables, identify trends, conduct data range analyses, etc.	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.7	Sort and filter	The solution will provide the ability to sort and filter reports by predefined data fields	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.8	Operational reports	The solution will provide pre-defined reports that support day-to-day PMIS business functions that are automatically generated and distributed (pushed to the user) by the PMIS at a user defined time for publication	**Out-of-the-Box**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
3.9	Export	The solution will provide the ability to export presentation layer assets (CSV, Excel, PDF)	**Future Release**	BI/Reporting Module	Please see *#6. Section 3 Business Intelligence* in the Passport Labs, Inc. – Section 3 Business Intelligence documents for full details.
4	**Integrations**	**This section describes Business Intelligence, Analytics & Reporting that will be provided as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.1	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Permit Management ii) Business Intelligence iii) Handheld Enforcement iv) Genetec LPR v) Scofflaw for ability to alert agents of boot eligible vehicles vi) Genetec LPR equipment vii) PayByPhone and other Mobile Payment providers viii) Web/Mobile ix) Collections x) City Cashiering System Xi Others identified during Discovery with current vendor	**With Custom Programming**	Client Portal	Passport intends to integrate with all of the listed City systems.

S4-Web Mobile

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Web / Mobile**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**	**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Create Account	Ability to create a customer account	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
1.2	Access Permit	Ability to access permit information associated with a customer account	**Out-of-the-Box**	Customer Portal	Customers can easily access their permit information via a Customer Portal and access their citation information via a separate Customer Portal. The portal can be configured to prevent the sale of permits if there are outstanding citations on the customer's account as well as notify a permit holder if new citations are issued. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
1.4	Permit Inquiry	Ability to make permit inquiries by permit number, License Plate, meter number or account	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
1.5	PII	Ability to hide Personal Identifiable Information (PII) such as customer name and address while performing an inquiry/search	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
1.6	Notifications/Reminders/Alerts	Ability to provide reminders and alerts for account activity	**Out-of-the-Box**	Customer Portal	If the customer holds an active permit, Passport can provide notification in that permit holder's account of any newly issued citations. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for details.
2	**Permit Application and Status**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
2.1	New Permit	Ability to request new permits and include supporting documentation	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.2	Verify Eligibility	Ability to verify eligibility for permit application submittal based on documentation supplied by the end user	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.3	Permit Type	Ability to display the appropriate permit type based on the selection of account type (employee/resident/visitor/City official) and address	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.4	Address normalization	Autofill and standardize address entries	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.5	Permit Request Status	Ability to view the status of permit requests, including wait-list positions.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.6	Multiple Permits	Ability to purchase more than one permit in a single transaction	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.7	Renew Permit	Ability to renew existing permits	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.8	Modify Permit	Ability to modify existing permit (e.g., Vehicle or License Plate update)	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.9	Cancel Permit	Ability to cancel permits	**Future Release**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.10	Add to Waitlist(s)	Ability to request placement on multiple waitlists	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
2.11	Remove for Waitlist(s)	Ability to remove names from waitlists	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.12	View Waitlist(s)	Ability to view wait-list positions	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.13	Payment for Waitlist(s)	Ability to Accept payment for a waitlist position and later apply that payment to the permit	**Future Release**	Customer Portal; Permit Settings	This can be accommodated via the creation of a specific permit type (i.e. a "waitlist" permit type).
2.14	Eligibility	Ability to restrict permit application eligibility i) Outstanding citations or other unpaid violations ii) Maximum number of permits met iii) Other	**Future Release**	Customer Portal; Permit Settings	This can be accommodated via the creation of a specific permit type (i.e. a "waitlist" permit type).
3	**Meter Bagging**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
3.1	Meter Bag Application	Ability to request a meter bag permit through responsive web application	**With Custom Programming**		
3.2	Meter Bag Availability	Ability to see which meters are available to be bagged by date	**With Custom Programming**		
3.3	Meter Bag Confirmation	Ability to receive email notification when meter bag has been approved	**With Custom Programming**		
4	**Payments**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.2	Payment Types	Ability to process permit and waitlist payments by i) credit card ii) debit card	**Out-of-the-Box**	Customer Portal	Passport's Customer Portal accepts all major credit/debit cards (Visa, Mastercard, Discover, and AMEX) as well as credit-card issuer-backed debit cards (i.e. the Visa/MasterCard logo is present on the card), but does not currently accept payment via e-check. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
4.2.1	Payment Types	Ability to process permit and waitlist payments by i) Electronic Check	**Future Release**	Customer Portal	Passport's Customer Portal accepts all major credit/debit cards (Visa, Mastercard, Discover, and AMEX) as well as credit-card issuer-backed debit cards (i.e. the Visa/MasterCard logo is present on the card), but does not currently accept payment via e-check. Please also see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
4.3	Waitlist Payment	Ability to process payments for wait-list positions	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
4.4	Permit Payment	Ability to process permit payments	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
5	**FAQs and Content**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
5.1	FAQs	Provide FAQs for permit, waitlist features and other features.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
5.2	In-line and on-page content	Provide inline/on-page content to guide the user experience.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details
5.3	Guide	Vendor is expected to create a guide on how to apply for permits and waitlists which must be available on the web/mobile	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
5.4	Redirects	Ability to accept redirects from Denver.gov and redirect customers back to Denver.gov upon completion of a user flow	**With Configuration**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
6	**Credentials**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
6.1	Credentials	Establish account credentials following City security protocols	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for additional details.
6.2	Username and password reset	Ability for customer to request forgotten username and/or request password reset from the Customer Portal and receive support/reset instructions/links through customer authorized channels including email	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
7	**Compliance**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
7.1	Compliance	All Contractor managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines (collectively, "Guidelines") 3-20.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
8	**Integrations**	**This section describes Web Mobile requirements that are required as part of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
8.1	Integrations	Integrate with existing City systems and vendor applications. Integrations needed will depend upon the final solution architecture and configuration and may include: i) Permit Management ii) Business Intelligence iii) City Cashiering System	**With Configuration**	Customer Portal	Passport intends to integrate with all of the listed City systems.

All Sections - Non-funtional Requirements

ID	Requirement Name	Requirement Description	Requirement Compliance	Product/Module	Vendor Response Comments
1	**Identity Management and Security**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**		**<Please use this space to note what product/module of the solution is required to address the requirement.>**	**<Please use this space to expand on your response and/or reference supporting documentation (e.g. file attachments, online information, etc.) on how your solution meets the requirement.> <Note: If your solution only partially meets the requirement, please indicate clearly and specifically the elements of the requirement it does not meet.>**
1.1	Identity Management	Ability to integrate with the City's multifactor authentication (MFA) and single sign-on (SSO) solution DUO Security.	**With Custom Programming**	N/A	**This is a mandatory requirement.** Passport does not support single-sign-on capability in its system. Passport does employ 2FA within its back-end system via Google Authenticator. After inputting their user ID/password credentials, users must enter a 6-digit validation code that is generated from the Google Authenticator app in order to log in.
1.2	Credentials	Ability to comply with the City's Identity Management protocols. Internal corporate or customer (tenant) user account credentials shall be restricted ensuring appropriate identity, entitlement, and access management and in accordance with the following established policies and procedures: a) Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) b) Account credential lifecycle management from instantiation through revocation c) Account credential and/or identity store minimization or re-use when feasible d) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)	**With Custom Programming**	N/A	**This is a mandatory requirement.** Passport is unable to comply with management protocols listed here such as single-sign-on. As stated in 1.1, Passport does employ the use of multi-factor authentication via Google Authenticator in order to access the system.
1.3	Role-Based Security	Role based security where access to data, screens, and critical functions can be limited based on roles or groups	**Out-of-the-Box**	User Management	Please see *User Activity and Permissions* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
1.4	Audit Logging	Audit logging where user activity is recorded for security and auditing	**Out-of-the-Box**	User Management; Reporting	Please see *User Activity and Permissions* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
2	**End User and Device Compatibility**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
2.1	Web Browsers	All web applications that will be accessed by the public must be compatible with current versions of Microsoft Edge and Google Chrome.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.2	Computing Environment	Compatibility with current desktop, laptop or tablet computing environments. Computing environment specifications and additional written responses will be required if the vendor is shortlisted.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
2.3	Mobile Devices	Any software that is intended to run on mobile devices should support the current release of iPhone, iPad, Android and Windows Phone.	**Out-of-the-Box**	Customer Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3	**Usability and Accessibility**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
3.1	Image Alt text and Color Contrast	Images are properly described (using alt text) and provide readable color contrast	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.2	Image enlargement	Text and images are large and/or enlargeable	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.3	Logical order	Headers are used in a logical order of hierarchy	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.4	Contact and Contrast	Link and button text are descriptive with underline and properly contrasted color	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.5	Video	Videos are closed captioned	**Future Release**	N/A	While Passport plans to build out video functionality in its system, the availability of closed captioning on those videos has not yet been determined.
3.6	Web Flash	Web pages do not contain anything that flashes more than three times in any one second period	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.7	Content	Content is written in plain language and illustrated with instructional diagrams (when applicable)	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.8	Document accessibility	Documents are fully accessible and converted to PDF format for best use	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.
3.9	White Label	Use City Brand standards for white label portions of the solution. White label designs will be subject to City approval	**Out-of-the-Box**	Customer Portal; Client Portal	Please see *#7. Section 4 Web/Mobile* in the Passport Labs, Inc. – Section 4 Web/Mobile documents for full details.

3.10	**Application and Interface Security**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
3.11	Application Security	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements - Connectivity* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
3.12	Data Integrity	Data input and output integrity routines (i.e. reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
3.13	Data Integrity and Security	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration or destruction. These policies and procedures shall be in accordance with known legal, statutory and regulatory compliance obligations.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
3.14	Connections to External Systems	All credentials required for communication with external systems shall be encrypted.	**Out-of-the-Box**	Client Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
3.15	System and Application logging	Ability to utilize the City's centralized system for security information and event management.	**Cannot Meet**	Client Portal	Passport would need more information on what the City is looking for in order to scope and commit to this requirement. Passport welcomes discussions to better understand the City's intention and use case(s).
4	**Interoperability**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**	**VENDOR RESPONSE REQUIRED**		
4.1	APIs	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements - Connectivity* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
4.2	Standardized Network Protocols	The provider shall use secure (e.g. non-clear text and authenticated) standardized network protocols for the import and export of data.	**Out-of-the-Box**	Client Portal; Developer Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
5	**Deployment Model**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
5.1	Hosted or Hybrid Model	a) Use one of the following deployment models: i) Cloud hosting ii) Managed hosting iii) Hybrid cloud and managed hosting	**Out-of-the-Box**	Client Portal	Please see *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
6	**Policy Compliance**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
6.1	Policies	Vendor will ensure that the PMIS solution meet all City Policies as well as Federal, State, and local laws and regulations and will attest to adherence with City Policies at the beginning of the contract and annually thereafter. i. Data Retention Policy ii. Department of Finance Cash City and County of Denver – Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds iii. ADA policy iv. Branding and UX Standards v. Security Policy vi. TS Architecture Standards vii. PCI/PII Compliance viii. Internet of Things (IOT)	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.

7	**Data Migration**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
7.1	Migration Strategy	Ability to provide a comprehensive migration strategy to migrate all data from existing permit, citation and issuance/enforcement, boot &, customer contact, and collections systems to new solution. This includes but is not limited to eTIMs General Processing, eTIMs Workflow, ReportWeb, City Sight Enforcement, Tableau, Merge, Scofflaw and operational spreadsheets.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.2	Extract data	Ability to extract data; capture all data in scope for migration.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.3	Transform data	Ability to transform data as required for input into new solution.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.4	Data Validation	Ability to perform data validation/data clean up on migrated and transformed data.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
7.5	Data Testing	Ability to perform comprehensive testing to ensure migration quality, integrity and completeness.	**Out-of-the-Box**	Implementation	Please see *#2. Vendor Project Approach* as well as *#9. Integrations and Non-Functional Requirements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8	**Operational Service Level Agreements**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
8.1	Operational Hours	Ability to comply with the City's Operational Hours. The PMIS components shall be operational 24 hours per day, Monday through Sunday.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.2	Maintenance Window	Maintenance to the online environment shall not be performed by the Vendor between 6:00 AM and 11:00 PM, Monday through Sunday without the express permission of the City.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.3	Maintenance Window	Schedule PMIS System maintenance between the hours of 12:00AM and 4:00AM with notification to City staff one (1) week in advance.	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.4	Hosted/Cloud Availability %	99.9% Availability for hosted/cloud services. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.5	Application Availability %	99.9% Availability for software applications. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
8.6	Integration/Interface Availability %	99.9% Availability for software applications. Availability that does not meet this standards will be subject to penalties that will be defined in the Statement of Work (SOW).	**Out-of-the-Box**	SLA	Please see *#14. Service Level Agreements* in the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document for full details.
9	**Capacity**	**This section describes the technical/non-functional requirements required for all systems and components of the PMIS.**			
9.3	Number of Users Permitting	Minimum of 50 total and concurrent users.	**Out-of-the-Box**	Client Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document.
9.6	Web Mobile - Number of Visits City Customers	Ability to support 5,000 visits per day.	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.9	Web Mobile - Number of Visits City Customers	Support a minimum 1000 Permit Applications per day	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.10	Web Mobile - Number of Visits City Customers	Meet benchmark application page load under 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.11	Web Mobile - Number of Visits City Customers	Meet benchmark TTFB (Time-to-First-Byte) under 1.5 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.12	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for standard reports and dashboards 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.13	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for interactive queries 3 seconds	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.
9.14	Web Mobile - Number of Visits City Customers	Meet benchmark TTD (Time-to-Display) for deep analytics 60 minutes	**Out-of-the-Box**	Customer Portal	Please see Passport's responses throughout the *Passport Labs, Inc. – Section 2 Permit Program* document and the *Passport Labs, Inc. – Section 1 Parking Management and Enforcement* document as well as *#7. Section 4 Web/Mobile* in the *Passport Labs, Inc. – Section 4 Web/Mobile* documents for full details.

Prioritization Type	Prioritization Description
Must Have	Requirements labeled as "Must Have" are critical to the current delivery timebox in order for it to be a success. If even one "Must Have" requirement is not included, the project delivery should be considered a failure (note: requirements can be downgraded from "Must Have", by agreement with all relevant stakeholders; for example, when new requirements are deemed more important).
Should Have	Requirements labeled as "Should Have" are important but not necessary for delivery in the current delivery timebox. While "Should Have" requirements can be as important as "Must Have", they are often not as time-critical or there may be another way to satisfy the requirement, so that it can be held back until a future delivery timebox.
Could Have	Requirements labeled as "Could Have" are desirable but not necessary, and could improve user experience or customer satisfaction for little development cost. These will typically be included if time and resources permit.
Won't Have	Requirements labeled as "Won't Have" have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time. As a result, "Won't Have" requirements are not planned into the schedule for the next delivery timebox. "Won't Have" requirements are either dropped or reconsidered for inclusion in a later timebox. (Note: occasionally the term Would like to have is used; however, that usage is incorrect, as this last priority is clearly stating something is outside the scope of delivery).

