

## **DENVER PARKING MANAGEMENT AGREEMENT**

**THIS AGREEMENT** is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the “City”), and **SP PLUS CORPORATION**, a Delaware corporation, with its principal place of business located at 200 E. Randolph Street, Suite 7700, Chicago, IL 60601 (the “Contractor”), jointly “the Parties” and individually a “Party.”

### **W I T N E S S E T H:**

**WHEREAS**, the City requires an able and experienced parking operator to operate and manage the City’s parking lots and garages; and

**WHEREAS**, a comprehensive Request for Proposals (RFP) has been promulgated by the City and proposals from potential long-term operators have been received and reviewed by the City and the Contractor has, pursuant to its Proposal, offered to provide such services to the City; and

**WHEREAS**, the Parties entered into that certain Denver Parking Management Agreement dated May 3, 2022 (City Contract Control #DOTI-202160398-00), pursuant to which the City’s Department of Transportation and Infrastructure would administer the DPAC garage from the effective date of that agreement through December 31, 2021, and thereafter the DPAC garage would not be administered by DOTI pursuant to that agreement; and

**WHEREAS**, as of January 1, 2022, the DPAC garage will be administered by the City’s Denver Arts & Venues, pursuant to the terms of this Agreement; and

**WHEREAS**, the Contractor possesses the requisite experience and expertise in operating and managing off-street parking facilities, and is ready, willing and able to undertake and manage the DPAC garage as an independent contractor under the general direction of the City;

**WHEREAS**, the City desires to enter into this Management Agreement with the Contractor to provide for the management and operation of the DPAC garage; and

**WHEREAS**, it is the intent of the City that the DPAC garage be managed and maintained so as to ensure the utmost in courteous and prompt service to the general public and that the Contractor shall provide adequate personnel for operation of the DPAC garage and shall comply with the Scope of Work attached as Exhibit A.

**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, and incorporating the recitals above, the City and the Contractor agree as follows:

**1. COORDINATION AND LIAISON.** The Contractor shall fully coordinate all services under the Agreement with the Executive Director of Denver Arts & Venues, (“Executive Director”) or the Executive Director’s Designee.

**2. SERVICES TO BE PERFORMED.**

**2.1.** As the Executive Director directs, the Contractor shall diligently undertake, perform, and complete all of the services and produce all the deliverables set forth in **Exhibit A**, the **Scope of Work**, to the City’s satisfaction.

**2.2.** The Contractor is ready, willing, and able to provide the services required by this Agreement.

**2.3.** The Contractor shall faithfully perform the 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.

**3. TERM.** The Agreement will commence on January 1, 2022, and will expire, unless sooner terminated, on December 31, 2024 (the “Term”). Subject to the Executive Director’s prior written authorization, the Contractor shall complete any work in progress as of the expiration date and the Term of the Agreement will extend until the work is completed or earlier terminated by the Executive Director.

**4. COMPENSATION AND PAYMENT.**

**4.1. Fee.** The City shall pay and the Contractor shall accept as the sole compensation for services rendered and costs incurred under the Agreement the monthly amount FOUR THOUSAND EIGHTY THREE DOLLARS AND NO/100 (\$4,083.00) every month through the end of the Term. Amounts billed may not exceed rates set forth in **Exhibit B**, except for approved reimbursable expenses.

**4.2. Operating Expenses and Reimbursement to Contractor.** The Contractor shall pay all operating expenses for the DPAC garage as set forth in this Agreement. In addition to the fees referenced in above, the Contractor shall be reimbursed by the City for approved reimbursable expenses as set out in the Scope of Work.

**4.3. Invoicing.** The Contractor shall provide the City with a monthly invoice in a format and with a level of detail acceptable to the City including all supporting documentation required by the City. The City's Prompt Payment Ordinance, §§ 20-107 to 20-118, D.R.M.C., applies to invoicing and payment under this Agreement.

**4.4. Maximum Contract Amount.**

**4.4.1.** Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed **FIVE MILLION DOLLARS AND ZERO CENTS (\$5,000,000)** (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by the Contractor beyond that specifically described in **Exhibit A**. Any services performed beyond those in **Exhibit A** are performed at the Contractor's risk and without authorization under the Agreement.

**4.4.2.** 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 this 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.

**5. STATUS OF CONTRACTOR.** The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the 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.

**6. TERMINATION.**

**6.1.** Contractor shall be considered to be in default of this Agreement should Contractor fail to comply with its terms or provisions, and the failure to comply is not cured within ten (10) days after written notice to Contractor, at which point the City has the right to terminate the Agreement effective immediately. The City has the right to terminate the Agreement without cause upon sixty (60) days prior written notice to the Contractor. However, nothing gives the Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Executive Director.

**6.2.** Notwithstanding the preceding paragraph, the City may terminate the Agreement if the 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, kickbacks, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with the Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

**6.3.** Upon termination of the Agreement, with or without cause, the 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.

**6.4.** If the Agreement is terminated, the City is entitled to and will take possession of all materials, equipment, tools and facilities it owns that are in the Contractor's possession, custody, or control by whatever method the City deems expedient. The Contractor shall deliver all documents in any form that were prepared under the Agreement and all other items, materials and documents that have been paid for by the City to the City. These documents and materials are the property of the City. The Contractor shall mark all copies of work product that are incomplete at the time of termination "DRAFT-INCOMPLETE."

**6.5.** The Contractor shall have the right to terminate this Agreement in the event that the City fails to make payments as required under this Agreement.

**7. 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 the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The 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 the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. 20-276.

**8. WHEN RIGHTS AND REMEDIES NOT WAIVED.** In no event will any payment or other action by the City constitute or be construed to be a waiver by the City of any breach of covenant or default that may then exist on the part of the Contractor. No payment, other action, or inaction by the City when any breach or default exists will impair or prejudice any right or remedy available to it with respect to any breach or default. No assent, expressed or implied, to any breach of any term of the Agreement constitutes a waiver of any other breach.

