MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT ("Agreement") is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City") and **SCRIBSOFT HOLDINGS INC**., a North Carolina corporation, d/b/a Permitium LLC, registered to do business in Colorado, whose address is 10617 Southern loop Blvd, Pineville, North Carolina, 28134 ("Contractor"), individually a "Party" and jointly "the Parties."

RECITALS

WHEREAS, the City is desirous of engaging a hosted third-party solution provider to aid the City in the processing of conceal and carry weapons permits and the Contractor has agreed to provide the hosted solution, services and other deliverables under the terms and conditions as set out below; and

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

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 the City's Acceptance of a Deliverable, or the System. The 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. **"City Data"** means all information, whether in oral or written (including electronic) form, created by or in any way originating with the 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 the 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.

1.7. "**Confidential Information**" means 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, federal or state tax information ("Tax Information"), Criminal Justice 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 or 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.

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

1.9. **"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 the 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 the 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 City Data, or the ability of the City to access City Data.

1.10. **"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.

1.11. **"Documentation"** means, collectively: (a) all materials published or otherwise made available to the 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 the 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 the City or as required to be produced by Contractor subject to the terms of this Agreement.

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

1.13. **“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.

1.14. **“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 Contractor has elected to make generally available to its customers.

1.15. "**Equipmen**t" 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.

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

1.17. **“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.

1.18. "**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 the 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.

1.19. **“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.

1.20. **“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.

1.21. **“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.

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

1.23. **“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.

1.24. **“Services”** means Contractor’s computing solutions, provided to the 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.

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

1.26. "**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.

1.27. **"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.

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

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

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

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 the 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 the 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.

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.

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.

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:

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

4.4.2. 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.

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

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

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

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

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

4.4.8. 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.

4.4.9. 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.

4.4.10. 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:

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

4.6.2. 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;

4.6.3. 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. 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.

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

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

5.1.1. 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;

5.1.2. Consult with the City regarding its response;

5.1.3. 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

5.1.4. 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.

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.

7. <u>DATA RETENTION AND DISPOSAL</u>

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.

8. <u>DATA TRANSFER UPON TERMINATION OR EXPIRATION</u>

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. All services related to such transition shall be performed at no additional cost beyond what would be paid for the Services in this Agreement. 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.

9. SERVICE LEVEL AGREEMENTS; INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE. See Exhibit B.

10. COMPLIANCE WITH APPLICABLE LAWS AND CITY POLICIES.

10.1 Contractor will comply with all applicable laws 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.

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.

d. Notwithstanding the foregoing, Contractor's SaaS software in conjunction with City provided on premise support of in person processing, shall make said services accessible to all persons who are completing application on City premises.

10.3 **Criminal Justice Information Services (CJIS)**: As applicable, private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

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.

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.

13. <u>COLORADO OPEN RECORDS ACT</u>. 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.

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 Exhibits A and A-1 and perform the technology related services described on attached Exhibits A and A-1(the "Statement of Work" or "SOW").

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:

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

14.5.2. Account credential lifecycle management from instantiation through revocation;

14.5.3. Account credential and/or identity store minimization or re-use when feasible; and

14.5.4. 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.

15. <u>GRANT OF LICENSE; RESTRICTIONS</u>

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.

16. <u>DELIVERY AND ACCEPTANCE</u>

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.

17. <u>TERM</u>. The term of the Agreement is from April 1, 2021 through April 1, 2024 (the "Term"). The Parties agree that the Agreement may be renewed for an additional five (5) year term upon the same terms and conditions with an increase in no more than three percent (3%) of the cost for the renewal term. At the end of the initial Term the Parties shall adjust the pricing based upon the City's actual or anticipated usage.

18. <u>COMPENSATION AND PAYMENT</u>

18.1. Fee: The fee for the Services and any fees for credit card/banking services is described in the attached Exhibits A (the "Fee"). The Fee shall be retained by the Contractor. Any Fee for professional technology services payable to the Contractor shall be paid pursuant to the City's Prompt Payment Ordinance and in accordance.