Parking Management Information System

Pricing

As compensation during the Term of the Agreement and for providing the entirety of the programs, equipment, software, implementations, and all related processes, services and staff outlined within this Scope of Work, unless otherwise noted within, the City agrees to pay and Passport agrees to accept, as full compensation, the following fee schedule, and descriptions.

Fee Schedule	
Parking Management and Enforcement Program	
Citation Processing Fee per citation	$3.27
Manual Citation Entry Fee per citation	$0.33
Notice Fee per notice	$0.24
AutoVu Managed Service 2.0 Fee per patroller annually	$497.20
Genetec Patroller and AutoVu Extended Warranty per patroller annually	$1,734.20
Implementation cost – One-time fee	$90,000.00
Professional Services	
Call Center Fee per month	$42,242
Interactive Voice Response (IVR) per month	$5,072
Lockbox Processing per payment processed	$5
Implementation cost – One-time fee	$15,000.00
Permit Program	
Permit Program Fee per month	$27,916.66
Custom Development	
Solution Team per hour	$250.00

Parking Management & Enforcement Fees and Costs

1. A Citation Processing Fee of $3.27 per citation issued via the system.
    a. This fee includes:
        i. DMV inquiries in state and out of state, where applicable
        ii. Training
        iii. Technical support
        iv. Continuous Improvement tasks
        v. Upgrades and Maintenance where applicable, including Handheld devices
        vi. Software licenses, warranties and/or cloud hosting for all applications provided
        vii. Ticket stock for citations issued via the handheld devices.
    b. This fee excludes (not chargeable):
        i. Citations issued in error or otherwise cancelled by the City.
        ii. Warnings issued by the City

2. A Manual Citation Entry Fee of $0.33 per citation entered manually into the system by Passport or its subcontractors. There shall be no charge for use of the Manual Citation Entry feature by the City or its subcontractors.
3. A Notice Fee of $0.24 for system generated notices.
    a. This fee covers all mailed out communications generated through the system.
    b. Postage is excluded from this fee.
4. An AutoVu Managed Service 2.0 Fee of $497.20 per Patroller Connection
    a. This fee includes:
        i. Subscription Fee for AutoVu Managed Service 2.0
        ii. AutoVu Service Upgrade to Pay-by-Plate Multi
        iii. The per unit cost is based on 31 units. If a smaller number of units are implemented, a quote may be recalculated for a lower quantity implementation.
    b. This fee excludes:
        i. Mobile License Plate Reader (LPR) devices and peripherals
        ii. Mobile License Plate Reader (LPR) warranty, return or repair
        iii. Activated SIM cards or data plans for LPR
5. A Genetec Patroller and AutoVu Vehicle Hardware Extended Warranty Fee of $1,734.20 per unit where applicable.
    a. This fee includes:
        i. Return and Repair coverage
        ii. AutoVu vehicle hardware and Genetec Patroller software upgrades
6. Hardware and Operational Equipment
    a. At the direction of the City, Passport may procure hardware and equipment. Hardware and equipment orders that have been approved by the City may be fully reimbursable to Passport including shipping costs.
    b. Passport's hardware and equipment offerings are provided through Passport's e-commerce website store.passportinc.com.
    c. The e-commerce store will be used to place, manage, and track orders.
    d. The City and Passport will review replacement of devices prior to end of their life and develop replacement plans, as needed.
    e. City is responsible for any extended handheld device warranty or repair costs outside of the manufacturer's warranty.
    f. Nothing in this Agreement shall affect, supersede, or modify any duly promulgated or enacted fee or changes of the Denver County Court or its Bureaus in any way affecting Parking Citations.
7. Data plans for all devices will be provided by the City.

Professional Services

1. A Customer Contact Center fee of $42,242 per month

a. Included in this fee
    i. Talk Time minutes on an ASA of 60 seconds. Talk Time minutes are defined as the amount of time a customer contact agent talks to a customer during an interaction as measured by the automatic call distributor (ACD).
2. Lockbox Processing fee of $5 per payment processed
3. IVR setup, administration, and maintenance fee of $5,072 per month

Permit Program

1. A monthly **Fee of $27,916.66**.
    a. This fee includes:
        i. Access to Passport's Permit Program SaaS platform
        ii. Permit Program Mobile/Web platform
        iii. Training
        iv. Technical support
        v. Continuous Improvement tasks
        vi. Upgrades and Maintenance where applicable

Custom features or integrations

i. A Solution Team fee of $250.00 per hour will apply for additional custom development or integrations during the contract. This fee applies if the City's requested feature or functionality for the City's sole use, are not identified in the Statement of Work and are not incorporated into the core software product. This fee is inclusive of all team members.

Additional Resource Fees	
Solution Team including Product Manager, Full Stack Engineers and others as assigned.	$250.00 per hour for entire team

ii. Passport will assign resources according to the needs and complexity of the customization or integration.
iii. Passport agrees to maintain the most cost-effective team structure for the customization or integration.

Attachment F

Service Level Agreements (SLA)

Service Level Agreements

Service Level Agreements will be utilized to monitor compliance with stated performance levels and to provide the City with remedies in the event Passport does not meet stated levels. Described herein are the minimum levels of service including a description, minimum requirement, measurement, and remedy for:

1. Service Availability
2. Feature and Function Availability
3. Call Center Performance
4. Solution Delivery Effectiveness
5. Continuous Improvement and Annual Policy Compliance

1. Service Availability

Description: The Vendor shall provide a stable and reliable solution for the City to operate its Parking and Permit programs. Service availability guarantee includes uptime percentage and timely response to reported incidents based on service level. Uptime is the percentage of time that an application, technical, or hosting service is online, available, and operational. Availability is the ability of the user to obtain a service or access a site, platform, or application.

Minimum Requirement: The Service Availability for uptime percentage is ninety-nine point nine 99.9% per month (IP connectivity, web server availability, database availability excluding maintenance windows for system maintenance and excluding other planned System Outages.

Measurement: The Service Availability requirement for uptime will be calculated monthly, and calculations will be reported on a schedule determined by the City. The Service Availability uptime percentage will be calculated for each day (24 hrs.) and broken down to a by-minute formula.

Uptime Percentage = ((Agreed Service Time (AST) – Downtime (DT))/Agreed Service Time (AST))*100

Where:

1. Agreed Service Time AST is the total number minutes in the current month.
2. Downtime is any time that part or all of the system is not available to the city or their customers.
3. Planned downtime will be requested no less that 21 days before in writing and will not exceed a 4 hour window. Planned downtime will not be factored into the uptime percentage.

Attachment F

Monitoring: Passport will monitor all levels of the service infrastructure and application. Passport will automate warnings and alerts for deviations in the environment from established thresholds. All alerts and warning will be available to the city.

Remedy: In the event that the Vendor does not meet the stated Service Availability requirement for uptime percentage, a reduction of the total invoiced amount shall be applied.

The service credit shall be based on a calculation of the average revenue per minute per year (minute revenue loss). The calculation consists of the average yearly value for functional area and minutes in a year.

Functional Area	**Yearly Value**
Citation Issuance & Management	Average yearly value of citations issued in the previous three fiscal years
Permit Issuance & Management	Average yearly value of permits issued in the previous three fiscal years
New rates for each functional area will be calculated at the beginning of the new fiscal year and the City will notify the Vendor of the new rates to be applied in a credit event. The areas itemized above for Remedy Calculations, Citation and Permitting, may be refined or subject to change based upon the final solution proposed and architecture implemented	

Example calculation:

Yearly Value for Functional Area	= $_____
Divided by hours in a year	= 8760
Divided by minutes	= 60
Total	= $_____

The resulting credit will be applied as a reduction of the total invoiced amount, for citation processing or permit processing respectively for the month in which the SLA has not been met. The credit calculation shall be submitted to the City on a schedule determined by the City.

Communication and Response Time for Outages:
All outages and service unavailability incidents will be treated with Emergency or High priority. Communication regarding the monitoring, root cause and action plans for resolution of the outage will be timely and frequent, following an agreed Incident Communication Process.

Service Level	**Service Response Time**	**Communication Update Frequency**
Emergency	Less than 15 min	Every 30 minutes
High	1 hour	Every 2 hours

Service Response Time refers to the maximum elapsed time after a problem is identified by system monitoring protocols or, if unmonitored, logged for investigation and action by Passport. Passport

will communicate with the City's CPM and support team within the determined timeframe with a resolution plan.

Communication Update Frequency refers to the maximum elapsed time after a problem is identified by system monitoring protocols or, if unmonitored, logged for investigation before a status update is provided to the City. Passport will provide status updates to the City's CPM and support team within this frequency interval until the problem is resolved.

Planned System Outages: The Vendor will coordinate with the City on maintenance, upgrades and patches that may affect system uptime. The Vendor will schedule such outages at times of low system utilization. The Vendor will work to continually limit planned outages. All planned outages, regardless of duration, will require 21-day written notification to the City and be approved by the City Contract Manager. Emergency maintenance upgrades and patches will be coordinated on a case-by-case basis and be considered unplanned downtime

2. Feature and Function Availability

Description: The Vendor shall provide a stable and reliable solution for the City to operate its Parking and Permit programs. Feature and Functions Availability is the ability of City customers and internal users to successfully execute key functions that are categorized as Critical or Highly important for customer service or operational effectiveness.

Minimum Requirement: The Feature and Function Availability requirement is resolution of any reported and confirmed issue within 4 hrs., 24 hrs., 5 days, or 20 days based on the classification of the feature and severity of the issue.

Severity Classification	Service Resolution Goal
Emergency	Less than 4 hours
High	Within 24 hours
Medium	Within 5 business days
Low	Within 20 business days

Severity Classification

Severity Classification	Description
Emergency	Service is unavailable, a substantial subset of functionality, or Critical functionality is unavailable without a workaround. This includes security breaches or other security issues.
High	Service is experiencing intermittent issues or unavailability, or system is experiencing severe performance degradation. A substantial subset of functionality or Critical functionality is unavailable. A workaround exists but may be cumbersome to sustain.
Medium	Service is experiencing moderate performance degradation. A subset of functionality, Critical functionality or Important functionality is unavailable. A workaround exists but can only be sustained for a short period without significantly impacting workflow efficiencies.

Low	Service is experiencing minor performance degradation. Some functionality is unavailable or requires enhancement or configuration update. A workaround exists.

Feature Classification Example: Features and Functions will be classified during the Analysis and Design phase of the initial implementation. System upgrades, enhancements or City policy changes may also necessitate that feature classifications be updated.

Example Classification Table		
Area	**Feature Description**	**Classification**
Citation Issuance & Management	Time Marking	Critical
	Send Notifications	Critical
	Edit Citation Notes	Medium
	Vehicle Location Tracking	Important
Permit Issuance & Management	Review Applications	Critical
	Accept and Process Payment	Critical
	Delete Application	Medium

Measurement: Feature and Functions Availability will be measured as total time for resolution in hours or days, depending upon severity for each incident reported. Calculation will start at time of functional unavailability as logged for investigation by the City in agreed upon Incident Report system. Calculation will end when technical resolution acceptance is recorded in the agreed upon Incident Report system.

Remedy: In the event that the Vendor does not meet the stated Feature and Functions Availability requirement a reduction of 2% of the total monthly invoice amount per outage day shall be applied. Partial days will be calculated accordingly.

The service credit shall be based on the total monthly invoice amount.
Example calculation:

Monthly Invoice	=$ 10,000
Days Credit	= 2
Percentage of Invoice	= .02
Credit Total	= $400

The resulting credit will be applied as a reduction of the total invoiced amount, for citation processing or permit processing respectively for the month in which the SLA has not been met. The credit calculation shall be submitted to the City on a schedule determined by the City.

Communication and Response Time for Outages: All disruptions in the executions of and functions and inaccessibility of features will be responded to in accordance with the schedule below. Communication regarding the monitoring, root cause and action plans for resolution of the outage will be timely and frequent, following an agreed Incident Communication Process.

Service Level	Service Initial Response Time	Communication Update Frequency
Emergency	Less than 15 min	Every 30 minutes
High	1 hour	Every 2 hours
Medium	2 hours	Every 24 hours
Low	8 hours	Every 5 business days

Service Response Time refers to the maximum elapsed time after a problem is identified by system monitoring protocols or, if unmonitored, logged for investigation and action by Passport. Passport will communicate with the City's CPM and support team within the determined timeframe with a resolution plan.

Communication Update Frequency refers to the maximum elapsed time after a problem is identified by system monitoring protocols or, if unmonitored, logged for investigation before a status update is provided to the City. Passport will provide status updates to the City's CPM and support team within this frequency interval until the problem is resolved.

3. Call Center Performance

Description: The Vendor shall provide efficient, productive, and effective Call Center services. Call Center Performance includes how quickly and effectively City customers are served.

Minimum Requirement: The Call Center Performance requirements are (1) an Average Speed to Answer (ASA) of sixty (60) seconds or less and (2) a Call Abandonment Rate (CAR) of no more than 5% after sixty (60) seconds.

Measurement: The Call Center Performance requirement for Average Speed to Answer (ASA) is measured as the total wait time that callers are in queue, divided by the number live voice calls handled excluding abandoned calls each week. The Call Center Performance requirement for Call Abandonment Rate (CAR) is measured by number of abandoned calls divided by the total number of calls handled (live and IVR) each week.

Remedy: In the event that the Vendor does not meet the stated Call Center Performance requirement during any week in a given month either (1) a remediation plan will be required or (2) a reduction of the total invoiced amount shall be applied.

Classification	**Remedy**
First Missed Goal in Year	Remediation Plan
Second or Subsequent Missed Goal in Year	Credit for each missed Goal in the amount of 2% per day of monthly invoice

4. Solution Delivery Effectiveness

Description: The Vendor shall the solution as specified in this Agreement, meeting all specified functional and nonfunctional requirements in a timely manner and according to quality standards.

Minimum Requirement: The Service Delivery Effectiveness requirement is that the Solution delivered and accepted will meet 97% of stated Functional and Nonfunctional Requirements in the

agreed upon Design delivered no more than 10% beyond the established Delivery and Acceptance timeline. This requirement will apply to the Initial Service Delivery and any subsequent enhancements.

Measurement: The Service Delivery Effectiveness requirement measuring the percentage of Functional and Nonfunctional requirements delivered will be calculated as the number of delivered requirements divided by the total number of requirements. Timeline overage tolerance will be calculated as Total Number of Days in Timeline multiplied by 0.10.

Remedy: In the event that the Vendor does not meet the stated Service Delivery requirement the Vendor will be responsible for paying the City penalties against future or current monthly charges billed by the Vendor equal to ($1,000.00) per day of delay as fixed and agreed penalty, for each Day or fraction of a Day said deliverable later than set forth above.

5. Continuous Improvement and Policy Compliance

Description: The Vendor shall meet or exceed the City expectations for Continuous Improvement as outlined above in M09 -Support, Maintenance, and Continuous Improvement.