**9. INSURANCE.**

**9.1. General Conditions:** The 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. The 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 be 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, the 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 the Contractor. The 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 the Contractor. The 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.

**9.2. Proof of Insurance:** The Contractor shall provide a copy of this Agreement to its insurance agent or broker. The Contractor may not commence services or work relating to the Agreement prior to placement of coverages required under this Agreement. The 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 the 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 redacted policies and endorsements.

**9.3. Additional Insureds:** For Commercial General Liability, Auto Liability, and Excess Liability/Umbrella (if required) the 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.

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

**9.5. 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 the Contractor. The 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. The Contractor agrees to provide proof of insurance for all such subcontractors and subconsultants upon request by the City.

**9.6. Workers' Compensation/Employer's Liability Insurance:** The 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. The Contractor expressly represents to the City, as a material representation upon which the City is relying in entering into this Agreement, that none of the 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 the Contractor executes this Agreement.

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

**9.8. Business Automobile Liability:** The 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.

**9.9. Commercial Crime:** Contractor shall maintain minimum limits of \$1,000,000 in commercial crime insurance coverage. Coverage shall include theft of City's money, securities or valuable property by contractor's employees, including any extended definition of employee. The City and County of Denver shall be named as Loss Payee as its interest may appear.

**9.10. Garagekeeper's Liability:** Contractor shall maintain Garagekeepers Liability insurance with minimum limits of \$1,000,000 aggregate.

## **10. DEFENSE AND INDEMNIFICATION.**

**10.1.** The 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 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 negligence or willful misconduct of City.

**10.2.** 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 cause of claimant's damages.

**10.3.** 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.

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

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

**11. LIMITATION ON LIABILITY.** Notwithstanding anything in this Agreement to the contrary, Contractor shall not be responsible or liable for any claims, judgments, suits, liabilities, damages, demands or claims for indemnification arising from or related to any revenue control equipment or systems failing to be compliant with (i) the Payment Card Industry's Data Security Standard, as currently in effect and as may be amended from time to time ("**PCI DSS**") or (ii) the Fair and Accurate Credit Transactions Act of 2003, as may be amended from time to time ("**FACTA**") (collectively, "**PCI Related Claims**") unless such failure is caused by Contractor's breach of the PCI DSS or FACTA related responsibilities that are specifically assigned to Contractor in the Self-Assessment Questionnaire D and Attestation of Compliance for Service Providers (the "**SAQ-D**") which is attached to this Agreement as **Exhibit F** and incorporated herein by reference.

**12. COLORADO GOVERNMENTAL IMMUNITY ACT.** In relation to the Agreement, 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, C.R.S. § 24-10-101, *et seq.*



**13. TAXES, CHARGES AND PENALTIES.** The City is not liable for the payment of taxes, late charges or penalties of any nature, except for any additional amounts that the City may be required to pay under the City's prompt payment ordinance D.R.M.C. § 20-107, *et seq.* The Contractor shall promptly pay when due, all taxes, bills, debts and obligations it incurs performing the services under the Agreement and shall not allow any lien, mortgage, judgment or execution to be filed against City property.

**14. ASSIGNMENT; SUBCONTRACTING.** The Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the Executive Director's prior written consent. Any assignment or subcontracting without such consent will be ineffective and void, and will be cause for termination of this Agreement by the City. The Executive Director 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) the 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.

**15. INUREMENT.** The rights and obligations of the parties to the Agreement inure to the benefit of and shall be binding upon the parties and their respective successors and assigns, provided assignments are consented to in accordance with the terms of the Agreement.

**16. 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 the Contractor receiving services or benefits pursuant to the Agreement is an incidental beneficiary only.

**17. NO AUTHORITY TO BIND CITY TO CONTRACTS.** The 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.

**18. 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.

**19. CONFLICT OF INTEREST.**

**19.1.** No employee of the City shall have any personal or beneficial interest in the services or property described in the Agreement. The 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.

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

**20. 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 the addresses below:

SP Plus Corporation  
Attn: Legal Department  
200 E. Randolph Street, Suite 7700  
Chicago, IL 60601

With a copy of any such notice to:

SP Plus Corporation  
Attn: Nicole Hankins, Senior Vice President  
1700 Pacific, Suite 1890  
Dallas, TX 75201

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.

**21. NO EMPLOYMENT OF A WORKER WITHOUT AUTHORIZATION TO PERFORM WORK UNDER THE AGREEMENT.**

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

**21.2.** The Contractor certifies that:

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

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

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

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

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

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

**21.3.** The Contractor is liable for any violations as provided in the Certification Ordinance. If the Contractor violates any provision of this section or the Certification Ordinance, the City may terminate this Agreement for a breach of the Agreement. If this Agreement is so terminated, the Contractor shall be liable for actual and consequential damages to the City. Any termination of a contract due to a violation of this section or the Certification Ordinance may also, at the discretion of the City, constitute grounds for disqualifying the Contractor from submitting bids or proposals for future contracts with the City.

**22. DISPUTES.** All disputes between the City and the 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 Executive Director as defined in this Agreement.

**23. 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 (Denver District Court).

**24. NO DISCRIMINATION IN EMPLOYMENT.** In connection with the performance of work under the Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.

**25. COMPLIANCE WITH ALL LAWS.** The 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. Notwithstanding the foregoing to the contrary, with respect to compliance of laws, where such compliance requires physical changes to any parking lots or garages, for example, Americans With Disabilities Act of 1990 requirements, then compliance shall be City's responsibility rather than Contractor.

**26. LEGAL AUTHORITY.** The 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 the Contractor represents and warrants that he has been fully authorized by the Contractor to execute the Agreement on behalf of the Contractor and to validly and legally bind the 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 the Contractor or the person signing the Agreement to enter into the Agreement.