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:

18.4.1. Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed **SIXTY THOUSAND DOLLARS** ($60,000.00) (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.

18.4.2. 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.

19. <u>STATUS OF CONTRACTOR</u>. 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.

20. <u>TERMINATION</u>

20.1. The City has the right to terminate the Agreement, or a product under the Agreement, with cause upon written notice effective immediately. City has the right to terminate without cause upon twenty (20) days prior written notice to Contractor, but no earlier than 30 days from "Go-Live" for the application. 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.

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.

22. WHEN RIGHTS AND REMEDIES NOT WAIVED. 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.

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 C, 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, Contractor's insurer shall waive subrogation rights against the City.

23.5. 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.

23.6. 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.

23.7. Commercial General Liability: Contractor shall maintain a Commercial General Liability insurance policy with limits of $6,000,000 for each occurrence, $6,000,000 for each personal and advertising injury claim, $6,000,000 products and completed operations aggregate, and $6,000,000 policy aggregate.

23.8. Business Automobile Liability: Contractor shall maintain Business Automobile Liability with limits of $1,000,000 combined single limit applicable to all owned, hired and non-owned vehicles used in performing services under this Agreement.

23.9. Technology Errors & Omissions: Contractor shall maintain Technology Errors and Omissions insurance including cyber liability, network security, privacy liability and product failure coverage with limits of $5,000,000 per occurrence and $5,000,000 policy aggregate.

23.10. Additional Provisions:

23.10.1. For Commercial General Liability, the policy must provide the following:

23.10.1.1. That this Agreement is an Insured contract under the policy;

23.10.1.2. Defense costs are outside the limits of liability;

23.10.1.3. A severability of interests or separation of insureds provision (no insured vs. insured exclusion); and

23.10.1.4. A provision that coverage is primary and non-contributory with other coverage or self-insurance maintained by the City.

23.10.2. For claims-made coverage:

23.10.2.1. The retroactive date must be on or before the Agreement date or the first date when any goods or services were provided to the City, whichever is earlier.

23.10.2.2. Contractor shall advise the City in the event any general aggregate or other aggregate limits are reduced below the required per occurrence limits. At their own expense, and where such general aggregate or other aggregate limits have been reduced below the required per occurrence limit, Contractor will procure such per occurrence limits and furnish a new certificate of insurance showing such coverage is in force.

24. DEFENSE AND INDEMNIFICATION

24.1. Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all 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.

24.2. 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.

24.3. 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.

24.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of Contractor under the terms of this indemnification obligation.

Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.

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

24.6. 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.

24.7 Notwithstanding the foregoing Permitium's maximum indemnification for IP claims, will be limited to the amount of insurance set forth within section 23.

25. 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).

26. 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.

27. ASSIGNMENT; SUBCONTRACTING. 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. Any assignment or subcontracting without such consent will be ineffective and void and shall be cause for termination of this Agreement by the City. The Manager has sole and absolute discretion whether to consent to any assignment or subcontracting, or to terminate the Agreement because of unauthorized assignment or subcontracting. In the event of any subcontracting or unauthorized assignment: (i) Contractor shall remain responsible to the City; and (ii) no contractual relationship shall be created between the City and any sub-consultant, Subcontractor or assign. Notwithstanding the foregoing, Permitium may (without the City's consent) assign this agreement and all of its rights, duties, interests and obligations hereunder to any entity into which it merges, has a change in control representing a conveyance of more than 50% of its ownership interests, or to which it sells all or substantially all of its assets. Permitium agrees to notify the client within 10 business days of any assignment.

28. 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.

29. 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.

30. 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.

31. 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.

32. CONFLICT OF INTEREST

32.1. 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.

32.2. Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the Agreement. 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 Contractor by placing Contractor's own interests, or the interests of any party with whom 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 Contractor written notice describing the conflict.

33. 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.

34. 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.

35. 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.

36. NO DISCRIMINATION IN EMPLOYMENT. In connection with the performance of work under this contract, Contractor may not refuse to hire, discharge, promote or demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, gender, age, military status, sexual orientation, gender identity or gender expression, marital status, or physical or mental disability. Contractor shall insert the foregoing provision in all subcontracts.