Minimum Requirement: The Continuous Improvement requirement is to deliver 100% of the required documentation on or before the established timelines as stated in M09 - Support, Maintenance, and Continuous Improvement .

Measurement: The Continuous Improvement is measured on the date each required document is accepted.

Remedy: In the event that the Vendor does not meet the stated Continuous Improvement requirement the Vendor will be responsible for paying the City penalties against future or current monthly charges billed by the Vendor equal to ($1,000.00) per day of delay as fixed and agreed penalty, for each Day or fraction of a Day said deliverable later than set forth above.

Architecture Standards

April 2020

Our Mission

To improve city performance.

Our Vision

Denver departments deliver exceptional services.

Table of Contents

Purpose

This document provides the City and County of Denver (CCD) a framework to mature governance effectiveness and improve service delivery through architecture standards. It supports Executive Order No. 18 and Technology Services (TS) with delivering technology services across the City government.

This document should be used by CCD to evaluate how newly proposed solutions align to our standards. It could also be used to evaluate standards alignment within the current service portfolio. Any proposed solution not able to meet active standards could be disqualified from consideration, however, a technology exception waiver can be applied for and granted by TS as a term and condition of the contract.

All listed standards represent the CCD supported configurations for current and future environments (~6 months). They represent the active standard. In some cases, a deprecated standard will be identified. Standards do not generally exist for all time, they adapt as new innovations enter the market. New standards are identified and managed through a lifecycle process. Therefore, this document is maintained by the TS technical architecture review board and reviewed/updated biannually.

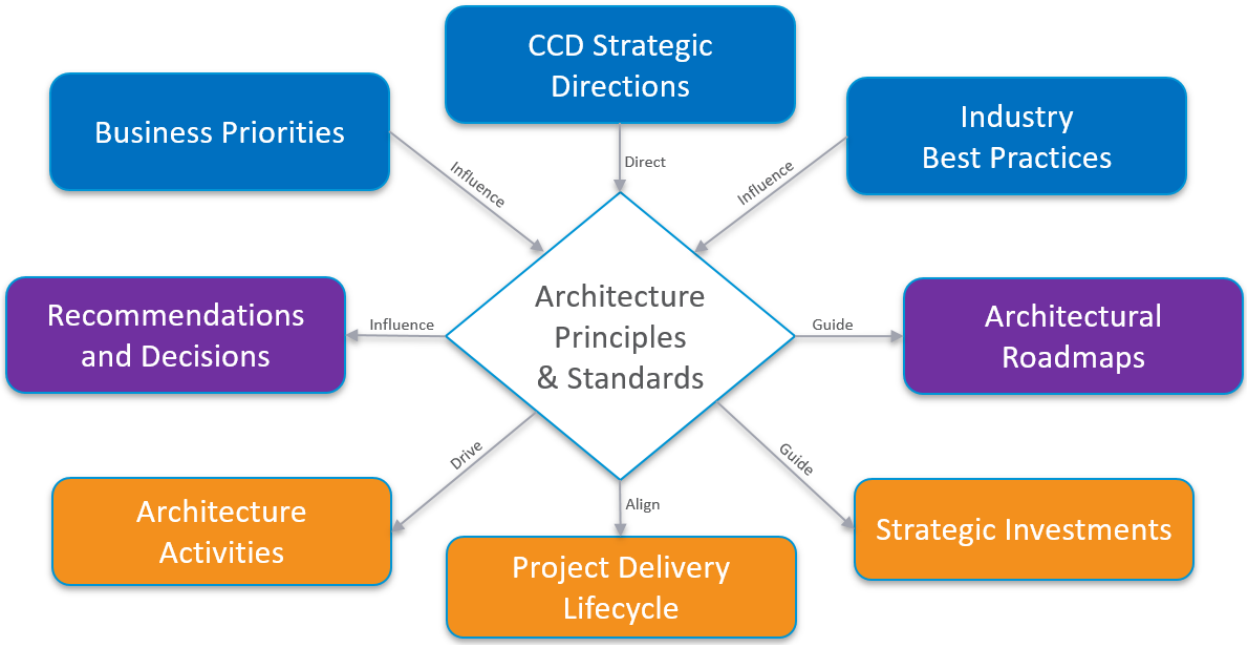


Figure 1: Architecture Principles & Standards Reference Model

Section I: End User Devices

1-CCD-01 Desktop, Workstation and Laptop Hardware

The following specifications are based on the City's existing systems and represent the expected maximum hardware specification for a given class of hardware. These specifications serve as a reference for current and future hardware environment states.

Hardware Class	Basic PC	Advanced PC	Workstation PC	Standard Laptop	Ultrabook	Workstation Laptop	Tablet
Intel Core i5-9500, 4.4 GHz	●						
Intel Core i7-9700, 4.7 GHz		●					
Intel Core I7-9700, 8 Core,4.7 GHz			●				
Intel Core i5-8265U, 4 Core, 1.6 GHz				●			
Intel Core i7-8665U, 4 Core, 1.9 GHz					●		
Intel Core i7-9850, 6 Core, 4.6 GHz						●	
Intel Core i5-7300U, 2.6 GHz							●
Intel Core i5-8350U Quad-Core, 1.7 GHz							●
RAM (GB)	8	8/16	16/32	8/16	8/16	16/32	8/16
NVIDIA GeForce GT 730, 2GB	●						
AMD Radeon RX 550, 4GB		●					
AMD Radeon RX 5500, 4GB			●				
Intel HD Graphics 620, Integrated, 300 MHz				●	●		●
Intel UHD Graphics 620, Integrated, 300 MHz							●
NVIDIA Quadro T1000, 4GB						●	

1-CCD-02 Device Software

The City and County of Denver installs and maintains a standard set of software on all desktops and laptops. All software that is acquired by the City and County of Denver must be compatible with the expected environment.

Type	Name	Requirement
Operating System	Microsoft Windows (preferred)	Windows 10 Enterprise Version 1909 and above
	Apple macOS	Current Release
Browser	Edge	Current Release
	Google Chrome	Current Release
User Productivity & Collaboration	Microsoft Office 365 ProPlus (Word, Excel, PowerPoint, Outlook, Teams)	Current Release
Software Framework	Microsoft .NET	Current Release
Java	Oracle JRE (deprecated)	Java SE 8u201
PDF Reader	Adobe Acrobat Reader DC	Current Release
Multimedia Framework	HTML 5	Current Release
Hard Drive Encryption	Microsoft BitLocker	Current Release
Secure VPN	Cisco AnyConnect	Current Release

1-CCD-03 Mobile Devices

The City and County of Denver supports the following mobile devices. Any software that is intended to run on mobile devices should support the following specifications.

Type	Name	Requirement
Smartphone	iPhone	Current Release
	Android	Current Release
Tablet Computer	iPad	Current Release
	Surface Pro	Current Release

1-CCD-04 Special Purpose Devices

The following specifications represent the expected maximum hardware specification for that class of hardware.

Mobile Compute/Device Terminal (MCT/MDT) Tablets

NOTE: Applies to Denver Police, Sheriff, Fire, and Animal Protection departments. Docking stations and mounting hardware are required for all mobile installations.

Hardware Class	Requirement
Processor/Memory	Intel Core i7-8665U 16GB RAM
Storage	256GB M.2 SED
Display	13.3" FHD Touchscreen, Anti-Glare, Backlighting
Interface	Touchscreen, Stylus Pen, Keyboard
Wireless	WLAN 802.11ac/a/b/g/n Bluetooth v5 LTE wireless broadband
Durability	MIL-STD-810G/IP65
Warranty	1 Year Extended Service

Rugged Laptop

NOTE: Applies to Denver Fire Department

Hardware Class	Requirement
Processor/Memory	Intel Core i5-7300U 16GB RAM
Display	13.3" Display
Durability	MIL-STD-810G/IP65

Section II: Infrastructure

2-CCD-01 Communications (Networks, Voice, Video)

NOTE: Available by Consultation

2-CCD-02 Compute

Type	Name	Requirement
Server Hardware	Cisco	UCS

2-CCD-03 Virtualization

Type	Name	Requirement
Platform	VMWare	ESX 6.7
Client	VSphere client	6.7
Platform	Oracle VM (deprecated)	Current Release

2-CCD-04 Server Operating System

Type	Name	Requirement
Microsoft	Windows Server	2016 Standard or Current Release
Linux	Red Hat	7 or Current Release

2-CCD-05 Storage

Type	Name	API or Protocol
Object Storage (Preferred)	Hitachi Content Platform (HCP) Storage-as-a-Service	• HCP REST (Hitachi REST API) • HCP HS3 (Amazon S3 compatible REST API) • HSwift (OpenStack Swift compatible REST API) • MAPI (HCP Management API) • Metadata Query API
File Storage	HCP Gateway	• NFS • SMB and CIFS
Block Storage	Pure Storage	• 16/32Gbps Fiber Channel • 25/50Gbps NVMe/RoCE
Archive Storage	Amazon S3 Glacier or Amazon S3 Glacier Deep Archive	• Amazon S3 REST API

2-CCD-06 End User Device Management

Type	Name	Requirement
Endpoint Configuration	Microsoft System Center Configuration Manager	2012 R2 1803
Endpoint Management	IBM BigFix	9.5
Vulnerability Management	Qualys Cloud Agent	Current Release
Privilege Management	BeyondTrust PowerBroker for Windows	Current Release
Endpoint Protection (Antivirus) & Response	Crowdstrike Client	Current Release
Multi-factor Authentication (MFA)	Cisco Duo Agent	Current Release

Section III: Infrastructure Services

3-CCD-01 Enterprise Application Control

Type	Name	Requirement
Application Delivery Network	F5 BIG-IP	12

3-CDD-02 Domain Services (DNS, DHCP, Directory Services)

Type	Name	Requirement
DNS	Infoblox DDI	RFC Compliant DNS
DHCP	Infoblox DDI	RFC Compliant DHCP (Dynamically allocated IP address only. Fixed IPs by DHCP.)
Directory Services	Microsoft Active Directory	DENVERCO.GOV DFL & FFL: Windows Server 2016 DNVR FFL & GOV/SFTY DFL: Windows Server 2012 R2 FFL=Forest Functional Level DFL=Domain Functional Level

3-CCD-03 Identity Management

Type	Name	Requirement
Identity Management	SailPoint IdentityIQ	Current Release
	Oracle OIM (deprecated)	11g R2 PS3
Access Management	Oracle OAM (deprecated)	Current Release & SAML 2.0 Compliant
Multi-factor Authentication (MFA)	Cisco Duo	Current Release

3-CCD-04 Data Center & Infrastructure

Name	Requirement
Generic Telecommunication Cabling for Customer Premise	TIA-568.0-E
Commercial Building Telecommunications Cabling Standard	TIA-568.1-E
Balanced Twisted-Pair Telecommunications Cabling and Components Standard	TIA-568.2-D
Optical Fiber Cabling and Components Standard	TIA-568.3-D
Broadband Coaxial Cabling and Components Standard	TIA-568.4-D
Administration Standard for Telecommunication Infrastructure	TIA-606-B
General Telecommunication Bonding and Grounding for Customer Premises	TIA-607-C
Customer-Owned Outside Plant Telecommunications Infrastructure Standard	TIA-758
Structured Cabling Infrastructure Standard for Intelligent Building Systems	TIA-862-B
Telecommunication Infrastructure for Data Centers	TIA-942-A

3-CCD-05 Event Management

Type	Name	Requirement
Network Management	Op5	Current Release
	SolarWinds	Current Release
Systems Management	SolarWinds	Current Release
Application Performance Management	Dynatrace	Current Release
Infrastructure Performance Management	Turbonomics	Current Release
Security and Event Management	IBM QRadar	Current Release

Section IV: Applications

4-CCD-01 Accepted Application Delivery Models

To reduce ongoing operating costs, maximize service delivery and improve IT risk management/mitigation, the City and County of Denver targets the following software delivery models, in order of preference:

Type	Name
Cloud (SaaS)	"Software as a Service" software is licensed on a subscription basis and is centrally hosted and managed. Internal software details are immaterial.
Cloud-hosted & Vendor Managed	The software is generally the "on-premise" software hosted on off-site dedicated servers managed by the vendor. Some internal details are known to and approved by TS.
On-premise & Vendor Managed	Software must follow standards within this document for on-premise installations.
On-premise & Commercial off the Shelf (COTS)	Software is installed on-premises and managed by TS and must follow standards within this document.
Cloud-native & Custom Developed Solutions	All developed solutions (whether produced by TS or a third party) must be implemented on an existing application/platform identified in the "Business Services" section.
On-premise & Custom Developed Solutions	

4-CCD-02 Middleware

Type	Name	Requirement
Application Server	Oracle Weblogic (deprecated)	12c
Web Server	Microsoft IIS	10.0
	Apache Tomcat	9
Data Integration Services	Microsoft SSIS	2017
Reporting Services	Microsoft SSRS	2017
Enterprise Integration Services	MuleSoft AnyPoint Platform	Current Release
Managed File Transfer	Globalscape EFT	7.2

4-CCD-03 Database

Type	Name	Requirement
Database Server	Microsoft SQL Server	2017

4-CCD-04 Business Services

The following table represents the standard applications, or the “go-forward platforms”, used to support specific business services.

Type	Name	Requirement
Appraisal & Tax Management	Tylertech iasWorld	Current Release
Planning & Zoning Management	Accela	9.3.15
Permitting & Inspection Management	Accela	9.3.15
Human Resource Management	Workday HR	Current Release
Financial Management	Workday Financials	Current Release

Case Management & Customer Relationship Management	Salesforce Service Cloud	Current Release
ECS Cashiering & Payment Services	ACTIVE Network (deprecated)	8.1
Content Management	Microsoft SharePoint	Current Release
Document Management	Alfresco	4.2.3
Document Scanning	Kofax Capture	11.0
Web Content Management	Adobe Experience Manager	Current Release
IT Service Management	ServiceNow	Current Release
Computer Aided Dispatch (CAD)	TriTech Software Systems	5.8.7
Geographic Information System (GIS) Services	ESRI ArcGIS	10.4.1
Resident Experience & Web Applications	Denver Apps (See Appendix A for detail)	Current Release

Section V: Data

5-CCD-01 Software

Type	Name	Requirement
Business Intelligence and Dashboard	Microsoft PowerBI	Current Version
Records Inventory	Zasio Versatile Enterprise	Current Version
Data Protection and Privacy Assessments/Compliance	OneTrust	Current Version
Document Repository	Alfresco	(See "Business Services" Section)
Open Data Portal	CKAN	Current Version
Data Classification (and Info Sec)	Varonis	Current Version

Data Replication	Zerto	Current Version
Data Backup & Recovery	CommVault	V11 SP8

5-CCD-02 Records Management

Name	Requirement
General Record Retention Schedule	Current Schedule (September 2018)
Offsite Storage & Tape Destruction	All American Records Management

5-CCD-03 Data Privacy and Data Protection

Name	Requirement
City and County of Denver Executive Order Information Governance Committee (IGC)	Executive Order 143
Personal identifying information (PII)	House Bill 18-1128
NIST Privacy Controls for PII	NIST 800-53, Revision 4, Appendix J
Federal Tax Information (FTI)	IRS Pub 1075 R
Fair Credit Reporting Act (FCRA)	FTC FCRA PDF
Family Educational Rights and Privacy Act Regulations (FERPA)	FERPA 34 CFR Part 99
Payment Card Industry (PCI)	PCI DSS Standards
Disclosure of Substance Abuse Records	42 CFR Part 2 FAQ 42 CFR Part 2 Law
Criminal Justice Information Services	CJIS Security Policy
Health Insurance Portability and Accountability Act (HIPAA)	45 CFR Parts 160,162, and 164 NIST/HIPAA Crosswalk NIST 800-66
American Institute of Certified Public Accountants	AICPA Framework

Section VI: Software Quality

6-CCD-01 Non-Functional Requirements

Nonfunctional requirements (NFRs) define the criteria that are used to evaluate the whole system, but not for specific behavior (the functional requirements). We organize our NFRs around the standard ISO/IEC 25010 and the product quality model. They typically can be divided into two main categories:

- NFRs that affect system behavior, design, and user interface during work.
- NFRs that affect the development and support of the system.