**27. 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.

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

**29. INTELLECTUAL PROPERTY RIGHTS.** The City and the Contractor intend that all property rights to any and all materials, text, logos, documents, booklets, manuals, references, guides, brochures, advertisements, URLs, domain names, music, sketches, web pages, plans, drawings, prints, photographs, specifications, software, data, products, ideas, inventions, and any other work or recorded information created by the Contractor and paid for by the City pursuant to this Agreement, in preliminary or final form and on any media whatsoever (collectively, "Materials"), shall belong to the City. The Contractor shall disclose all such items to the City and shall assign such rights over to the City upon completion of the Project. To the extent permitted by the U.S. Copyright Act, 17 USC § 101, *et seq.*, the Materials are a "work made for

hire” and all ownership of copyright in the Materials shall vest in the City at the time the Materials are created. To the extent that the Materials are not a “work made for hire,” the Contractor (by this Agreement) sells, assigns and transfers all right, title and interest in and to the Materials to the City, including the right to secure copyright, patent, trademark, and other intellectual property rights throughout the world and to have and to hold such rights in perpetuity. The City and Contractor agree that all materials, text, logos, documents, booklets, manuals, references, guides, brochures, advertisements, URLs, domain names, music, sketches, web pages, plans, drawings, prints, photographs, specifications, software, data, products, ideas, inventions, and any other work or recorded information of Contractor made available, directly or indirectly, by Contractor to City as part of the Scope of Services, are the exclusive property of Contractor or the third parties from whom Contractor has secured the rights to use such product. The Contractor Materials, processes, methods and services shall at all times remain the property of the Contractor; however, the Contractor hereby grants to the City a nonexclusive, royalty free, license to use the Contractor Materials for the duration of the Term of this Agreement. The Contractor shall mark or identify all such Contractor Materials to the City. Nothing in this Agreement shall give City an interest in any of Contractor’s pre-existing intellectual property which is and shall remain the sole property of Contractor.

**30. 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, the 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.

**31. ADVERTISING AND PUBLIC DISCLOSURE.** The Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of the Contractor’s advertising or public relations materials without first obtaining the written approval of the Executive Director. Any oral presentation or written materials related to services performed under the Agreement will be limited to services that have been accepted by the City. The Contractor shall notify the Executive Director in advance of the date and time of any

presentation. Nothing in this provision precludes the transmittal of any information to City officials.

## **32. CONFIDENTIAL INFORMATION.**

**32.1. City Information.** The Contractor acknowledges and accepts that, in performance of all work under the terms of this Agreement, the Contractor may have access to Proprietary Data or confidential information that may be owned or controlled by the City, and that the disclosure of such Proprietary Data or information may be damaging to the City or third parties. The Contractor agrees that all Proprietary Data, confidential information or any other data or information provided or otherwise disclosed by the City to the Contractor shall be held in confidence and used only in the performance of its obligations under this Agreement. The Contractor shall exercise the same standard of care to protect such Proprietary Data and information as a reasonably prudent contractor would to protect its own proprietary or confidential data. "Proprietary Data" shall mean any materials or information which may be designated or marked "Proprietary" or "Confidential," or which would not be documents subject to disclosure pursuant to the Colorado Open Records Act or City ordinance, and provided or made available to the Contractor by the City. Such Proprietary Data may be in hardcopy, printed, digital or electronic format.

### **32.2. Use and Protection of Proprietary Data or Confidential Information.**

Except as expressly provided by the terms of this Agreement, the Contractor agrees that it shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available any data, including Proprietary Data or confidential information or any part thereof to any other person, party or entity in any form of media for any purpose other than performing its obligations under this Agreement. The Contractor further acknowledges that by providing data, Proprietary Data or confidential information, the City is not granting to the Contractor any right or license to use such data except as provided in this Agreement. The Contractor further agrees not to disclose or distribute to any other party, in whole or in part, the data, Proprietary Data or confidential information without written authorization from the Executive Director and will immediately notify the City if any information of the City is requested from the Contractor from a third party.

**32.2.1.** The Contractor agrees, with respect to the Proprietary Data and confidential information, that: (1) the Contractor shall not copy, recreate, reverse engineer or

decompile such data, in whole or in part, unless authorized in writing by the Executive Director; (2) the Contractor shall retain no copies, recreations, compilations, or decompilations, in whole or in part, of such data; and (3) the Contractor shall, upon the expiration or earlier termination of the Agreement, destroy (and, in writing, certify destruction) or return all such data or work products incorporating such data or information to the City.

**32.2.2.** The Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted data received from, or on behalf of City. It is the responsibility of the Contractor to ensure that all possible measures have been taken to secure the computers or any other storage devices used for City data. This includes industry accepted firewalls, up-to-date anti-virus software, controlled access to the physical location of the hardware itself.

**32.3. Employees and Subcontractor.** The Contractor will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of the Contractor under this Agreement shall survive the expiration or earlier termination of this Agreement. The Contractor shall not disclose Proprietary 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.

**32.4. Disclaimer.** Notwithstanding any other provision of this Agreement, the City is furnishing Proprietary Data and confidential information on an “as is” basis, without any support whatsoever, and without representation, warranty or guarantee, including but not in any manner limited to, fitness, merchantability or the accuracy and completeness of the Proprietary Data or confidential information. The Contractor is hereby advised to verify its work. The City assumes no liability for any errors or omissions herein. Specifically, the City is not responsible for any costs including, but not limited to, those incurred as a result of lost revenues, loss of use of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for similar costs. If discrepancies are found, the Contractor agrees to contact the City immediately.

**32.5. Contractor’s Confidential Information; Open Records.** If the City is furnished with proprietary data or confidential information that may be owned or controlled by Contractor (“Contractor’s Confidential Information”), the City will endeavor, to the extent



provided by law, to comply with the requirements provided by the Contractor concerning the Contractor's Confidential Information. However, the Contractor understands that all the material provided or produced by the Contractor under this Agreement 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 will advise the Contractor of such request in order to give the Contractor the opportunity to object to the disclosure of any of it's the Contractor Confidential Information and take necessary legal recourse. 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 the Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. The Contractor further agrees to defend, indemnify, save, and hold harmless the City from any Claims arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section including, without limitation, prompt reimbursement to the City of all reasonable attorneys' fees, costs, and damages that the City may incur directly or may be ordered to pay by such court.