37. 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.

38. 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 validly and legally bind Contractor 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.

39. **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.

40. **ORDER OF PRECEDENCE**. In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.

41. **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.

42. **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.

43. **TIME IS OF THE ESSENCE**. The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.

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.

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

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.

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.

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.

49. **ADVERTISING AND PUBLIC DISCLOSURE**. Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of 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. 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.

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.

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.

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.

53. ON-CALL SERVICES. This Agreement or the SOW may contain hourly or daily rates and Contractor and the Manager may enter into work orders for ongoing 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.

54. PCI DSS COMPLIANCE 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.

ATTACHED EXHIBITS

EXHIBIT A – SERVICE/ STATEMENT OF WORK
EXHIBIT A-1-WORKFLOW
EXHIBIT B -SLA
EXHIBIT C - CERTIFICATE OF INSURANCE
APPENDIX H-CJIS

Contract Control Number: TECHS-202158235-00
Contractor Name: PERMITIUM, LLC.

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

SEAL

ATTEST:

____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: ________________________________

CITY AND COUNTY OF DENVER:

By: ________________________________

REGISTERED AND COUNTERSIGNED:

By: ________________________________

By: ________________________________

Contract Control Number: TECHS-202158235-00
Contractor Name: PERMITIUM, LLC.

DocuSigned by:

By: Matt Solomon

6E5552DFA724474...

Name: Matt Solomon
(please print)

Title: Partner
(please print)

ATTEST: [if required]

By: ____

Name: ____
(please print)

Title: ____
(please print)

STATEMENT OF WORK (SOW) – EXHIBIT A

Overview

The Denver Police Department's (DPD) Concealed Weapons Unit currently uses an access database backed up to MS OneDrive to manage and administer their concealed carry weapons permitting process. DPD has identified Permitium's PermitDirector as an online alternative solution that will reduce the current significant manual processes. PermitDirector automates workflow and legally required reporting procedures, as well as improves the data security and retention of this important data source. PermitDirector for weapon permits serves as an end-to-end online solution that includes the application, background check tracking, processing, payment and issuance of gun and concealed carry permits. This SOW describes the implementation process for the Permitium PermitDirector solution.

Implementation Plan

Permitium Responsibilities:

- Configure the initial instance of the new **Permitium** solution based on the Citys current pistol permit process and **Permitium's** demonstration site
- Refine the new **Permitium** solution through an iterative process based on input received from the City during the testing phase
- Test the **Permitium** solution, revise as needed and prepare it for production
- Provide training for the City as needed
- Provide ongoing support, hosting and management of the **Permitium** Solution

Implementation Team

Permitium	Support Team	855-712-PERM	support@permitium.com
Client	Main Contact	Daniel Everett	Daniel.everett@denvergov.org

Cost of Service

PERMITIUM CHARGE: Cost for **PermitDirector** software, implementation services or support – Permitium will charge

- _X__$4.00 administrative fee for all Concealed Weapon transactions.
- ____$250/month - Integration URL API – used to export data to external systems

THIRD PARTY CHARGES: Permitium will use their Merchant ID to receive online payments. Credit card merchant fees incurred by Permitium in the processing of City Customer payments will be retained by Permitium from on-line City Customer payment through Permitium. The current merchant fee rate is $.30 per transaction in addition to 2.9% of the total transaction cost. If City elects to offer some or all services for free, the $4.00 administrative fee will still apply and the City will be liable to pay Permitium .

In person cash transactions shall not incur fees.

Fee Collection and Payment- Permitium shall deliver the City a monthly statement which will itemize every transaction submitted the prior thirty days along with a check or ACH for the net total amount collected.

Change Orders

The City may at anytime during the term of this contract elect to add the URL / API services upon mutual agreement between both parties. This request shall be documented by Permitium.