The "Type" column below reflects these quality characteristics/sub-characteristics. The "Name" column reflects the name of the specific NFR. The City and County of Denver values proposed software solutions that can meet these requirements:

Type	Name	Requirement
Security/Confidentiality	Data Encryption	All City Data and End User Data will be encrypted in transmission (including via web interface) and in storage. Applications must secure data in transit using the TLS 1.2 protocol or newer. Moreover, endpoints shall not support TLS 1.1 or older.
Security/Authentication	Federated Authentication	Supports federated authentication using the SAML 2.0 protocol
Compatibility/Standards Compliance	TS Architecture Standards	The solution is compatible with the technology/standards represented within this document
Compatibility/Interoperability	Web Services	Web Applications can efficiently and effectively support data exchange (sending/receiving) using established Web Services standards/Open API
Reliability/Availability	High Availability	The solution shall meet the agreed availability targets (service time and/or hours and planned downtime) as defined in the service/operational level agreement (SLA/OLA)
Reliability/Recoverability	Disaster Recovery	The software can re-establish its level of performance and recover the data directly affected in the case of a failure.
Usability/Accessibility	WCAG 2 Level AA compliant	Public-facing solutions are accessible for people with disabilities (WCAG 2 Level AA compliant)

Usability/Responsive Design	Responsive UI	Web Applications must meet responsive design standards which detects users' screens and adjusts the layout based on the screen size and orientation (example; does the application render using a modern browser or smartphone)
Maintainability/Analyzability	Fault Discovery and Remediation	The solution provider can easily find and fix faults within the software system and has a sound maintenance process to support changes
Maintainability/Testability	QA Testing	Changes to the solution can be efficiently and effectively tested in a non-production environment
Portability/Adaptability	Hardware/Software Independence	The solution can be transferred from its current hardware or software environment to another when necessary
Performance/Time Behavior	Processing Times	Solution response, processing times and throughput rates, when performing its functions, meets requirements
Performance/Resource Utilization	Scalability	The system can handle load increases without decreasing performance
Performance/Capacity	Storage Capacity	The solution can store the necessary record volume to support business processes

Appendix A: Denver Apps Platform

The Denver Apps Platform is a collection of technologies and frameworks for applications developed in-house or by vendors to satisfy service needs that can't be met by a SaaS or COTS solutions or that are unique to or that distinguish the City and County of Denver to its residents.

Type	Name	Technical Requirement
Browser-based User Interface (UI)	Angular	Current Release
Hybrid API (BFF-Microservices)	.NET Core	Current Release
Data Layer	SQL Server	2017
Scheduling Services	Hangfire	1.6.19
Platform Analytics	Adobe Analytics	N/A
Platform Telemetry	Azure Application Insights	N/A
Static Analysis	SonarQube	8.0
CI/CD	Azure DevOps	N/A

All applications written for the Denver Apps Platform must be:

- stateless and will run correctly on any number of load-balanced servers
- standard .NET Core / standard IIS and not rely on additional feature installs (WCF, etc.)
- self-contained and addressable via a unique non-root segment URL ("/abc" not "/")

Installed to the platform must be:

- Scriptable - all steps of the installation must be scriptable (via PowerShell for example) and autonomously executable
- Reversible - the installation and all impacts of it on the environment must be autonomously reversible

Repeatable and idempotent - a repeated install should have no impact on the environment or application

Revision History

Date	Modified By	Revision Comments
4/8/2020	Dan George	Updated from previous version

Data Record Retention Policies

Section	Title	Description	Retention Guideline	Destruction Guideline
CITATIONS/PARKING CASES/PROCEEDINGS				
40.100*	ADMINISTRATIVE CITATION	Records related to written citations that are non-criminal tickets issued to individuals who do not correct violations of the City code. This includes parking tickets, Animal Citations, Restaurant Inspection Citations, Noise ordinance violation citation, Air ordinance violation citation, etc.	4 years from date of issuance	NA
85.020C	CASE FILES	Parking Cases	1. Paper Retention Once scanned into case management the paper document can be destroyed 2. Electronic Record 2 year	NA
85.030	RECORDED PROCEEDINGS AND LOG NOTES (Reference: State Judicial Records Retention Schedule)	Notes, digital or analog audio or video recording of Civil, Small Claims, Traffic Infraction, Traffic, Misdemeanor, Ordinance Violations, Felony proceedings before the County Court	2 years	NA
POLICE RECORDS				
100.080 L	Passive Surveillance Record [CRS 24-72-113] 1. License Plate Recognition Data	Data and images recorded by means of automated license plate recognition systems (one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of registration plates into computer-readable data) used to capture license plate numbers for parking enforcement, booting, stolen vehicle identification or other law enforcement purposes	21 days for data and images	Mandatory destruction after 365 days, except that "hits" are retained for life of

				related case file
100.080Y	POLICE RECORDS - Vehicle Impound Records	Records documenting the impoundment of licensed and non-licensed motorized vehicles and sports craft that have been taken into custody for violations of laws that govern their use, operation and ownership.	2 years after vehicle is released to owner or otherwise disposed of	NA
PERMITS/MAILNG PERMIT RECORDS/VARIANCE TRAFFIC				
75.020 F	Permits Issued by Denver in General	Records including applications, proof of payment and insurance coverage and other supporting documentation for permits issued to allow specific activities; includes (but is not limited to) permits for alarm system installation, banners, billboards, boats on municipal lakes, burning of refuse, candles and open flames in public places, cemetery monument placement, communication towers, concealed weapons, excavation, explosives, facility use, fence installation, fireworks and pyrotechnical displays, flammable or combustible liquids storage or sale, gas and oil drilling structures, grading, guard dogs, home occupations, house moving, hunting, landscaping, loudspeakers, odor control, parking, parades and assemblies, right-of-way planting, signs, special events or uses, spray booths, tents or canopies, tree trimming or removal, watering, etc.	2 years after expiration, revocation, denial or termination of permitted use	NA
75.020 F	G. Permits to Work in Public Way	Encroachment permits, revocable permits, street cut permits, public right-of-way permits or other permits issued for permanent, indefinite or temporary trespass on, under or over the public right-of-way (streets, sidewalks, adjacent public right-of-way or publicly owned property); for private use or construction to place improvements, communications, utility or other installations or temporary uses in the public way, such as demolitions, excavations, street cuts, blasting, crane operations, barricade	3 years after permit expiration, revocation or discontinuance of use and after expiration of any warranties for activity or work done in public way	NA

		installations, concrete construction (curb, gutter, sidewalks) or the moving of heavy equipment; supporting documentation includes applications, maps and drawings, proof of insurance, departmental reviews, approvals, etc.		
40.170E	MAILING AND DISTRIBUTION RECORDS	Meter and permit usage records	1 year	NA
60.050	VARIANCE AND EXEMPTION CASE FILES (see also Sch.110 #110.010.D*)	Records pertaining to approval of variances to code requirements, such as setback and parking requirements, requested by property owners and developers due to hardships and circumstances outside of their control	10 years after expiration, revocation or discontinuance of use	NA
60.050	STREET AND TRAFFIC OPERATIONS RECORDS *K. Traffic Marking, Timing and Signalization Files*	Records and data documenting traffic signal timing, traffic marking and signalization and construction zone, crosswalk parking and no parking zones, speed zone and truck route designations.	2 years after superseded	NA
EQUIPMENT				
35.010	EQUIPMENT RECORDS IN GENERAL	Records pertaining to all types of equipment, mechanisms and systems and their maintenance, inspection and repair history, including fire and water detection alarm systems; heating, ventilation, air conditioning (HVAC) systems; disaster warning systems; elevators; sump pumps; power generators; boilers; measuring and weighing devices; tools; office equipment, recording systems; etc. Documentation includes warranties, operating manuals, calibration and testing records, inspections, vehicle registration certificates, titles, bills of sale, et	Until equipment is no longer under municipal control or life of equipment + 1 year and/or after any contractually required audit, unless another retention period is required by law or specified elsewhere in this Retention Schedule	NA
FINANCIAL RECORDS				
30.020*	ACCOUNTS RECEIVABLE (A/R) RECORDS	Records of collection of monies such as record documenting payments to Denver in which the City holds a property lien	3 years	NA

		until the debt is satisfied (e.g., liens arising from demolition, lot cleaning), including original liens and lien releases; includes but is not limited to automatic clearinghouse (ACH) forms; on-line payments, cash books, journals, receipts, reports and supporting documentation; fines, fees and charges receipts, other payments and supporting documentation; accounts receivable balance sheets; cash register validation tapes; statements and invoices issued by Denver, etc. See also 30.210, Utility Billing.		
30.021	ACCOUNTS DEEMED UNCOLLECTABLE	Records of accounts deemed uncollectable, including write-off authorizations.	3 years after the year of write-off date	NA
30.030A	ASSET RECORDS A. Annual Fixed Asset Reports	Worksheets listing fixed assets, purchases and disposition of assets.	Until superseded	NA
30.030B	ASSET RECORDS B. Disposition Records	Records of disposal of surplus property (except real estate) and unclaimed, abandoned or confiscated property such as bicycles and vehicles by auction, competitive bidding or destruction, including date, department name, description of item, value, disposition, method and reason for disposition, condition, value and approvals.	3 years after disposition	NA
30.030C	Inventories	Listings of expendable and nonexpendable property and assets, including buildings, real estate, vehicles, furniture, equipment, supplies, trees, merchandise for sale at Denver agencies operated concessions or gift shops and other assets; may include description, cost, date purchased, location, name of vendor and depreciation detail.	Until superseded	NA
30.030D	Unclaimed Property	Documentation Any form of record sufficient to verify information on unclaimed property previously reported to the State Treasurer showing the name and last known address of the apparent owner of reportable unclaimed	Date on which property is reportable + 10 years	NA

		property, a brief description of the property, and the balance of each unclaimed account, if appropriate.		
30.040*	CREDIT CARD RECEIPTS [see also #30.010.B Credit Card Records and #30.020 Accounts Receivable Records]	Credit card receipts of customer who purchases a product or service from the City and County of Denver using his/her credit card.	18 months from date of original transaction	NA
30.050A	BANK RECORDS	Records documenting the current status and transaction activity of funds held at banks. A. Bank Records – Routine banking records, including but not limited to duplicate copies of checks, check stubs, voided checks, deposit slips and trial balances. See also 30.010, Accounts Payable (A/P) Records for checks and check registers, and 30.140.A, Investment Instruments for CDs, money market certificates, etc.	3 years	NA
30.050B	Bank Security Records	Records documenting the pledge of bonds or securities by banks serving as depositories for public funds including depository contracts, security pledges and statements, surety bonds, and similar records.	Permanent	NA
30.050B c	Bank Statements, Pass Books and Reconciliations	Monthly statements pass books or reconciliations showing funds on deposit.	Retention: 7 years	NA

INFORMATION TECHNOLOGY AND COMMUNICATION SYSTEMS

55.010 COMMUNICATION SYSTEMS RECORDS

A. Call Detail and Telephone Usage Records

Records relating to telephone, radio transmission, pager and other communication systems.

Records of outgoing calls.

Retention: 2 years or until system capacity is exceeded

B. Communication Sites Records

Records of sites used for installation of communication system infrastructure such as communication towers.

Retention: Until site is no longer under Denver's jurisdiction or no longer serves a communication system purpose

C. Licenses – Communication Systems

Licenses issued by the Federal Communications Commission (FCC) or other agencies for television or radio system and other communication system operations and supporting documentation.

Retention : : 1 year after expiration of license

D. System Management Records – Communication Systems

Relating to creation, modification and disposition of communication systems, including: acquisition and installation records, equipment records, FCC records, maintenance contracts (copies), repair order forms, service orders, system planning records, etc.

Retention: Life of system + 1 year

E. User Data – Communication Systems Includes the following types of electronic data: cap codes, electronic records of users, extension and pager numbers, service providers, Voice over Internet Protocol (VoIP) user records, etc.

Retention: Until superseded

55.020* COMPUTER SYSTEM RECORDS

Records pertaining to the installation and operation of computer systems and software.

A. Access Control and Security Records

Records required to establish and maintain computer security, including: access requests, authorizations, encryption keys, journals, password documentation, reports, system access logs and other access control records.

1. System Access Logs

Retention: 6 months

2. All Other Access Control/Security Records

Retention: Delete when no longer administratively useful

B. Computer Audit Reports

Completed to determine compliance with policies relating to software and electronic records management.

Retention: Until subsequent audit is completed

C. Computer Backup Records

1. Computer Backup Documentation related to how and when regular computer records backups are completed.

Retention: 1 year after superseded or obsolete

2. Computer Contingency Backups

Records recorded on electronic media consisting of copies of programs or instructions necessary to retrieve copied information and data identical in physical format to a master file or database and retained in case the master file or database is damaged or inadvertently erased.

Retention: Retain off-site until replaced or superseded

D. Computer Hardware and Software Documentation

Written documentation necessary to operate computer equipment or programs and to access or retrieve stored information or data. Documentation may be in paper or electronic formats and may include: application bluebooks, flowcharts, hardware specifications, maintenance requirements, operation and user manuals, system change records, license agreements (copies), “gold” copies of software, records of rights to use customized software, source codes, etc.

Retention: Until computer equipment or software is no longer used or needed to retrieve or store
data

E. Computer System Maintenance Records

Documentation of maintenance of computer systems and components needed to ensure compliance with warranties or service contracts, schedule regular maintenance and diagnose system or component problems. Includes: component maintenance records, computer equipment inventories, failure logs, hardware performance reports, invoices (copies), maintenance contracts (copies), warranties, etc.