**32.6.** If the Contractor receives personal identifying information ("PII") under this Agreement, the Contractor shall implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the PII and the nature and size of the Contractor's business and its operations. The Contractor shall be a "Third-Party Service Provider" as defined in C.R.S § 24-73-103(1)(i), and shall maintain security procedures and practices consistent with C.R.S §§ 24-73-101 *et seq.* Unless the Contractor agrees to provide its own security protections for the information it discloses, the Contractor shall require all its subcontractors, employees, agents, and assigns to implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the PII disclosed and reasonably designed to help protect the PII subject to this Agreement from unauthorized access, use, modification, disclosure, or destruction. The Contractor and its subcontractors, employees, agents, and assigns that maintain electronic or paper documents that contain PII under this Agreement shall develop a written policy for the destruction of such records by shredding, erasing, or otherwise modifying the PII to make it unreadable or indecipherable when the records are no longer needed.

**33. 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 or suspended for a period as may be reasonably necessary to compensate for such delay.

**34. CITY EXECUTION OF AGREEMENT.** The Agreement will not be effective or binding on the City until it has been fully executed by all required signatories of the City and County of Denver, and if required by Charter, approved by the City Council.

**35. AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS.** 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.

**36. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS.** The Contractor shall cooperate and comply with the provisions of Executive Order 94 and its Attachment A 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 contract personnel being barred from City facilities and from participating in City operations.

**37. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS.** The Contractor consents to the use of electronic signatures by the City. The Agreement, and any other documents requiring a signature under the Agreement, 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.

**38. PAYMENT OF CITY MINIMUM WAGE.** Contractor shall comply with, and agrees to be bound by, all requirements, conditions, and City determinations regarding the City's Minimum Wage Ordinance, Sections 20-82 through 20-84 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid no less than the City Minimum Wage in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, Contractor expressly acknowledges that Contractor is aware of the requirements of the City's Minimum Wage Ordinance and that any failure by Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.

**39. PREVAILING WAGE REQUIREMENTS.**

**39.1.** Contractor shall comply with, and agrees to be bound by, all requirements, conditions and City determinations regarding the Payment of Prevailing Wages Ordinance, Sections 20-76 through 20-79, D.R.M.C. including, but not limited to, the requirement that every covered worker working on a City owned or leased building or on City-owned land shall be paid no less than the prevailing wages and fringe benefits in effect on the date the bid or request for proposal was advertised. In the event a request for bids, or a request for proposal, was not advertised, Contractor shall pay every covered worker no less than the prevailing wages and fringe benefits in effect on the date funds for the contract were encumbered.

**39.2.** Date bid or proposal issuance was advertised May 21, 2021.

**39.3.** Prevailing wage and fringe rates will adjust on the yearly anniversary of the actual date of bid or proposal issuance, if applicable, or the date of the written encumbrance if no bid/proposal issuance date is applicable. Unless expressly provided for in this Agreement, Contractor will receive no additional compensation for increases in prevailing wages or fringe benefits.

**39.4.** Contractor shall provide the Auditor with a list of all subcontractors providing any services under the contract.

**39.5.** Contractor shall provide the Auditor with electronically-certified payroll records for all covered workers employed under the contract.

**39.6.** Contractor shall prominently post at the work site the current prevailing wage and fringe benefit rates. The posting must inform workers that any complaints regarding the

payment of prevailing wages or fringe benefits may be submitted to the Denver Auditor by calling 720-913-5000 or emailing [auditor@denvergov.org](mailto:auditor@denvergov.org).

**39.7.** If Contractor fails to pay workers as required by the Prevailing Wage Ordinance, Contractor will not be paid until documentation of payment satisfactory to the Auditor has been provided. The City may, by written notice, suspend or terminate work if Contractor fails to pay required wages and fringe benefits.

**40. NON-DISPLACEMENT OF QUALIFIED WORKERS.**

**40.1.** Consistent with the efficient performance of this Agreement, the Contractor and any subcontractors shall, except as otherwise provided herein, in good faith offer those employees (other than managerial and supervisory employees) employed under the predecessor contract whose employment will be terminated as a result of an award of this Agreement or the expiration of the contract under which the employees were hired, a right of first refusal of employment under this Agreement in positions for which employees are qualified. The Contractor and its subcontractors shall determine the number of employees necessary for efficient performance of the work. Except as provided in paragraph (b) there shall be no employment opening under this Agreement, and the Contractor and any subcontractors shall not offer employment under this Agreement, to any person prior to having complied fully with this obligation. The Contractor and its subcontractors shall make an express offer of employment to each employee as provided herein and shall state the time within which the employee must accept such offer, but in no case shall the period within which the employee must accept the offer of employment be less than 10 days.

**40.2.** The Contractor shall retain, for a ninety (90) day transition employment period, qualified employees who have exercised their right to accept employment with the Contractor as provided in paragraph (a) of this section. During the ninety (90) day transition employment period, the Contractor shall not discharge without cause an employee retained pursuant to this section. For purposes of this section, the term "cause" shall include, but not be limited to, the employee's conduct while employed under the predecessor contract that may have contributed to any decision to terminate the predecessor contract. At the end of the ninety (90) day transition employment period, the Contractor shall perform a written performance evaluation for each service employee retained pursuant to this section. If the employee's performance during such ninety (90) day period is satisfactory, the

Contractor shall offer the employee continued employment under the terms and conditions established by the Contractor or as required by law; provided, however, nothing in this section shall be construed to create any right or entitlement to continued employment by the Contractor for any particular period of time in excess of the ninety (90) day transition employment period.