EXHIBIT A-1
WORKFLOW

Denver Police Concealed Weapon Process Sequence

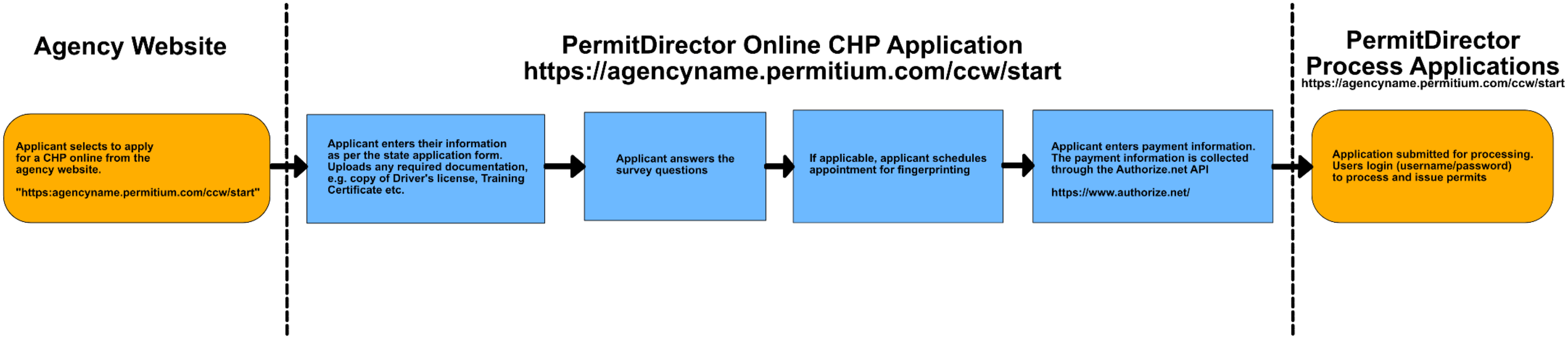
Proposed Process

1. Applicant visits Denvergov.org/police and navigates to the concealed weapon page to review requirements and select the link to apply online.
    - Once the link is clicked, the citizen is taken to the Permitium application process for Denver Police CCW. There they will complete the County Sheriffs of Colorado Concealed Handgun Permit Application electronically. They will also upload the following documents:
        - Alien Supplementary Questionary (if the applicant marks yes on question 14 on the application)
        - An original handgun training certificate
        - Colorado drivers license / military ID
        - Proof of Denver County Residency
    - Once all items are uploaded, the customer can select an in-person appointment for fingerprints and photographs.
    - The final step of the process is to provide payment through the Permitium application.
2. DPD will have access to the applications on the Permitium site. The items are reviewed by a DPD ASA to ensure all items are complete. If not, the customer will be contacted through Permitium to follow up on incomplete items.
3. At the time of the in-person appointment, the applicant's information is entered into Picture link and a case number is created. The applicant's information is also entered into the CCW database and Versadex (Permits and licensing) under the same case number. All files will remain in an open status until the background check is completed
4. At the date of the appointment the applicant completes the following DPD forms:
    - Non-Criminal Justice Application Privacy Screening
    - Authorization for Release of Information
    - Live Scan Fingerprint Form
5. The subject is photographed using Picturelink software
6. The subject is fingerprinted using Morpho Livescan software and equipment.
    - The fingerprints are transmitted electronically to the CBI for a fingerprint-based background check.
7. The complete file is forwarded to the CCW detective for review.
8. Once CBI returns the results of the background check the CCW detective reviews the background for disqualifying information.
    - If the background contains disqualifying or concerning information, it is sent to the manager of Identification for secondary review.
    - If the manager of Identification agrees with the Detective's assessment, the denial recommendation is sent to the Deputy Director of Safety who must officially deny the request.
    - Once an official denial is given, the Manager of Identification generates a denial letter with the disqualifying statute and the file is sent back to the Detective.
    - The CCW Detective marks the file and updates all three database systems that the permit is denied.

- The denied file is hand carried to the ID Bureau to be immediately scanned into Versadex by a CSA employee.
- The denial letter is mailed, and the file is closed.