Retention: Life of system or component + 1 year

F. Computer System Program Records

Documentation pertaining to development, installation, modification, troubleshooting, operation and removal of software from computer systems; records required to plan, develop, operate, maintain and use electronic records; and technical specifications, file specifications, code books, record layouts, flowcharts, job control language, operating instructions, user guides, system overviews, output specifications, migration plans and other records pertaining to systems operations.

Retention: : Until superseded or no longer needed to retrieve or read data and information that is stored electronically

G. Computer System Test Records

Electronic files or reports created in the monitoring and testing of system quality and performance, as well as related documents for the electronic files/records.

Retention: Delete or destroy when no longer administratively useful

H. Network and Fiber Optics Records

Documentation of the wiring of the computer network system, including blueprints, diagrams and drawings of layout and installations of fiber optics, computer networks, cables, computer equipment connections and similar documentation.
Retention: Until superseded

I*. System Usage Records

Electronic files created to monitor system usage, including log-in files, audit trail files, cost-back files used to assess charges for system use, system-created or vendor-originated logs documenting various aspects of information technology systems operations.
Retention: 3 years except for Human Resources audit trail records to be retained until audit requirements are met.

55.030 DISASTER PREPAREDNESS AND RECOVERY PLANS – IT

Documents the protection and reestablishment of data processing services and equipment in case of a disaster; includes: checklists, emergency contact information and procedures.
Retention: Until superseded by revised plan

55.040* ELECTRONIC RECORDS IN GENERAL

Computer-generated and -maintained records in electronic formats retained for recordkeeping purposes, including the following examples: digital recordings – audio and video; e-mail messages and attachments; imaged records; databases and spreadsheets; word processing files; recorded videoconferences; digital photographs; geographic information systems datasets; and other records retained in electronic format.
A*. Electronic Records (Copies) Retained Solely for Convenience
Retention: Until no longer needed, provided that definitive or record copy of record is retained for applicable retention period, except that metadata need not be preserved.

B*. Electronic Records Retained for Recordkeeping Purposes

Retention: Based on content, retain for retention period for specific type of record; i.e., electronic records have same retention periods as paper or microfilm records with same content, except that metadata need not be preserved.

55.050 ELECTRONICALLY STORED INFORMATION (ESI) DATA MAPS

Diagrams of computer systems and associated narrative information explaining the locations and context of the information stored within the computer systems, used for electronic discovery purposes.
Retention: Until superseded

55.060 PROJECT RECORDS – INFORMATION TECHNOLOGY AND COMMUNICATION SYSTEMS

Project records relating to the planning, development, design, selection, acquisition, installation, modification, conversion, upgrade and replacement of communications, computer and information systems technology; project files may include: analyses, assessments, evaluations, reports and studies; copies of contracts, proposals, invoices, project bonds, purchase orders and vendor literature; correspondence and project notes; project charters, plans, planning and development records, project team and vendor meeting records; user requirements, specifications, drawings, standards,

architecture and design; quality assurance testing reports, statistics and coverage requirements; issues logs; and other project records and documentation.

A. Implemented Systems

Retention: 6 years after replacement of information system or communication infrastructure; except prior to destruction, evaluate for continuing legal, administrative or historical value

B. Systems not implemented

Retention: 3 years

55.080 WEBSITE AND INTRANET RECORDS

A group of World Wide Web or internal web pages containing hyperlinks to each other and made available online for responding to public inquiries and providing information.

A. Access Reports

Web Pages Reports tracking hits to the website or intranet.

Retention: 2 years

B. Development and Evolution Records

Web Pages Documentation of development and changes to the website or intranet web pages.

1. Web Pages and Related Scripts – Internet and Extranet – Home Pages and Indexes

   Retention: 10 years for superseded pages and 2 years for informational only pages

2. Intranet Web Pages Designed for Internal Access to Information

   Retention: Delete when no longer useful

C. Page Design Records – Web Pages

Style guide for web page design.

Retention: Until superseded or until no longer needed for reference

C. Use Tracking Logs

Website and Intranet Electronic logs for tracking websites visited by internal sources.

Retention: 2 years

Branding, UI, UX Guidelines

https://www.denvergov.org/content/denvergov/en/denver-marketing-and-media-services/brand-guidelines/logo-seal.html

City and County of Denver – Department of Finance
Cash, Risk and Capital Funding Division
Receipting Requirements for City Funds

Reference:
City Charter Article II – Mayor and Executive Departments, Part 5 – Finance, §2.53 and §2.54
Revised Municipal Code – Chapter 20 – Finance, Article III – Disposition of Funds, Division 2 - Handling of Receipts and Procedures for Making Refunds, Section 36 and 38
Fiscal Accountability Rule 3.3 – Change Fund and associated procedures and forms
Fiscal Accountability Rule 3.4 – Receipt and Deposit and associated procedures and forms

Payment, Receipt, Cash Handling or Banking of City Funds – Any implementation or process involving payment, receipt, cash handling or banking of City funds (as defined by Denver Revised Municipal Code 20-36) shall be approved by and coordinated directly with the City's Cash Management Section within the Department of Finance's Cash, Risk and Capital Funding Division. The Department of Finance has the authority to establish what forms of payment the City accepts and what mechanisms are used to process the payments.

Deposit of Funds – Funds gross of any fees are the property of the City and shall settle directly to a City-owned bank account approved by the Cash Management Section.

Funds shall be deposited daily by either electronic or physical delivery into a City-owned bank account approved by the Cash Management Section. Any third-party service handling City funds for transport to the bank shall be bonded. The City's preferred method for physical bank delivery is armored car.

Credit Card Payments – Credit card payments shall be processed through a City-owned Merchant Identification (MID) code approved and issued by the Cash Management Section under the existing merchant services agreement managed therein. Any third-party system integrations must certify to process with the City's existing merchant services provider prior to implementation.

The assessment of credit card convenience fees to customers is not part of the City's current receipting business model. Any proposal to assess fees beyond the cost of City services shall be submitted to the Cash Management Section for review and submission to the Manager of Finance for approval.

Systems, structures and procedures implemented shall prove compliant with Payment Card Industry Data Security Standards (PCI DSS), be reviewed and approved by the Cash Management Section and the City's Data Security Team, and/or identified as out of scope by the Data Security Team prior to selection or implementation.

Electronic Funds Transfers – Systems, structures and procedures implemented shall comply with the National Automated Clearing House Association (NACHA) and other applicable rules and regulations regarding electronic funds transfers. ACH and/or Wire payment mechanisms shall be reviewed and approved by the Cash Management Section prior to implementation.

Payment and Banking Mechanisms – Any payment, receipt, cash handling or banking products or services such as lockbox, online services, point-of-sale or other receipting or transfer mechanisms shall operate using the City's currently contracted providers as overseen by the Cash Management Section. If a business need cannot be met with currently contracted providers, the proposed solution and processing structure shall be reviewed and approved by the Cash Management Section.

Third-Party Services – If a third-party is involved in the payment, receipting, cash handling or banking process, the initiating City department or designee shall coordinate the structure, process and implementation with the Cash Management section and the third-party. All payment, receipting, cash handling or banking structures and processes shall be reviewed and approved by the Cash Management Section prior to selection and implementation. The City's Department of Finance has final approval of all payment, receipting, cash handling or banking structures and processes.

Internet of Things (IoT) Device Policy	
What:	To provide direction and governance to City Departments and Agencies and their vendor partners to successfully manage operation of IoT Devices and their associated risks throughout the devices' Lifecycles.
Why:	IoT Devices are advancing how the City operates using smart or smarter technologies. These devices are changing the cybersecurity and privacy risk landscape for the City. These risks can be mitigated in three ways: (1) protect device security, (2) protect data security, and (3) protect individuals' privacy.
How do we communicate/implement:	Communications plan jointly developed by the IGC and Technology Services. Plan implemented by Technology Services.
How do we measure success/compliance:	Success of this program can be indirectly measured through: (1) the ability of the City to innovate and increase performance using smart or smarter devices, and (2) through audit and policy compliance.
IGC Reviewers:	IoT IGC Working Group and Committee *en banc*

Policy Control Information	
Executive Sponsorship	Information Governance Committee
Related Policies	
Effective Date	June 5, 2020

Purpose

The Internet of Things (IoT) is an umbrella term for the rapidly evolving and expanding collection of diverse technologies that both connect to a network or the Internet and interact with the physical world. IoT Devices are the logical progression of combining the worlds of Information Technology (IT) and Operational Technology (OT). Many IoT Devices are the result of the convergence of mobile computing, cloud computing, embedded systems, industrial controls, low-priced hardware, and other technological advances. IoT Devices provide functionality, data storage, and network connectivity to devices that previously lacked them, fostering innovation through general efficiencies and economies; real-time or near-time control of systems and their environment; and the ability to better anticipate future events.

The City is already using large number of IoT Devices. It is necessary to consider how these current devices and any future IoT Devices will affect the City's cybersecurity, privacy, and infrastructure risks, and how those risks might differ from conventional information technology. Additionally, IoT

Devices may have unforeseen and unintended consequences upon the City's continuity of government, business operations, and critical infrastructure programs; incident management and operational coordination; public information and warning; emergency planning; as well as community preparedness and post-disaster recovery coordination. The purpose of this policy is to provide direction and governance to City Agencies and Departments and their vendor partners to successfully manage the operation of IoT Devices and associated risks.

Scope

This policy applies to all City Agencies and Departments, including auxiliary units and external business or organizations, that use or provide IoT Devices to the City and County of Denver.

Executive Sponsorship

Executive sponsorship for this document comes from Information Governance Committee and City and County of Denver Executive Order 143, as amended.

Policy

1. Vendors or contractors that provide an IoT Device to the City shall ensure and provide attestation that the IoT Devices provided:
    1.1. do not knowingly contain any Hardware, Software, or Firmware component with any restriction, known Security Vulnerability, or other exploitable defects as listed in:
        1.1.1. Federal Acquisition Regulations (FAR) or active FAR Circulars (Code of Federal Regulations, 48 C.F.R.);
        1.1.2. the National Vulnerability Database (NVD) of NIST;
        1.1.3. any additional database selected by Technology Services that tracks Security Vulnerabilities, defects, or restrictions, that is credible, and is similar to the FAR and NVD; and
    1.2. ensure that data is properly protected while in-transit and at-rest on the device using Strong Cryptography by default; and
    1.3. are only capable of accepting Properly Authenticated Updates from the vendor to the exclusion of all other methods (for all Software or Firmware components of the devices); and
    1.4. use only non-deprecated and current industry-standard protocols and technologies for functions including, but are not limited to:
        1.4.1. communications, such as standard ports for network traffic;
        1.4.2. Strong Cryptography;
        1.4.3. interconnection with other devices or peripherals; and

1.5. do not include any Fixed or Hard-Coded Credentials used for remote administration, the delivery of updates, or communication; and

1.6. have mechanisms to prevent unauthorized and improper physical and logical access to, usage of, and administration of the device by people, processes, and other computing devices; and

1.7. have mechanisms to monitor and analyze the device activity for signs of incidents involving security and improper use; and

1.8. have mechanisms to maintain a current, accurate inventory of all IoT Devices and their relevant characteristics throughout the devices' Lifecycle.

2. Vendors or contractors that provide an IoT Device to the City shall promptly notify the City of any known Security Vulnerabilities or other defects subsequently disclosed to the vendor by a security researcher or of which the vendor or contractor becomes aware for the duration of the agreement.

3. IoT Device Software or Firmware components shall be promptly updated or replaced, consistent with other provisions of the governing terms of support, in a manner that allows for any future Security Vulnerability or other defect in any part of the Software or Firmware to be patched in order to fix or remove a vulnerability or defect in the Software or Firmware component as a Properly Authenticated Update.

4. Vendors or contractors that provide an IoT Device to the City shall provide a patch, repair, or replacement in a timely manner in respect to any new Security Vulnerability or other defect discovered through any of the databases as described in §1.1 or from notifications in §2 in the event the vulnerability cannot be remediated through an update as described in §3.

5. Vendors or contractors that provide an IoT Device to the City shall provide the City with general information on the ability of the device to be updated, such as:

5.1. the manner in which the device received security updates;

5.2. the anticipated timeline for ending security support associated with the network-connected device;

5.3. formal notification six (6) months prior to when the security support will cease; and

5.4. any additional information required by the City or recommended by industry best-practices.

6. City Agencies and Departments shall maintain continuous and non-lapsing support and maintenance over the IoT Devices' Lifecycle that provide for Properly Authenticated Updates of Security Vulnerabilities and other defects on all devices that are within their span of control.

7. City Agencies and Departments shall securely and uniformly configure and properly deploy and operate all IoT Devices, including proper use of mechanisms in §1.6, §1.7, and §1.8, on all devices that are within their span of control.

8. In the event that a City Agency or Department reasonably believes the procurement of an IoT Device that is consistent with §1 through §5 would be unfeasible or economically impractical, the Agency or Department may request a waiver to this policy from the Information Governance Committee or its delegate in order to purchase or otherwise use a non-compliant IoT Device with compensating controls to mitigate the cybersecurity, privacy, and infrastructure risks as well as address any other impacts the device may impose. These compensating controls may include:

8.1. network segmentation or micro-segmentation;

8.2. the adoption of system-level security controls, including but not limited to operating system containers and micro-services;

8.3. multifactor authentication or other cryptographic methods;

8.4. intelligent network solutions and edge systems, such as gateways or proxies, that can isolate, disable, or remediate the IoT Device's non-compliance; and

8.5. additional redundancy or continuity of operation mechanisms.

9. Technology Services may stipulate additional requirements for management and use of non-compliant devices regardless of the method of acquisition or any type of grandfather clause to address the long-term risk of any active non-compliant IoT Devices. These requirements may include:

9.1. deadlines for the removal, replacement, or disabling of non-compliant devices (or their network connectivity);

9.2. defining the minimal requirements for compensating controls to ensure the integrity or security of the non-compliant device.

10. If an existing credible and recognized third-party security standard for an IoT Device provides an equivalent or greater level of security to that described in §1 through §5, the City may allow the vendor or contractor to demonstrate compliance with that standard in lieu of the requirements under §1 through §5 of this policy. Vendors or contractors that provide an IoT Device to the City shall provide third-party certification and attestation that the device complies with the security requirements of the industry certification method of the third party.

Definitions

The following terms are used in this policy:

Firmware: a computer program and the data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the program and data cannot be dynamically written or modified during execution of the program.

Fixed or Hard-Coded Credential: a value, such as a password, token, cryptographic key, or other data element used as part of an authentication mechanism for granting remote access to an information system or its information, that is:

a) established by a product vendor or service provider; and
b) incapable of being modified or revoked by the City or vendor partner lawfully operating the information system, except via a Firmware update.