**40.3.** Notwithstanding the obligation under paragraph (a) above, the Contractor and any subcontractor (1) may employ under this Agreement any employee who has worked for the Contractor or subcontractor for at least 3 months immediately preceding the commencement of this Agreement and who would otherwise face lay-off or discharge, (2) are not required to offer a right of first refusal to an employee(s) of the predecessor contractor who are not service employees within the meaning of Section 3.0 of Executive Order No. 136, and (3) are not required to offer a right of first refusal to any employee(s) of the predecessor contractor whom the Contractor or any of its subcontractors reasonably believes, based on the particular employee's past performance, has failed to perform suitably on the job.

**40.4.** The Contractor shall, not less than 10 days before completion of this Agreement, furnish the contract administrator a certified list of the names of all service employees working under this Agreement and its subcontracts during the last month of contract performance. The list shall also contain anniversary dates of employment of each service employee under this Agreement and its predecessor contracts either with the current or predecessor contractors or their subcontractors. The contract administrator will provide the list to the successor contractor, and the list shall be provided on request to employees or their representatives.

**40.5.** If it is determined that the Contractor or its subcontractors are not in compliance with the requirements of this clause, appropriate sanctions may be imposed and remedies invoked against the Contractor or its subcontractors, as provided in this Agreement.

**40.6.** In every subcontract entered into in order to perform services under this Agreement, the Contractor will include provisions that ensure that each subcontractor will honor the requirements of paragraphs (a) through (b) with respect to the employees of a predecessor subcontractor or subcontractor working under this Agreement, as well as of a predecessor contractor and its subcontractor. The subcontract shall also include provisions to ensure that the subcontractor will provide the Contractor with the information about the employees of the

subcontractor needed by the Contractor to comply with paragraph (c) above. The Contractor will take such action with respect to any such subcontract as may be directed by the contract administrator as a means of enforcing such provisions, including the imposition of sanctions for non-compliance: provided, however, that if the Contractor, as a result of such direction, becomes involved in litigation with a subcontractor, or is threatened with such involvement, the Contractor may request that the City enter into such litigation to protect the interest of the City.

**40.7.** Prior to the end of the Term of this Agreement the Contractor agrees to cooperate with the City and provide necessary requested information by the City to effectuate the requirements of Executive Order No. 136.

**40.8.** Contractor agrees to comply with Title II, Chapter 58, Article III of the D.R.M.C pertaining to worker retention.

**41. DIVISION OF SMALL BUSINESS OPPORTUNITY.**

**41.1.** This Agreement is subject to Article V of Chapter 28, Denver Revised Municipal Code (“D.R.M.C.”), designated as §§ 28-117 to 28-199 D.R.M.C. (the “Goods and Services Ordinance”) and any Rules or Regulations promulgated pursuant thereto. The contract goal for MWBE participation established for this Agreement by the Division of Small Business Opportunity (“DSBO”) is 5%.

**41.2.** Under § 28-132, D.R.M.C., the Contractor has an ongoing, affirmative obligation to maintain for the duration of this Agreement, at a minimum, compliance with its originally achieved level of MWBE participation upon which this Agreement was awarded, unless there is a change in the work by the City, or as otherwise as described in § 28-133, D.R.M.C. The Contractor acknowledges that:

**41.3.** The Contractor must maintain records and submit regular reports, as required under the ordinance and as directed by DSBO, which will allow the City to assess progress in complying with the MWBE participation goal.

**41.4.** If contract modifications are issued under the Agreement, whether by amendment or otherwise, the Contractor shall have a continuing obligation to immediately inform DSBO in writing of any agreed upon increase or decrease in the scope of work of such contract, upon any of the bases discussed in § 28-133, D.R.M.C., regardless of whether such increase or decrease in scope of work has been reduced to writing at the time of notification.

**41.5.** If there are changes in the work that include an increase in scope of work under this Agreement, whether by amendment or otherwise, which increases the dollar value of the contract, whether or not such change is within the scope of work designated for performance by an MWBE at the time of contract award, such change or modification shall be immediately submitted to DSBO for notification purposes.

**41.6.** Those amendments or other modifications that involve a changed scope of work that cannot be performed by existing subcontractors shall be subject to the original goal on the contract. The Contractor shall satisfy such goal with respect to the changed scope of work by soliciting new MWBEs in accordance with §§ 28-133, D.R.M.C. The Contractor must also satisfy the requirements under §§ 28-128 and 28-136, D.R.M.C., with regard to changes in MWBE scope or participation. The Contractor shall supply to the DSBO Director all required documentation described in §§ 28-128, 28-133, and 28-136, D.R.M.C. with respect to the modified dollar value or work under the contract.

**41.7.** For contracts of one million dollars (\$1,000,000.00) and over, the Contractor is required to comply with § 28-135, D.R.M.C., as applicable, regarding prompt payment to MWBEs. Payment to MWBE subcontractors shall be made by no later than thirty-five (35) days after receipt of an MWBE subcontractor invoice.

**41.8.** Failure to comply with these provisions may subject the Contractor to sanctions set forth in § 28-139 of the Goods and Services Ordinance.

**41.9.** Should any questions arise regarding DSBO requirements, the Contractor should consult the Goods and Services Ordinance or may contact the designated DSBO representative at (720) 913-1999.

**42. PCI DSS COMPLIANCE.** The SAQ-D is attached hereto as Exhibit F and identifies if responsibility resides with Contractor for each PCI control requirement. Only items marked “Yes” on pages 9-84 of the SAQ-D shall be considered Contractor’s responsibility.

**Exhibits:**

- Exhibit A - Scope of Work**
- Exhibit B - Fees and Proposed Budget**
- Exhibit C - Certificate of Insurance**
- Exhibit D - Wage Rates**
- Exhibit E - DSBO Forms**
- Exhibit F - SAQ-D**

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK**



**Contract Control Number:** THTRS-202160770-00  
**Contractor Name:** SP Plus Corporation

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

**SEAL** **CITY AND COUNTY OF DENVER:**


**ATTEST:** By: \_\_\_\_\_  
\_\_\_\_\_

**APPROVED AS TO FORM:** **REGISTERED AND COUNTERSIGNED:**  
Attorney for the City and County of Denver  
By: \_\_\_\_\_ By: \_\_\_\_\_

By: \_\_\_\_\_

**Contract Control Number:**  
**Contractor Name:**

THTRS-202160770-00  
SP Plus Corporation

By:  2C0D898A8348469...