9. If the application is approved, the CCW permit is issued and the card is mailed to the applicant.
    - All three databases are updated with the approval date and closed out.
        - RMS
        - CCW Access
        - CCW Permit Volume Sheet
    - The approved packet is taken to the ID Bureau and placed on the shelf to be scanned in.

Transaction Workflow



Agency Website

Applicant selects to apply for a CHP online from the agency website.

"https:agencyname.permitium.com/ccw/start"

PermitDirector Online CHP Application https://agencyname.permitium.com/ccw/start

Applicant enters their information as per the state application form. Uploads any required documentation, e.g. copy of Driver's license, Training Certificate etc.

Applicant answers the survey questions

If applicable, applicant schedules appointment for fingerprinting

Applicant enters payment information. The payment information is collected through the Authorize.net API

https://www.authorize.net/

PermitDirector Process Applications

https://agencyname.permitium.com/ccw/start

Application submitted for processing. Users login (username/password) to process and issue permits

Permitium

Empowering Government Agencies And Their Customers

Service Level Agreement

Introduction

This service level agreement (SLA) describes the levels of service that City and County of Denver(‘the client’) will receive from Permitium, LLC (‘Permitium’).

Purpose

The client depends on IT software and services (together: ‘the IT system’) that are provided, maintained and supported by Permitium. Some of these items are of critical importance to the business.

This service level agreement sets out what levels of availability and support the client is guaranteed to receive for specific parts of the IT system. It also explains what penalties will be applied to Permitium should it fail to meet these levels.

This SLA forms an important part of the contract between the client and Permitium. It aims to enable the two parties to work together effectively.

Scope

Dates and reviews

This agreement begins on _______________ and will run for the duration of the Master Agreement**.**

It may be reviewed at any point, by mutual agreement. It may also be reviewed if there are any changes to the client’s IT system.

Software and services covered

This SLA covers only the software and services in the table below. This list may be updated at any time, with agreement from both the client and Permitium.

Please note:

- Permitium guarantees **response times** for all items listed in this section.

- Permitium guarantees **uptime** only for items with a tick in the '**Covered for uptime?'** column.

These items have been assigned a priority level, from 1 (most important) to 3 (least important). The priority levels help determine the guaranteed uptime and response time.

Item type	**Number of items**	**Priority**	**Covered for uptime?**
PermitDirector for Gun Permits	1	1	yes
PermitDirector for Gun Permits CCW	1	1	yes
PermitDirector for Civil Process	1	1	yes
PermitDirector for Fingerprinting	1	1	yes
PermitDirector for Offender Tracker	1	1	yes
VitalDirector	1	1	yes
PermOnline	1	1	yes
Cloud Data Snapshots (15 minutes - 1 hour)	1	2	–
Permitium Reports	1	3	no

Exclusions

This SLA is written in a spirit of partnership. Permitium will always do everything possible to rectify every issue in a timely manner.

However, there are a few exclusions. This SLA does not apply to:

- Any equipment, software, services or other parts of the IT system not listed above

- Software, equipment or services not purchased via and managed by Permitium

Additionally, this SLA does not apply when:

- The problem has been caused by using equipment, software or service(s) in a way that is **not recommended.**
- The client has made **unauthorized changes** to the configuration or set up of affected equipment, software or services.
- The client has prevented Permitium from **performing required maintenance and update** tasks.
- The issue has been caused by **unsupported** equipment, software or other services.

This SLA does not apply in circumstances that could be reasonably said to be beyond Permitium' control. For instance: floods, war, acts of God and so on.

This SLA also does not apply if the client is in breach of its contract with Permitium for any reason.

Having said all that, Permitium, LLC aims to be helpful and accommodating at all times, and will do its absolute best to assist client wherever possible.

Responsibilities

Permitium responsibilities

Permitium will provide and maintain the IT system used by the client.

Additionally, Permitium will:

- Ensure relevant software, services and equipment are available to the client in line with the uptime levels listed below.
- Respond to support requests within the timescales listed below.
- Take steps to escalate and resolve issues in an appropriate, timely manner.
- Maintain good communication with the client at all times.