Hardware: the physical components of a device

Interface Capability: the capability of a device that enables device interactions (*e.g.*, device-to-device communication, human-to-device interaction). These types of Interface Capabilities include:

a) Application Interface: the ability for other computing devices to communicate with an IoT Device through an IoT Device application. An example of an application interface capability is an application programming interface (API).
b) Human User Interface: the ability for an IoT Device and people to communicate directly with each other. Examples of Human User Interfaces include: touch screens, haptic devices, microphones, keypads, multifunction printers (*e.g.*, touch screen), and cameras.
c) Network Interface: the ability for an IoT Device to interface with a communication network for the purpose of communicating data to or from an IoT Device. A network interface capability includes both Hardware and Software. Examples of Network Interfaces include: 802.3 (ethernet), 802.11 (WiFi), WiMAX, ISO/IEC 18000 (RFID), ECMA-340 & ISO/IEC 18092 (NFC), 802.15 (Bluetooth), Long-Term Evolution (LTE), IMT-2020 (5G), Z-Wave, and 802.14 (ZigBee).

Internet of Things (IoT) Device: The full scope of the Internet of Things is not precisely defined by the industry; it is clearly vast. Each City Agency or Department may have its own type of IoT Devices, such as: traffic and smart road technologies, and underground tank monitoring technologies in Transportation & Infrastructure; smart LED lighting and smart landscape watering in Parks and Recreation; service kiosks in Human Services; building automation devices and electronic door locks in General Services; smart voting and smart petitions in Elections; garage door automation in Denver Fire Department; and video sensors and gunshot detection systems in the Denver Police Department; air quality and environmental monitoring devices in Public Health & Environment; not to mention smart televisions, queue management, and employee time clocks in Technology Services. For the purposes of this policy, the term "IoT Device" means a device that:

a) is a Network-Connected Device, and
b) has one or more of the following capabilities:
   i. Transducer Capability,
   ii. Interface Capability,
   iii. Supporting Capability.

Lifecycle: activities associated with an IoT Device that fully encompass the device's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its decommissioning and disposal.

Network-Connected Device: a device that:

a) is capable of connecting to and is in regular connection with any type of City network or the Internet; and
b) has computer processing capabilities that can collect, send, or receive data

Properly Authenticated Update: an update, remediation, or technical fix to a Hardware, Firmware, or Software component issued by a product vendor or service

	provider used to correct particular problems with the component, and that, in the case of Software or Firmware, contains some method of authenticity protection utilizing Strong Cryptography, such as a digital signature, so that unauthorized updates can be automatically detected and rejected.
Security Vulnerability:	any attribute of Hardware, Firmware, Software, process, or procedure or any combination of these factors that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected.
Software:	a computer program and associated data that may be dynamically written or modified.
Strong Cryptography:	the current and promulgated cryptographic standards and mechanisms as defined by the National Institute of Standards and Time (NIST). Any cryptographic standard or mechanism that has been deprecated or otherwise removed from the current promulgated standards and mechanisms shall not be grandfathered or otherwise considered compliant.
Supporting Capability:	the capability of a device to provide functionality that supports the other IoT capabilities. Examples of Supporting Capabilities include, but are not limited to: device management, cybersecurity, and identity (*e.g.*, PKI certificates or other identification tokens) capabilities.
Transducer Capability:	the capability of a device to interact with the physical world and serve as the edge between digital and physical environments. Transducer capabilities provide for the ability for a Network-Attached Device to interact directly with physical entities of interest. The two types of Transducer Capabilities are: a) Sensing: is the ability for a device to provide an observation of an aspect in the physical world in the form of measurement data. Examples include: temperature measurement, radiographic imaging, optical sensing, audio sensing, multifunction printer (*e.g.*, scanner), or door position. b) Actuating: is the ability to change something in the physical world. Examples include: heating coils, cardiac electric shock delivery, electronic door locks, servo motors, unmanned aerial vehicle operation, robotic arms, multifunction printer, electronic valves and switches.

Policy: Payment Card Industry (PCI) Security| 2/9/2016

DENVER
TECHNOLOGY SERVICES

Policy Control Information	
Division	Information Security
Team	Governance, Risk and Compliance
Regulatory Compliance	PCI
Effective Date	February 9, 2016

Table of Contents

Purpose

Establish ownership, guidelines, and governance regarding PCI compliance for the City and County of Denver

Scope

This policy applies to all technology and business domains within the City and County of Denver, with the following exceptions:

- Denver International Airport (DEN): Uses its own merchant identification number (MID) on non-Technology Services controlled devices deployed at DEN. DEN is also on a separate network that Technology Services does not support.
- District Attorney's office: Uses its own (MID) and on a separate network that Technology Services does not support.
- Denver Public Library and Denver County Courts: Use CCD's MID but on a separate network that Technology Services does not support.

Governing City Rules (Fiscal, etc.)

Executive Order No. 16, "Use of Electronic and Communication Systems and Services"

Executive Order No. 18, "Establishment of Technology Services and Definition of its Mission and Functions"

Executive Sponsorship

Executive sponsorship for this document comes from the Chief Information Officer (CIO), City and County of Denver. The CIO shall review this policy periodically with senior management to determine if changes to this policy are required.

Definitions

CDE – Cardholder Data Environment: the logical environment in which cardholder data is processed, transmitted or stored

MID – Merchant Identification number - a unique number assigned to a merchant account to identify it throughout the course of processing activities

PCI – Payment Card Industry: a set of security standards created by the payment card industry to protect cardholder information

PCI DSS – Payment Card Industry Data Security Standard: the specific standards that must be followed to ensure PCI compliance

PA DSS – Payment Application Data Security Standard: the specific standards of development that must be followed to ensure an application's compliance with PCI

Policy Overview and PCI Background

This document explains the City and County of Denver's technology-based PCI information security requirements for all employees. The City and County of Denver's (CCD) management has committed to these security policies to protect information utilized by CCD in attaining its business goals. All employees are required to adhere to the policies described within this document.

The Payment Card Industry Data Security Standard (PCI DSS) program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all credit card brands. CCD ensures adherence to the active release of the PCI-DSS.

The PCI Data Security Standard requirements apply to all payment card network members, merchants, and service providers who store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites and retail Point of Sale (POS) systems that process credit cards over the Internet. This document addresses the requirements of the PCI DSS. Additional information regarding this standard can be found at https://www.pcisecuritystandards.org.

Scope

PCI System Components

The PCI requirements in this document apply to all "system components". System components are defined as any network component, sever, application, or client that is included in or connected to the cardholder data environment (CDE), or that can affect the security of the CDE. The CDE is defined as part of the network that possesses cardholder data or sensitive authentication data. For example, the following types of systems would be in-scope for compliance within any environment:

- Systems storing cardholder data (e.g. databases, PCs used by accounting for generating reports)
- Systems processing cardholder data (e.g. web servers, application servers, POS devices, etc.)
- Network devices transporting or directing cardholder traffic (e.g. border router, DMZ firewall, intranet firewall, etc.)
- Devices that create media containing cardholder data (e.g. fax machine, printer, backup tapes)
- Support systems (e.g. Active Directory, IDS, PCs performing support functions such as system administration, etc.)
- Any other component or device connected to the CDE (such as web redirection servers)

Agencies and Departments

Unless previously agreed to by CCD, all CCD Agencies and departments with PCI system components must comply with this policy. See scope section on page 5 for the agreed-to exceptions.

TECHNOLOGY SERVICES

Technology Services operates the majority of the technology that is utilized to deliver the PCI capability for CCD. However, several Agencies and departments retain staff to implement and/or operate components of their PCI technologies.

Throughout this document, references to the Technology Services Agency may be used to represent personnel in other Agencies when referring to their responsibilities around PCI compliance.

Additionally, there are many policies and procedures that pertain to technologies being utilized by CCD. Should a conflict arise between such policies and this document that is directly related to PCI system components or processes, this document shall supersede all others.

Adherence to Active PCI-DSS Requirements

1. Install and maintain a firewall configuration to protect cardholder data

1.1. PCI Change Control

All proposed software, hardware, and integration changes to the PCI system components must follow the change control policy and process prior to implementation of changes to any of the system components (*see* Policy – Change Management *and* Process – Change Management for complete change control requirements). The change control policy and process must adhere to the following minimum requirements.

1.1.1. Change Request Submittal

The party responsible for implementing the change must complete a Change Request in the Change Request system. All changes to PCI system components must comprise of the following:

- **Impact Documentation** – The impact of the change must be documented in order for all affected parties (internal and external) to have the ability to plan accordingly for any processing changes. Specifically, all systems, users and resources affected by the change must be documented, and the criticality of the change must be rated on a scale from low to high.
- **Test/Development Environment Verification** – The change request should contain details that exhibit that the change was successfully implemented in the test/development environment, and should contain details specific to the person implementing the change, and the time the changes were made.
- **Test Plan** – A set of planned tests must be developed to verify that the change meets the business requirements driving the need for change, and does not adversely affect other system components, or create a weakness in the security posture of the environment.
- **Back-Out Plan** – If the change does not go as planned, there must be a plan that describes the process for restoring the environment to its original state/configuration. This plan, referred to as a "back-out plan", must be completed **prior** to any implementation of changes.

- **Resources for Implementation** – The change request must outline which resources (by name) will be responsible for making the changes to the development, test/quality assurance, and production environments, and the anticipated time for implementation of the change.
- **Information Security Function Approval** – All changes must include the requirement for approval by the TS Information Security department.
- **Management Approval** – All changes must include management approval. This approval cannot be from a resource directly involved in implementing the change (separation of duties). For the purposes of this policy, management is defined as a business stakeholder or project lead with decision-making authority regarding the implementation of the change. Management must verify that the change request is complete and includes the information above prior to closing the change request. Additionally, management is responsible for maintaining a record of compliant change control documentation.

If the change involves the introduction of a change to software, or the introduction of new software to the environment, and the agency or department does not have adequate staffing levels to enforce separation of duties between test and production implementations, the agency or department must document the following:

- **Software Review and Approval** – New software or changes to existing software must be verified for compliance with all software development practices outlined in this policy.
- **Post-Deployment Documentation** – Upon the successful deployment of changes to the production environment, change control documentation must be updated.

1.1.2. Change Request Approval

Upon successful implementation of the change, management must document that the change was compliant with PCI change control requirements. This documentation must include electronic approval of completeness.

1.1.3. Change Testing

Prior to implementation in the production environment of the CDE, all changes must be tested on a QA or test network isolated from the production environment. The only exception to this is for the implementation of critical system patches provided by an appropriate vendor.

Testing of PCI application system components must include the following validation points:

- Validation of input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)
- Validation of proper error handling
- Validation of secure cryptographic storage
- Validation of secure communications
- Validation of proper role-based access control (RBAC)

NOTE: Production data (live primary account numbers (PANs)) are **not** to be used for testing or development. Only test account numbers can be used for this purpose (PCI DSS 6.4.3)

1.1.4. Change Implementation

All changes must be implemented according to documented change control procedures. Any discrepancies between expected results and actual results that impact the network, systems, applications, security, business requirements, or support procedures must result in the immediate invocation of documented back-out procedures.

1.1.5. Change Documentation and Archiving

Management is responsible for maintaining a documented history of all change requests to the PCI system components. This documentation must include the following:

- Original change request
- Approval for migration to production
- Documentation of testing results
- Documentation of change acceptance from the business stakeholders

1.2. Operational Support of PCI System Components

Maintenance and ongoing support of PCI system components will be performed in a manner that is documented, repeatable, and will incorporate industry or CCD best practices that are relevant to business needs. While each department or Agency may utilize their own policies or procedures for maintenance and ongoing support of PCI system components, such policies or procedures must incorporate the following minimum requirements.

1.2.1. PCI Network Services

a. *Allowed Services*

Only services specifically required to support the PCI system components are allowed access to PCI connectivity paths and services. All other services will be blocked or otherwise disabled. Information Security may be asked to utilize firewall configuration to augment the blocking of such services.

b. *Allowed Network Connection Paths and Configuration Requirements*

A firewall or compensating control mechanism that restricts connectivity must be configured between any demilitarized zone (DMZ) or wireless network and the PCI system components. This ensures that the connection paths for PCI system components are restricted.

Additionally, inbound traffic to PCI system components that is Internet-based is only permitted into a firewall-segmented DMZ.

In all cases, traffic should be limited to only those protocols necessary to meet CCD business requirements. Perimeter routers should not be configured with a route to internal address spaces of the PCI system components, with the exception of the DMZ.

For PCI system components, internal IP addresses must be hidden utilizing Network Address Translation (NAT) and Port Address Translation (PAT) when they are required to be exposed to the Internet.

Anti-spoofing technologies must be configured on perimeter devices, denying or rejecting all traffic with a:

- Source IP address matching internally allocated or CCD owned address space.
- Source IP address matching RFC 1918 address space.
- Destination IP address matching RFC 1918 address space.

Outbound traffic from internal production PCI system components must only be allowed to egress through either the DMZ or some other mechanism that restricts and logs outbound traffic. Additionally, this traffic should be restricted to only required protocols and services.

The use of a stateful packet inspection firewall or other compensating control mechanism must be utilized for Internet and wireless segmentation to only allow established connections into or out of network portions of the PCI system components.

c. Configuration Review

At least every six months, the Network Services team must thoroughly review each firewall and router rule set that have PCI system components and record and distribute results of the review to the Information Security function. The review must include the removal, when merited, of unused or unnecessary access paths. All proposed changes identified as a result of this review must be performed in accordance with existing change control policies, and must be approved by the Information Security team prior to implementation.

d. Host Based/Personal Firewalls

All PCI system components with direct connectivity to the Internet (e.g. computers used by cashiers) must have personal firewall and anti-virus software installed and activated. All such software must have non-user alterable configurations. Additionally, all PCI system components, where technically possible, must have restricted Internet browsing privileges, enforced by technical controls that allow access only to Internet sites that participate in the business process of that PCI system component, or are otherwise specified by the organization as being required to perform the role of the individual utilizing the workstation.

Modifications to any PCI system component settings for firewalls, anti-virus, or Internet browsing require approval of the Information Security team prior to implementation.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1. System Utilization

All PCI system components should be designated for a single primary purpose where possible (e.g. web servers, database servers, and DNS should be implemented on separate servers).

2.2. System Configuration Standards

All PCI system components, prior to deployment in the production environment, must conform to available system configuration standards provided by the vendor and approved by the Information Security team.

2.3. System Configuration Process

All new PCI system deployments will follow this high-level procedure:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters and secure the system according to available build documentation provided by the vendor.
4. Install applications and software:
   a. Install system-specific applications and software according to vendor-provided documentation.
   b. Install any additional applications and software necessary for the system's purpose.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to vendor-provided documentation.
7. Enable logging.
8. Ensure that all vendor-supplied defaults are changed before the system goes into production. For example, change all default passwords and Simple Network Management Protocol (SNMP) community strings, and eliminate all unnecessary accounts.
9. Enable only necessary and secure services as required for the system to function. NetBIOS, FTP and TELNET are **never** to be used for PCI system components, or if they are required, are enabled only after documenting the justification for their use and submitting the justification to the Information Security team for approval.
10. Ensure that systems and devices are configured to automatically terminate sessions after a period of fifteen minutes of inactivity.