Name: Nicole Hankins  
(please print)  
Title: Senior Vice President  
(please print)

ATTEST: [if required]

By: \_\_\_\_\_

Name: \_\_\_\_\_  
(please print)

Title: \_\_\_\_\_  
(please print)

## Exhibit A

### Scope of Work

#### **PARKING OPERATIONS FOR CITY PARKING FACILITIES STANDARD OPERATING PROCEDURES**

This Scope of Work for professional parking facility management is between the City and County of Denver (here in- after referred to as the “City”) and a qualified professional parking operator (here in-after referred to as the “Contractor”).

By terms of this management agreement, the Contractor will operate one (1) parking garage (here in-after referred to as the “Garage,” on behalf of the City. This Scope of Work constitutes the basic guidelines, standards, and specific procedures for the operation and maintenance of the Garages that the City requires the Contractor to meet. These guidelines, standards, and procedures are subject to change at the discretion of the City by written notification from the Manager of the Denver Performing Arts Complex (here in-after referred to as the “Manager”) or their designee. Failure to abide by this Scope of Work, at the discretion of the City could constitute a breach of this Agreement.

The one (1) parking Garage under this management Agreement is as follows:

- 1) Denver Performing Arts Complex Garage – 1055 13th Street, Denver, Colorado

#### **SECTION I: AREA OF GARAGE MANAGEMENT**

- A The Contractor, per this Scope of Work, will professionally manage the following Garage:

Denver Performing Arts Complex Garage – 1055 13<sup>th</sup> Street

The Contractor will manage **1,743** parking spaces serving paid public parking in the Theatre District, Central-Business District, and events in the vicinity. Monthly permit parking is offered in this Garage.

- B. The City, at any time, may give notice in writing to the Contractor if the amount of parking stalls managed in the Garage increases or decreases. The City may add or subtract Facilities within this management agreement without immediately amending the Management Agreement.

- C. On-Call, As-Needed Services

On-Call, As-Needed Services at other City facilities separate from the Garage identified above in Section A, paragraph A. If approved by the City, a flat rate hourly fee plus reimbursable expenditure may be charged by the Contractor for “on-call, as-needed” services to other, non-contracted parking facilities owned by the City.

“On-call, as needed” services include, but not limited to, enforcement, porter duties, light duty maintenance, and customer service or attendant services. The option by the City to agree to the On-Call Services Fee is

separate to the Management Fee. The City, at its sole discretion, may reject the On-Call Services Fee option without affecting the acceptance of the Management Agreement for Garage

- D. The Contractor is provided use of a primary office space on the Galleria/Third Level and secondary office space located on the 2<sup>nd</sup> Level near the 2<sup>nd</sup> Floor Elevator next to 13<sup>th</sup> Street Entrance within the Garage. Should this contract be terminated, the Contractor shall vacate these spaces within 30 days.

## **SECTION II: BUDGET AND REIMBURSABLE EXPENSES**

### **A. Annual Budget**

Within thirty (30) days of the execution of the Agreement, the Contractor shall submit to the City for approval, an annual budget of projected costs for the Garage. The budget shall be submitted each year on a date approved by the City. The annual budget must be approved in writing by the City. The budget shall include the following items:

1. Salary costs for managers and wages for all other employees according to classification supporting this agreement.
2. Employee benefit cost, which includes, according to category, FICA, City Occupational Tax, Worker Compensatory Tax and all other city approved employee benefits.
3. All other approved categorized expenses as allowed by this Agreement, which include, but are not limited to:
  - Off-Duty Police Officers (event traffic control)
  - Uniforms
  - Ticket inventory for revenue access control system
  - Telephone (landline, fax and manager/supervisor cellular phones)
  - Postage
  - Transponders, hang tags, or other approved devices used to manage monthly parkers
  - On-site office equipment and supplies
  - Receipt paper roll inventory for revenue control system(s)
  - Parking access control equipment repair and preventative maintenance
  - Payment systems repair and preventative maintenance
  - PayByPhone software fees
  - Servicing EV Stations
  - Audit supplies or services
  - Cleaning and janitorial equipment and supplies
  - Power sweeping
  - Power washing
  - Snow and ice removal services and resources
  - Trash and graffiti removal
  - Striping (line painting), curb painting and island painting
  - Signage
  - Sign installation and repair
  - Customer refunds
  - Itemized Miscellaneous Expenses
  - Insurance charges established by Contractor required under this Agreement and specifically set forth in the Budget

- Management fees
- Itemized Miscellaneous Expenses not included in the annual budget must be approved in writing by the City

#### B. Amendments to Budget

Amendments, changes, or modifications to the budgets can be made only by written request by the Contractor and written approval by the City. These amendments must be approved prior to any expenditure in the modified item.

#### C. Reimbursement of Monthly Expenditures

The City will reimburse the Contractor for the approved operating expenses (listed previously within this section). The Contractor shall maintain complete original files and journals of all cash disbursements, including payroll, at a location available for review by the City within a 24-hour notice. The following procedures pertain to the cash disbursement system:

1. All payroll expenditures will be recorded in a register and supported by approved timecards. For Prevailing Wage certification and approval, the Contractor must supply the Prevailing Wage office all required payroll information on a monthly basis. This information must be submitted through the on- line Prevailing Wage certified system. In the event there are changes to **SP+**'s labor or employment costs then **SP+** will be reimbursed for those increased costs.
2. All fringe benefit and payroll tax payments must be supported by pertinent tax returns and cash disbursements or accounts payable records.
3. All disbursements will be supported by voucher files that include original invoices and receipts (scanned copies of originals will suffice). Invoices and receipts that are illegible, not dated or labeled will not be reimbursed. If the City has a question on the legitimacy or accuracy of an item to be reimbursed, the item will not be reimbursed until it can be confirmed by the City
4. No later than the **15th** day of the following month, the Contractor will submit the previous month's expenditures to the City for reimbursement, along with the previous month's revenue report(s). Reimbursement to the Contractor from the City will be made within thirty-five (35) days of receipt and approval of expenses. Expenditures submitted to the City will include the original invoice or receipt (scanned copies will suffice) showing date paid and Contractor voucher number and specify the approved budget line item.