Client responsibilities

The client will use Permitium-provided IT system as intended.

The IT support contract between Permitium and the client includes full details of the IT system and its intended uses.

Additionally, the client will:

- Notify the client of issues or problems in a timely manner.

- Provide Permitium with access to equipment, software and services for the purposes of maintenance, updates and fault prevention.
- Maintain good communication with Permitium at all times.

Guaranteed uptime

Uptime levels

In order to enable the client to do business effectively, Permitium guarantees that certain items will be available for a certain percentage of time.

These uptime levels apply to items in the **Software and services covered** table that show a tick in the '**Covered for uptime?'** column.

The level of guaranteed uptime depends on the priority level of each item:

Priority level	Guaranteed uptime	Uptime Expectation
1	99.5%	99.9%
2	99.5%	99.9%
3	99%	99.9%

Measurement and penalties

Uptime is measured the using Permitium' automated systems, over each calendar quarter. It is calculated to the nearest minute, based on the number of minutes in the given month (for instance, a 31-day month contains 44,640 minutes).

If uptime for any item drops below the relevant threshold, a penalty will be applied in the form of a credit for the client.

This means the following month's fee payable by the client will be reduced on a sliding scale.

Priority level	Penalty
1	5% of total monthly conv fees collected
2	2% of total monthly conv fees collected
3	1% of total monthly conv fees collected

Important notes:

- Uptime penalties in any quarter are capped at 5% of the total monthly conv fee
- Uptime measurements exclude periods of routine maintenance. These periods include a daily window between 9:30 PM and 12:00 AM. All maintenance is kept to 2 minute intervals and are typically non-invasive.

Guaranteed response times

When the client raises a support issue with Permitium, Permitium promises to respond in a timely fashion.

Response times

The response time measures how long it takes Permitium to respond to a support request raised via Permitium' online support system.

Permitium is deemed to have responded when it has replied to the client's initial request. This may be in the form of an email or telephone call, to either provide a solution or request further information.

Guaranteed response times depend on the priority of the item(s) affected and the severity of the issue. They are shown in this table:

		Issue severity (see **Severity levels** section, below)			
		Fatal	Severe	Medium	Minor
Item priority	1	30 minutes	30 minutes	40 minutes	60 minutes
	2	30 minutes	30 minutes	45 minutes	60 minutes
	3	60 minutes	60 minutes	75 minutes	90 minutes

Response times are measured from the moment the client submits a support request via Permitium' online support system.

Response times apply during standard working hours (8am — 5pm) only, unless the contract between the client and Permitium specifically includes provisions for out of hours support.

Severity levels

The severity levels shown in the tables above are defined as follows:

- **Fatal:** Complete degradation — **all users and critical functions affected.** Item or service completely unavailable.
- **Severe:**Significant degradation — **large number of users or critical functions affected.**
- **Medium:** Limited degradation — **limited number of users or functions affected.** Business processes can continue.
- **Minor:** Small degradation **— few users or one user affected.** Business processes can continue.

Measurement and penalties

Response times are measured using Permitium support ticketing system, which tracks all issues from initial reporting to resolution. Response times will be calculated using an average of all the clients tickets for the quarter.

It is vital the client raises every issue via this system. If an issue is not raised in this way, the guaranteed response time does not apply to that issue.

If Permitium fails to meet a guaranteed response, a penalty will be applied in the form of a credit for the client.

This means the following month's fee payable by the client will be reduced on a sliding scale.

Priority level	Penalty
1	5% of total monthly conv fees collected
2	5% of total monthly conv fees collected
3	5% of total monthly conv fees collected

Important notes:

- Response time penalties in any quarter are capped at 5% of the total monthly conv fee
- Response times are measured during working hours (9am — 5pm).

  For instance, if an issue is reported at 5.00pm with a response time of 60 minutes, Permitium has until 10:00 AM the following day to respond.

Resolution times

Permitium will always endeavor to resolve problems as swiftly as possible. It recognizes that the client's computer systems are key to its business and that any downtime can cost money.