3. Protect Stored Cardholder Data

3.1. Cardholder Data

In order to reduce the complexity of the PCI environment, CCD policy prohibits the storing of the following payment card information in its environment:

- The Primary Account Number (PAN)
- Complete magnetic stripe data
- CVV2/CVC2/CID data
- The Personal Identification Number (PIN)

If an Agency requires payment card information to be stored in the CCD environment, a request must be made for an exception by submitting a ticket to the Problem Management System utilized by CCD. This request will be reviewed by the Chief Information Security Officer (CISO) or the designee.

Additionally, transmission of cardholder data via end-user messaging technologies (e-mail, SMS, chat) is prohibited. Copying, moving, or storing cardholder data onto local hard drives and removable electronic media is prohibited.

3.2. PCI Data and Information

PCI data and information will be handled according to the Data Classification and Handling Policy.

3.3. Cardholder Data Processing Applications

All CCD applications dealing with the processing or retrieval of cardholder data must, where there is not a business need to display full PAN, mask PANs to no more than the first six (6) or the last four (4) digits of the full PAN.

As CCD, by policy, does not store sensitive cardholder data, including PAN, this specification is required only by exception.

3.4. Cardholder Data Storage Applications

All CCD applications performing storage of cardholder data must be configured in a manner which does not retain sensitive cardholder data such as full track data, card-validation codes, card not present values, PINs or PIN blocks.

Any instances of stored PANs must be rendered unreadable through one of the following:

- Strong one-way hash functions (hashed indexes) such as SHA-1 with salts
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures

In particular, the PAN must never be stored in clear text in databases, or removable media (such as backup tapes). The PAN must not be written to audit logs. If cardholder data is ever received from wireless networks, it must be rendered unreadable wherever stored.

As CCD, by policy, does not store sensitive cardholder data, including PAN, this specification is required only by exception.

3.5. Third Parties and Third Party Agreements

3.5.1. Third-Party PCI Requirements for The City and County of Denver

CCD shall Maintain a list of payment service providers including a description of the service provided.

All third parties with whom cardholder data is entrusted are contractually required to acknowledge that they are responsible for the security of cardholder data they maintain or process for CCD. In addition, the following must be verified:

- All specifications required of vendors or third-party entities described in the General Roles and Responsibilities section of this document must be met or exceeded.
- Before engaging any third-parties, proper due diligence must be performed to make sure that the entity follows all the PCI requirements applicable to the services they provide. This will be accomplished in the following way:

- If the third-party is listed on the Visa or PCI Security Standards website as a compliant service provider, it should be verified that the approval was granted for the proposed service the third-party is offering to provide.

4. Encrypt transmission of cardholder data across open, public networks

4.1. Wireless Monitoring

The City does not allow wireless technology in its CDE. To ensure that this policy is enforced, continuous monitoring for rogue wireless signals must be conducted. Unauthorized wireless broadcasting of the payment network shall be immediately terminated.

4.2. Transmission Encryption

Transmission of cardholder data over open, public networks (such as internet) must use strong cryptography and security protocols. Additionally, the following are required:

- The acceptance of only trusted keys and certificates
- The use of only secure versions or configurations of a given encryption protocol
- The use of strong algorithms, ciphers and key lengths in encryption

5. Protect all systems against malware and regularly update anti-virus software or programs

5.1. Anti-Virus Software

All servers, workstations, and laptops at CCD must have anti-virus software installed and activated. Definitions must be updated regularly, based on software vendor recommendations, and devices must be scanned regularly to ensure that updated definitions are installed on all servers, workstations and laptops.

Anti-virus software must also be configured on all servers, workstations and laptops to prevent tampering and/or disabling by end users.

6. Develop and maintain secure systems and applications

6.1. Vulnerability Management

Members of the organization that support technologies utilized in the PCI ecosystem must be informed of information security issues and vulnerabilities applicable to PCI system components.

The City and County of Denver has specified that members of the organization that have responsibility for ongoing support of these components comply with the Vulnerability Management Policy, which ensures personnel are able to stay abreast of vulnerabilities that impact PCI system components, as well as other non-PCI related systems. This policy contains information pertaining to malware, and patching.

6.1.1. Vulnerability Scanning

On a quarterly basis, internal and external vulnerability scans must be performed on the CDE. Internal scans must be performed by the Information Security team. The Information Security team will save the internal scan reports on a monthly basis and have the most recent 12 months' reports

available, ensuring that there is no gap between scan reports greater than 90 days. External scans must be performed by an Approved Scanning Vendor (ASV) that has been approved by the PCI Security Standards Council (PCI SSC). Upon completion of the scan, all identified vulnerabilities should be remediated according to the applicable regulatory requirements.

6.2. Software Development for the PCI System Components

6.2.1. Development Environment

A test/development environment, separate from the production environment, must be used to test all new software, with the exception of patches identified as "critical" as outlined in the Vulnerability Management policy.

If resourcing levels of the department or agency performing software development allow, separation of duties between personnel assigned to the test/development environments and those assigned to the production environment must be observed. If the resourcing levels of the department or agency do not allow for separation of duties between test/development and production, change control mechanisms must include a review of the software by a party different than the developers prior to moving the software to the production environment.

Production data (real credit card numbers) will not be used for testing and development purposes. Personnel should make every effort to use mock data for testing on non-production systems and software. Test credit cards can be obtained for this purpose by contacting the Information Security team.

All test data and test accounts must be removed before a system goes into production. Similarly, all test custom application accounts, test user IDs and test passwords must be removed before an application goes into production or is released to end users.

6.2.2. Secure Software Development

PCI software development must occur under the guidelines of the Vulnerability Management Policy. At a minimum, development of payment application software must include means of preventing the following vulnerabilities:

- Injection flaws, particularly SQL injection
- Buffer overflow
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- Any "high" vulnerabilities as defined by PCI-DSS requirement 6.2
- Cross-site scripting (XSS)
- Improper access control, such as insecure direct object references, failure to restrict URL access, or directory traversal
- Cross-site Request Forgery (CSRF)

6.2.3. Developer Training

Developers of payment applications must receive training in secure coding practices upon hire. CCD does not develop our own payment applications but may develop customizations, reporting, configuration changes, or interfaces for payment applications. Additional recurring training should occur as coding vulnerabilities are identified by industry-accepted vulnerability management services (i.e. Center for Internet Security).

7. Restrict access to cardholder data by business need to know

7.1. Approval to Use PCI User Devices

Departments or agencies utilizing existing PCI user devices are responsible for approving the granting and revoking of permissions to users for these technologies. Technology Services or the responsible technology department will not allocate permissions to users for PCI user devices without prior documented approval of the business manager for the department or agency.

The approval of a manager must be documented, with record of the approval being kept until the system is retired.

7.2. Authentication of PCI User Devices

User authentication mechanisms on PCI user devices, where possible, must be integrated into the current CCD authentication systems. The user authentication requirements cannot be configured to be less strict than the specifications currently defined in the Network Admin Policy.

7.3. Third-Party Provider Access to PCI Systems

As with all access to the CDE, access to systems within the CDE by third-party providers must be strictly controlled. At a minimum, the following must be ensured:

- Access shall only be granted after a valid business need has been demonstrated
- Access shall be granted only for the duration necessary to complete required work
- Should permanent access be required, a third-party representative shall be designated to monitor access lists and ensure that employee terminations are immediately communicated to CCD

8. Identify and authenticate access to system components

8.1. Logical Access

Logical access to the CDE is controlled via two means: the City's directory services tool (network access), and the access control mechanisms of the payment application(s) itself (application access). Access to the CDE shall be limited to individuals who require access to perform their job duties. Each account created for the purpose of access to the CDE must comply with the following:

- Network access must follow the Network and Email Account Management policy and its associated process and standard.
- Application access must be approved by the application owner.
- Each user must have a unique ID; generic accounts cannot be used to grant application access. In certain cases, shared network accounts may be used in situations where requiring individual access to POS systems would create a significant hardship to the

business. However, these cases must be reviewed and approved by the Information Security team **prior** to creation.

- Access must be granted using the principle of "least privilege" – users can only be granted a level of access commensurate with their job responsibilities.
- Vendor accounts used for remote access must be disabled when not in use. This requirement does not apply to contractors who provide daily support.
- Vendor remote access must be monitored while being used.
- All accounts must be locked from use after six unsuccessful login attempts.
- Once an account is locked from use due to unsuccessful login attempts, it must remain locked for a minimum of 30 minutes, or until a system administrator resets the account.
- All new accounts must be assigned a temporary password that is unique to the user, and must include the requirement that the temporary password be changed after first use.
- Users requesting a reset of their password must be provided a temporary password that is unique to the user, and must include the requirement that the temporary password be changed after its first use.

9. Restrict Physical Access to Cardholder Data

As CCD, by policy, does not store sensitive cardholder data, including PAN, the following are the guidelines for general information security measures:

9.1. Employee Requirements

Employees and contractors of CCD, when accessing areas with PCI system components, must at all times, clearly display their ID badges. It is every employee's and contractor's responsibility to watch for individuals not displaying badges and attempting to access or attempting to utilize PCI system components.

9.2. Facilities

The Facilities department must limit access to the badge system that controls access to PCI system components.

The datacenter(s) that house PCI system components must have a Visitor Log in place. All visitors must sign the form, including:

- Their name
- Firm represented
- Employee authorizing physical access (escort)
- Time they completed the log entry

This log must be retained for at least three (3) months.

9.3. Badge Assignment Procedure

The Facilities department manages all aspects of the badge lifecycle at CCD in accordance with their documented policies and procedures.

9.4. Media Storage and Destruction

All PCI data is stored on discs and there is no tape storage. CCD utilizes a commercial backup solution and the data is encrypted using AES128. In addition, CCD uses a third party vendor to dispose of equipment. We obtain a certificate of destruction from the third party vendor upon disposal.

9.5. PCI User Devices

PCI User Devices are defined as being applicable to the technologies that are under the control of CCD personnel for the purposes of directly executing or managing payment transactions on PCI system components.

These technologies may include:

- Payment terminals
- Kiosks
- POS computing systems
- Handheld devices for credit card processing

9.5.1. PCI User Device Inventory

All approved PCI user devices must be tracked via a PCI user device inventory. Business managers are required to notify the Information Security team of any changes to their inventory by submitting a service ticket.

"Any changes" includes adding new devices, retiring existing devices, or in any way modifying the existing devices currently in use, to include taking the devices offline, changes requested to user internet browsing capability, or installation of any applications or plug-ins.

Technology Services employees will keep the inventory up-to-date based on the information received from the business managers via the submitted service ticket.

9.5.2. PCI User Device Identification

All approved PCI user devices must be labeled with the device owner (agency or departmental name), contact information and device purpose. Additionally, each PCI user device is to be assigned and maintain a static IP address.

9.5.3. PCI User Device Physical Inspection

Approved PCI user devices must be periodically inspected to detect tampering or substitution. This inspection will include examining the device for signs of tampering such as unexpected attachments or cables plugged into the device, missing or changed labels, broken or differently colored casing, or changes to external markings. The frequency of the inspections must be annually at a minimum and include at least ten percent of the sites that accept credit card payments

10. Track and monitor all access to network resources and cardholder data

10.1. PCI System Component Logging

10.1.1. Events Logged

Automated audit trails must be implemented for all PCI system components to reconstruct the following events:

- All user access to cardholder data
- All administrative actions utilizing user IDs with significant privileges above a general user (e.g. root, user IDs with administrator group privilege, etc.)
- Access to audit log files
- Any user or administrator authentication attempts (both valid and invalid)
- Identification and authentication mechanism used
- Creation or deletion of system-level objects (e.g. executables, libraries, configuration files, drivers, etc.)
- Initialization of audit log files
- All security events

10.1.2. Event Log Structure

All system access event logs must contain at least the following information:

- User identification
- Type of event
- Date and time of event
- Result of the event
- Originating location of the event
- The name of the affected data, system component, or resource

10.1.3. Log Review

Logs of PCI system components must be reviewed daily, through either manual means or via the use of a log analysis tool.

10.1.4. Log Security

All event logs must be collected in a centralized location or media that is protected from unauthorized access and difficult to alter via access control mechanisms, physical segregation, and/or network segregation. The viewing of such logs is to occur on a need-only basis.

The logs will be further protected by a file integrity monitoring (FIM) system or a change-detection software that alerts the department responsible for the technical support of the respective PCI system components upon unauthorized access or if existing log data is changed.

Logs for external-facing technologies must be copied onto a log server on the internal LAN.

10.1.5. Log Retention

All logs collected in a centralized location or media that is protected from unauthorized access and difficult to alter via access control mechanisms, physical segregation, and/or network segregation are to be retained for one year, with three months actively able to be reviewed.

10.1.6. Network Time Protocol (NTP)

With the exception of the internal CCD NTP servers, all CCD PCI system components must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment.

11. Regularly test security systems and processes.

11.1. Penetration Testing

An internal and external penetration test must be conducted on an annual basis. Internal penetration testing may be conducted by the Information Security team. External penetration testing must be conducted by the City's testing vendor. All penetration testing activities must follow industry standards, and at a minimum must include the following:

- Testing is based on industry-accepted penetration testing approaches.
- Testing includes coverage for the entire CDE perimeter and critical systems.
- Testing takes place from both inside and outside the network.
- Testing includes validation of any segmentation and scope reduction controls.
- Testing defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed by PCI-DSS.
- Testing defines network-layer penetration tests to include components that support network functions as well as operating systems.
- Testing includes review and consideration of threats and vulnerabilities in the last 12 months.
- Testing results and remediation activities results are retained for a minimum of 12 months or until the following Report of Compliance (ROC) is obtained, whichever is greater.

11.2. Intrusion Detection and Prevention

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed at the ingress/egress point to City networks. Specifically, any access from City networks to the CDE is interrogated by the IDS/IPS. IDS/IPS logs are forwarded to the City's SIEM tool for analysis, correlation and alerting (when applicable).

11.3. File Integrity Monitoring (FIM)

For systems storing or processing PCI data, CCD utilizes FIM software to alert personnel to unauthorized modification of critical system files (e.g. system and application executables), configuration and parameter files, and security logs.

VPN Client and Host-based/Personal Firewall Software:

All computers and laptops used for remote access to the CDE via the Internet must have the following software configured, enabled, and up-to-date with the latest vendor-provided signatures:

- Personal Firewall software
- Anti-virus software

Additionally, any software utilized by a CCD agency or department to access the environment (e.g. VPN clients), will be required.

Vendors responsible for the ongoing support of any PCI component at CCD are responsible for adhering to standards and practices that will not violate PCI-DSS or PA-DSS guidelines.

11.4. PCI Information Security Incidents

Responses to a PCI information security incident or suspected incident must take place immediately and must follow the Information Security Incident Response process.

11.4.1. Response to Information Security Incidents

Should it be determined that an information security incident has resulted in the loss of credit card information, the following additional steps must be done in accordance with PCI-DSS and payment card brand requirements:

- Notification must be made to the payment card brand(s) affected by the data breach. TS shall notify the Cash, Risk and Capital Funding group, who will notify the payment card brand(s).
- Additional requirements of the payment card brand(s) affected by the data breach must be followed, if applicable (see Information Security Incident Response process).