Expenditures that have not been approved by the City will not be reimbursed. The expenditure report will show the approved budget, monthly and cumulative expenditures for each budget line item. No expenditures exceeding the budget or in variance with the budget will be processed for reimbursement until the expenditure has been justified and approved by the City. Incomplete or inaccurate expenditure and financial packages will require the Contractor to resubmit proper documentation, including a newly dated original invoice reflecting the date in which the packages were deemed complete and acceptable by the City.

#### D. Reimbursement Exclusions

The following items are expressly excluded from reimbursement as operating expenses under the Budget. These items shall be provided, if applicable, by the Contractor at their own expense:

1. Executive and administrative level overhead expenses not previously approved
2. Contractor office lease/mortgage payments
3. Office equipment, including furniture and computers
4. Costs of repairs for damaged City property caused by Contractor's negligence
5. Travel expenses outside the City and County of Denver
6. Entertainment expenses
7. Professional memberships and subscriptions
8. Losses and expenses associated with theft or robbery of Garage revenue
9. Losses and expenses associated with employee theft, shortage, or mismanagement
10. Deductibles, if any, on all bonds, insurance policies, and programs

### **SECTION III: RECORDS AND REPORTING**

A. The following daily or continuous records and reports will be maintained for the Garage and available for inspection by the City:

1. Daily total count of all vehicles entering and exiting the Garage for each gate
2. Daily total sales receipts (cash, credit card and monthly transactions)
3. Daily combined recap of all cashier booth and pay-station activity
4. Daily account of monthly or other permits sold (Contractor to supply, sell and control use of monthly permits)
5. Daily account of all ticket validations, discounted tickets, and miscellaneous revenue received
6. Daily report of all Garage incidents (excluding security)
7. Garage closure log detailing specific times and reasons for closures
8. Daily Inventory County for Overnight Vehicles

B. Monthly records and reports. The following information for the Garage will bereported monthly to the City:

1. By the Fifth (5th) business day of the following month:
  - Preliminary Total Gross Revenues, by category (i.e., daily transient, special event, monthly), for the previous month.
2. By the Fifteenth (15th) calendar day of the following month:
  - Cover letter summarizing any significant variances in revenue and expenses and any significant abnormalities occurring in the Garages and surface lots during the month
  - Profit and Loss Statement (detailed) by month and year to date – Total Gross Revenues by category & Expenses by category
  - Revenue Summary Report(s)
  - Detailed Deposit Report(s)
  - Payroll Distribution Report
  - Annual Budget Roll-up Summary
  - Monthly Parker Billing Detail
  - Monthly Parker Accounts Receivable Detail
  - Aging Account Receivables Report
  - Variance report of revenues and expenses - Current month vs. budget, YTD vs. budget, and current month vs. same month prior year

- Ticket Summary report detailing by date all tickets issued and collected by category along with missing tickets
  - Monthly expenditure report by budget item showing current month and year-to-date
  - Copies of original invoices supporting the expenditures
  - Citation Summary (issued, revenue, and outstanding) – if required/applicable
  - Occupancy report generated from revenue control software
3. The Contractor shall provide accurate monthly reports and supporting documentation for reimbursable expenses to the City no later than the fifteenth (15th) of each month and shall deliver other accurate reports no later than the agreed upon schedule of time. The Contractor will reconcile total monthly receipts with Arts and Venues Finance no later than the fifth(5th) of the month.

In addition to the reports listed previously, the following reports are to be maintained by the Contractor and released to the City upon request.

- Counter logs (gates, ticket dispensers and loop count, if applicable)
  - Cashier shift reports
  - Bank deposit reports
  - Monthly parking database including free and discounted parkers
  - Ticket inventory (received and issued)
  - NSF check report/log
4. Originals of all settlement sheets, cashier shift reports, deposit slips, and tickets separated by shift will be stored at a secure location available with a 24-hour notice for a minimum of three years and made available at any time for review by the City.
5. A cash receipts journal system will be maintained at the Contractor's office to record daily deposits and revenue types. This journal will be used to provide daily transient and monthly deposit information at any time to the City.
6. The Contractor will maintain a list of Non-Sufficient Funds (NSF) checks up to one year old. Denver Arts and Venues Finance Department will report to the Contractor any NSF checks verified by the bank. The Contractor will attempt to collect a fifty (\$50.00) dollar NSF fee from the customer in addition to the original amount of the payment.
7. All reporting is subject to change with the installation of new PARCS equipment and will have new process.

## **SECTION IV: DEPOSITS AND SETTLEMENTS**

### **A. Deposits**

The Contractor shall deposit all monies collected into designated City bank account(s) at frequency directed by the City, and shall maintain documentation of the date and time of the deposit transaction. All pay stations, from the Garage and, shall be collected daily (Monday through Friday), unless previously authorized by City.

## **Daily Cash Deposits**

### **Deposit Slips**

- Totals match amount in the bag
- Must include full bag number above the MICR line

### **Deposit Bags**

- Full total on the deposit bag must match the deposit slip
- Contents must be verified before sealed

### **Armored Truck Logs**

- This is an important verification tool needed when discrepancies arise
- All information must be clear and complete
- Full bag numbers and full totals are a must

### **Ordering Deposit Slips and Bags**

- Contact Arts and Venues Finance to order deposit supplies
- Do not order supplies through Armored Knights



Deposit Bag with Deposit Slip

WARNING: Extremely Tamper Evident! Any Attempts At Entry Will Be Easily Detected!