However, Permitium is unable to provide guaranteed resolution times. This is because the nature and causes of problems can vary enormously.

For instance, it may be possible to resolve a fatal server issue in minutes, simply by restarting a system. But if a system fails due to data center outages (also classed as a fatal issue) it may take much longer to get back up and running.

In all cases, Permitium will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the client.

Permitium Contact Type	Email	Phone	Skype
Client	support@permitium.com	(855) 712-PERM	permitium.support
Consumer	help@permitium.com	(855) 642-2453	

Right of termination

Permitium recognizes that it provides services that are critical to the client's business.

If Permitium consistently fails to meet the service levels described in this document, the client may terminate its entire contract with Permitium, with no penalty.

This right is available to the client **if Permitium fails to meet these service levels more than ten times in any single calendar month.**

Signatures

This service level agreement is agreed as part of the IT support contract between ______________________________ and Permitium, LLC:

Signed on behalf of the Client:

Signature: ____

Name: ____________________, Title: ___________________ Date: _________

Signed on behalf of Permitium:

Signature: ____

Name: ____________________, Partner Date: _________

Contact Phone: _______________

Contact Email: __________________________

DocuSign Envelope ID: 2DA2F808-F0A6-4622-A638-E43B9CDCA109

EXHIBIT C

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 12/18/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

Watson Insurance
245 East Second Avenue
PO Box 879
Gastonia NC 28053

CONTACT NAME: Lisa Francis

PHONE (A/C, No, Ext): 704-865-8584 FAX (A/C, No): 704-866-9866

E-MAIL ADDRESS: lfrancis@watsoninsurance.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Hartford Fire Insurance Company	19682
INSURER B : Twin City Fire Insurance Company	29459
INSURER C : Hartford Accident & Indemnity Company	22357
INSURER D :	
INSURER E :	
INSURER F :	

INSURED ADVA-18

Scribsoft Holdings Inc DBA Advanced Imaging Systems, Inc; Scribbles Software, LLC and Permitium, LLC
10617 Southern Loop Blvd
Pineville NC 28134

COVERAGES **CERTIFICATE NUMBER:** 759684583 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
B	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: ☐ POLICY ☐ PRO-JECT ☒ LOC OTHER:	Y		22SBAAB3386	10/1/2020	10/1/2021	EACH OCCURRENCE	$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
							GENERAL AGGREGATE	$ 2,000,000
							PRODUCTS - COMP/OP AGG	$ 2,000,000
								$
C	AUTOMOBILE LIABILITY ☒ ANY AUTO ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS ☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY	Y		22UECBH5283	10/1/2020	10/1/2021	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
B	☒ UMBRELLA LIAB ☒ OCCUR ☐ EXCESS LIAB ☐ CLAIMS-MADE ☐ DED ☒ RETENTION $ 10,000			22SBAAB3386	10/1/2020	10/1/2021	EACH OCCURRENCE	$ 6,000,000
							AGGREGATE	$ 6,000,000
								$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? ☐ (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					☐ PER STATUTE ☐ OTH-ER	
							E.L. EACH ACCIDENT	$
							E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$
A A	Cyber Liability Professional Liability (E & O)			22TE0325969 20 22TE0325969 20	10/1/2020 10/1/2020	10/1/2021 10/1/2021	ea. wrongful act ea. wrongful act Prof Ded $25,000	5,000,000 5,000,000 Cyber Ded $25,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

As required by written contract, the City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers are included as Additional Insured as respects to Commercial General Liability and Business Auto.

CERTIFICATE HOLDER

City and County of Denver
Police Department
490 W Colfax Ave
Denver CO 80201

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Thomas C. Watson, III

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide

express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The securityaddendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI’s CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall

> specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Johnny Kouri — 6/10/2021

Printed Name/Signature of Contractor Employee — Date

Matt Solomon — 6/10/2021

Printed Name/Signature of Contractor Representative — Date

Permitium, LLC   Managing Partner

Organization and Title of Contractor Representative