Additionally, Information Security personnel must be available 24/7/365 to respond to information security incidents and for ongoing monitoring of the CDE.

11.4.2. Incident Response Training, Testing and Updates

To ensure the City's ability to respond to information security incidents remains at its highest level:

- Information Security personnel must receive annual training on emerging threats and/or new techniques for incident response.
- The Information Security Incident Response process must be tested annually. Responses to an actual incident may be substituted for a test, provided the post-response activities include lessons learned that are incorporated into the existing process.
- The Information Security Incident Response process must be reviewed and/or updated annually, at a minimum. The review process must include the incorporation of relevant industry developments which will increase the City's security posture.

12. General Roles and Responsibilities

12.1. Information Security

The Information Security team is responsible for coordinating and overseeing enterprise-wide definition of policies and procedures regarding the confidentiality, integrity and availability of its information assets.

The Information Security function works closely with TS managers and staff involved in securing the company's information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed.

Specific responsibilities of the Information Security team include:

- With approval of the Chief Information Security Officer (CISO), make high-level decisions pertaining to the PCI Security Policy.
- Approve exceptions to these policies on a case-by-case basis.
- On an annual basis, or upon significant changes to the environment, coordinate a risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- Coordinate the annual review of PCI and Information Security policies and procedures.
- Ensure that third-parties, with whom cardholder data is shared, are contractually required to adhere to the PCI-DSS and/or PA-DSS requirements and to acknowledge that they are responsible for the security of the cardholder data which they process.
- Monitor third-party access to the CDE and ensure that access is removed when necessary.
- Ensure that any incident response plans or procedures are updated and distributed to the appropriate audiences.
- Assure that security rules applied to the firewalls and routers are sufficient to prevent internal security events from breaching the PCI system components.
- Assure that security rules applied to the firewalls and routers are sufficient to protect CCD PCI system components from external attacks and unauthorized access.
- Ensure that all protocols/services allowed through the firewalls and routers are properly documented.
- Ensure risky protocols, such as FTP and TELNET, have undergone a risk assessment, have a current documented business need, and are secured in alignment with industry best practices. For the PCI environment, these protocols must not be used or must be encrypted via SSH or other technology.
- Mature the information security practices at the City and County of Denver.
- Adhere to all information security policies.

12.2. Technology Services Department

The Technology Services Department is charged with successfully securing supported CCD PCI resources and systems.

The Technology Services Department works with departmental system managers, administrators and users to develop security policies, standards, and procedures that will help to protect the assets of CCD PCI resources.

Specific responsibilities of the Technology Services Department include:

- Recommend the creation of new information security policies and craft new information security procedures, as needed.
- Maintain and actively communicate existing information security policies and procedures.
- Adhere to all information security policies.
- Act as a central coordinating department for implementation of the PCI Security Policy.
- Create, maintain, and distribute departmental incident response and escalation procedures.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Review security logs daily. Follow-up on any exceptions identified.
- Restrict and monitor access to sensitive areas. Ensure appropriate physical controls are in place where cardholder information is present.
- Ensure that users and administrators working in the CDE complete annual security awareness training that includes an acknowledgement of understanding of the PCI Security Policy.
- Ensure that anti-virus software and definitions are updated regularly, based on the software vendors' recommendations.

12.3. PCI System Administrators

CCD System Administrators are the direct link between information security policies and the network, systems and data. System Administrator responsibilities include:

- Applying CCD PCI security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Supporting other areas of Technology Services with monitoring and controlling all access to CCD data.
- Maintain an up-to-date network diagram, including wireless networks. The diagram must include the date when it was last updated and the name of the employee who performed the update. The diagram should also conform to guidelines provided by the assigned QSA.
- Restrict physical access to PCI system components.
- Adhere to all information security policies.

12.4. Network Security Administrators

CCD Network Administrators provide the first and best line of defense for PCI system components. As such, Network Administrators must:

- Assure that changes to hardware, software, and security rules of firewalls and routers that are PCI system components are approved by Technology Services or the appropriate management personnel for the agency or department and that all change control processes are followed for the change.

- Document all firewall and router security rule changes to PCI system components.
- Following every change, review and update network diagrams to ensure they accurately describe all connections to PCI system components.
- Enable appropriate logging on all security systems and perform active daily monitoring of the logs that report security events.
- Provide designated members of the Network Services team with read-only access to security event logs.
- Report out-of-pattern network security incidents to the Information Security team to address security events.
- Coordinate an appropriate response with the Information Security team to address security events.
- Ensure that router configuration files are secured and synchronized properly.
- Monitor system and application-specific alerts on critical systems (e.g. interface up/down, firewall daemon failing, system reboots, etc.).
- Actively monitor firewall and router security events to identify internal or external security incidents.
- Conduct review of all firewall and router rule sets every six months.
- Request approval from the Information Security function prior to the implementation of any PCI system component change.

12.5. Users

Each user of CCD computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all CCD information system users:

- Understand the consequences of their actions are with regard to computing security practices and act accordingly. Embrace the "Security is everyone's responsibility" philosophy to assist CCD in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Notify Technology Services personnel of all suspected violations of any approved policy or procedure.
- Provide subject matter expertise pertaining to the classification of data at CCD.
- Adhere to all information security policies.
- Seek clarification from the policy owner or appropriate governing body (e.g. Office of the CIO or CISO) if the appropriate behavior is unknown or unclear, prior to performing any activities under the scope of this policy.
- Notify direct supervisor immediately of any violations of approved policies and/or procedures, suspected credit card theft, misuse, or fraud incidents.

12.6. CCD Agencies w/POS Presence

CCD departments/agencies whose sales and payment information are collected electronically and/or manually have the following responsibilities:

- Adhere to the PCI-DSS requirements and agree to a quarterly network scan for all externally-facing IP addresses.
- Adhere to all City policies, procedures and guidelines related to payment card acceptance and processing.
- Follow all appropriate processes to notify Cash, Risk & Capital Funding (CRCF) and Technology Services to request new, removals, or changes to existing, payment card acceptance methods related to POS systems, merchant IDs physical terminal location moves, or related functionality.
- Review and resolve any disputes between the customer and their credit card merchant account in a timely manner.
- When a department/agency reports a problem with their front-end application, they will submit a service ticket to report the problem.
- Limit physical and electronic access to computing resources and cardholder information only to those individuals whose job requires such access.
- Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and assignment of privileges to individuals based on job classification and function.
- For all systems that participate in a PCI solution, verify a unique logon ID is being used by each user and that a default password is never used.
- For each level of access (i.e. transaction processing, refunding, and administration) continually ensure staff members are signing on to the solution to verify that authentication is functioning consistent with documented processes (for example, verify that each user must enter their user ID and password to gain access to the system).
- Verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.
- Ensure that POS terminals are physically secured when not in use. Ensure that all staff members are trained on terminal use, and how to identify signs of tampering. Verify that paper and electronic media containing full debit/credit card numbers are stored in a secure location (locked filing cabinet or office, secure filing room).
- Departments/agencies are responsible for reconciling transactions and submitting entries to the City's financial system.
- Departments/agencies are responsible for approving all change control documentation for changes they submit.
- Adhere to all information security policies.
- Notify Technology Services immediately of any violations of approved policies and/or procedures, suspected credit card theft, misuse, or fraud incidents.

12.7. Vendor and Third-Party Entities

Vendors and third-party entities who offer a commodity or service, whose prices are competitive, and whose services are reliable, are encouraged to pursue opportunities to do business with the City. The City and County of Denver is continuously searching for responsible sources to supply the City's broad range of needs. For PCI offerings, vendors and third-parties must:

- Prove initial and continued compliance with PCI-DSS requirements and PA-DSS validation, where identified as needed by Technology Services and Treasury.
- Provide a PA-DSS implementation guide specific to each payment application under the contracted services.
- Vendors and third-party service providers have the ultimate responsibility for defining the scope of their PCI security scan.
- Demonstrate adherence to the Denver Revised Municipal Code provisions regarding the ownership of payment card funds.
- Sign a third-party agreement that clearly specifies and assigns payment card liabilities.
- In the event that the vendor or third-party entity will be making any changes to their method of processing after the vendor or third-party has been initially set up, all changes must be approved by the Treasury Division before putting into production.
- Demonstrate the ability to protect confidential information, including identifying the encryption strength utilized by their proposed solution.
- Adhere to all information security policies.
- Notify Technology Services immediately of any violations of approved policies and/or procedures, suspected credit card theft, misuse, or fraud incidents.

13. Non-Compliance

13.1. General Non-Compliance

All perceived non-compliance with City and County of Denver policies carry the potential for penalty, including (without limitation): loss of technology privileges, civil or criminal litigation, contract termination or human resource action.

13.2. Reporting of Suspected Non-Compliance

All violations of this policy must be reported to the policy owner, regardless of the perceived repercussions to the suspected violator. All violations reported in good faith will be handled without reprisal.

Revision History

Date	Modified By	Revision Comments
11/1/2014	Alena Gouveia, IT Governance Manager	Created from existing documentation; placed in new format
10/22/2015	Alena Gouveia, IT Governance Manager	Updated to include 3.1 requirements
12/17/2015	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
12/22/2015	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
12/28/2015	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
1/14/2016	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
1/15/2016	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
2/9/2016	Alena Gouveia, IT Governance Manager	Updated to include additional 3.1 requirements
3/24/2016	Tricia Scherer, Business Process Analyst	Updated to include additional 3.1 requirements from sections 9.9.2a and 12.3.10a
4/8/2016	Tricia Scherer, Business Process Analyst	Updated to include additional 3.1 requirements from sections 9.7 and 9.8
1/18/2017	Samantha Shih, IT Compliance Analyst	Reviewed the entire PCI Policy with the Information Security team for currency
1/22/2017	Tricia Scherer, IT Governance Manager	Re-ordered the sections to more closely align with the order of PCI-DSS 3.2
2/15/2017	Stephen Coury, Chief Information Security Officer	Reviewed and commented on the PCI Policy
2/17/2017	Tricia Scherer, IT Governance Manager	Minor changes based on review by CISO
2/21/2017	Tricia Scherer, IT Governance Manager	Clarified scope section for DEN, District Attorney's Office, County Courts and Denver Public Library
5/15/2017	Tricia Scherer, IT Governance Manager	Updated section 6 to include saving monthly internal vulnerability scan reports

Signature

X

Scott Cardenas
Chief Information Officer

Policy Control Information	
Division	Information Security
Team	Information Security
Referenced Policy	System Hardening Data Backup
Related Process	Information Security Incident Response Process
Effective Date	11/01/2017

Purpose

The purpose of this policy is to ensure Technology Services (TS) has an incident response plan in place to manage information security incidents. This policy establishes requirements for TS to plan detect, contain, remediate and recover from information security incidents.

Regulatory Guidance

This policy is intended to align with the following regulations and industry standards:

Regulations and Industry Standards	
PCI - DSS	Payment Card Industry Data Security Standard
CSA CCM	Cloud Security Alliance - Cloud Controls Matrix
CJIS	Criminal Justice Information Services
CSC	Critical Security Controls from Center for Internet Security
NIST	National Institute of Standards and Technology – Computer Security Incident Handling Guide

Scope

This policy applies to all TS employees (including Career Service Authority and Non-Career Service Authority employees, appointees, and elected officials), contract employees and contingent workers who manage, maintain or support TS supplied products and services.

Executive Sponsorship

Executive sponsorship for this document comes from the CIO, City and County of Denver (CCD). The CIO shall review this policy periodically with senior management to determine if changes to this policy are required.

Policy

1. Incident Response Preparation

Incident response preparation should include the following actions:

- Harden all systems and networks according to “System Hardening” Policy and Standards.
- Establish and implement data backup according to “Data Backup” Policy and Standards.

- Define reportable incidents -
  A security incident may involve any or all of the following:
  - Violation of computer security policies and standards
  - Unauthorized computer or data access
  - Presence of a malicious application, such as a virus
  - Presence of unexpected/unusual programs
  - Denial of service condition against data, network or computer
  - Misuse of service, systems or information
  - Physical or logical damage to systems
  - Computer theft
- Describe incident response roles and responsibilities:
  All users who are given access to TS owned/managed systems, networks, and facilities are responsible for reporting any actual or potential breach of information security promptly in line with the incident management process.
  Security Operation Center (SOC) is responsible for coordinating and handling security incidents, as well as documenting and analyzing root causes.
- Create and distribute written Incident Response Process.
- Provide incident response training to personnel with assigned security roles and responsibilities, prior to being assigned an incident response role/responsibility, or when required by information system changes.

2. Incident Detection and Identification

TS, wherever feasible, shall employee automated mechanism (ex: virus detection, intrusion detection, system/network audit logs) and other resources to timely detect information security incidents. Security alerts shall be monitored, analyzed, and distributed to appropriate personnel.

TS staff, contractors, vendors, and business partners, within eight hours of the identification of a suspected reportable incident, will notify the information security team. Business contractors and vendors, shall notify their TS point of contact.

TS shall identify and fulfill the reporting requirements from applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance, such as Health Insurance Portability and Accountability Act (HIPAA), Personal Identifiable Information (PII), and Criminal Justice Information System (CJIS).

3. Incident Handling and Recovery

TS shall handle the identified incident by:

- limiting the scope and magnitude of an incident (Containment).
- removing the root cause of the incident (Remediation)
- restoring impacted systems to the normal mission status (Recovery)

SOC shall ensure the incident handling activities are coordinated with contingent planning activities.

4. Incident Documentation and Follow-Up

All incidents shall be tracked and documented in the incident tracking tool. The minimum information that shall be recorded is:

- Date and time the incident was reported, discover or occurred
- Who reported or discovered the incident
- How the incident was identified
- Description of the incident
- Incident related tasks and who performed each, and amount of time spent on each task;
- Person coordinating the incident response
- Individuals contacted regarding the incident, and
- Information system(s), application(s), vendor(s), business partner(s), or network(s) impacted
- Lessons learned from the incidents handling activities shall be reviewed and incorporated into the incident handling procedures, when appropriate

In the event of legal action is involved, evidence shall be collected, retained, and presented to conform to the rules of evidence.

Policy Compliance

Compliance

- The Information Security team will verify compliance to this policy.

Exceptions

- Any exception to the policy must be approved and documented by the Information Security Team in advance. Exception will be reviewed annually.

Non-Compliance

- An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Incident – An incident is described as any violation of policy, law, or unacceptable act that involves information assets such as computers, networks, smartphones, etc.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Approval Information

Scott Cardenas

Chief Information Officer

Revision History

Date	Modified By	Revision Comments
9/26/2017	Samantha Shih, IT Compliance Analyst	Initial Creation
9/27/2017	Tricia Scherer, IT Governance Manager Todd Deering, Information Security Manager Samantha Shih, IT Compliance Analyst	Reviewed for currency and accuracy
9/28/2017	Julie Sutton, Information Security Manager	Reviewed for currency and accuracy