IF THE WORDS "VOID TAMPERING ACTIVATED" APPEAR ON THE SECURITY TAPE ABOVE, TAMPERING MAY HAVE OCCURRED. DO NOT OPEN BAG. NOTIFY SENDER IMMEDIATELY.

IMPORTANT: PLACE CURRENCY AND OTHER SHIPPING CONTENTS IN PRIMARY POCKET

DEPOSIT TICKET 23-1017080  
CITY AND COUNTY OF DENVER  
CULTURAL CENTER GARAGE # 8032806  
DENVER, CO 80022  
CHASE  
CHASE BANK, N.A.  
DATE 5/10/18  
AMOUNT \$463.00  
SS 22908961 \$ 463.00

FROM: \_\_\_\_\_ TO: \_\_\_\_\_  
(Name of Depositor (Banking Center))  
DATE: \_\_\_\_\_  
SAID TO CONTAIN: \_\_\_\_\_  
BAG# \_\_\_\_\_ OF \_\_\_\_\_  
(Depositor Identification (Cost Center))

ITEM REORDER NO. 2742975

Deposit Bag

Remove this tear-off record BEFORE sealing bag

DATE: \_\_\_\_\_ SAID TO CONTAIN: \_\_\_\_\_  
BAG # \_\_\_\_\_ OF \_\_\_\_\_ NUMBER OF BAGS WITHIN THIS BAG \_\_\_\_\_

CAUTION: DO NOT FOLD PAST DASHED LINE

IF THE WORDS "VOID TAMPERING ACTIVATED" APPEAR ON THE SECURITY TAPE ABOVE, TAMPERING MAY HAVE OCCURRED. DO NOT OPEN BAG. NOTIFY SENDER IMMEDIATELY.

SS22908961

Insert shipping label in white interior pocket with ADDRESS FACING OUT

IMPORTANT: PLACE CURRENCY AND OTHER SHIPPING CONTENTS IN PRIMARY POCKET

SEALING INSTRUCTIONS

- Working on flat surface, remove tear off strip down and fold contents into bag.
- Remove release strip, fold bag around contents and fold flap forward on front of bag, tuck flap into fold past dashed line.
- Press flap down and smooth around bag. BAG IS NOW SEALED. DO NOT ATTEMPT TO REOPEN.

RECEIVER INSTRUCTIONS:

- 1) Verify contents (Strap Count) before opening bag.
- 2) Open bag as indicated and complete detailed verification of contents immediately.
- 3) Report any discrepancies immediately to JP Morgan Chase.

JPMorganChase

TO: \_\_\_\_\_ FROM: \_\_\_\_\_  
(Name of Depositor (Banking Center))  
DATE: \_\_\_\_\_  
SAID TO CONTAIN: \$ \_\_\_\_\_  
BAG# \_\_\_\_\_ OF \_\_\_\_\_  
(Depositor Identification (Cost Center))

ITEM REORDER NO. 2742975

Change Envelope Example



Armored Knight Log Example

Received by Armored Knights Inc. from Cultural Center Garage

DATE	PREPARED BY INITIALS	DEPARTMENT	BAG #	NO PKGS	SAID TO CONTAIN	TIME	DATE PICKED UP	MESSENGER-GUARD'S SIGNATURE
4/27	KS	CCG	SS1003111	1	360.00			
4/27	KS	CCG	SS1003112	1	72.00			
4/27	KS	CCG	SS1003113	1	14.00			
4/27	KS	CCG	SS1003114	1	119.00			
4/27	KS	CCG	SS1003115	1	63.00			
4/28	KS	CCG	SS1003116	1	781.00			
4/28	KS	CCG	SS1003117	1	121.00			
4/28	KS	CCG	SS1003118	1	360.00			
4/28	KS	CCG	SS1003119	1	12.00			
4/28	KS	CCG	SS1003120	1	171.00			
4/29	KS	CCG	SS1003121	1	32.00			
4/29	KS	CCG	SS1003122	1	412.00			
4/29	KS	CCG	SS1003123	1	1226.00			
4/29	KS	CCG	SS1003124	1	143.00			
4/29	KS	CCG	SS1003125	1	200.00			
5/1	KS	CCG	SS1003126	1	63.00			
5/1	KS	CCG	SS1003127	1	40.00			
5/1	KS	CCG	SS1003128	1	818.00			
5/1	KS	CCG	SS1003129	1	311.00			
5/1	KS	CCG	SS1003130	1	130.00			

## B. Credit Card Settlement

The Contractor will settle credit cards transactions daily. The parties agree that City is the merchant of record on all revenue control equipment and as such any credit card revenue will be deposited directly into City's bank account from the revenue control equipment.

## SECTION V: EQUIPMENT

### A. Revenue and Operational Control Equipment

The City will provide revenue and operational control equipment. The Contractor shall perform the following: maintenance, preventative maintenance repairs, and/or service of all parking equipment and their systems. The Contractor in conjunction with the City will draft a detailed preventative maintenance plan within thirty (30) days of the Agreement start date. Once approved by the City, any modifications to the maintenance plan must be approved in writing by the City.

In the event that any City provided equipment is damaged or destroyed by the negligence of the Contractor or the Contractor's employees, the Contractor shall notify the City and agrees to be liable for the repair or replacement of the equipment as necessary.

In the event of a revenue control equipment malfunction and subsequent repair, the appropriate repair vendor and the City are to be notified immediately, via e-mailing a description of the equipment malfunction with information stating date, time, location, duration and how the equipment was repaired. The Contractor will not reset, relocate or disconnect equipment without prior approval from the City.

Within thirty (30) days of the execution of the Agreement, the City in conjunction with the Contractor will generate an inventory including model and serial numbers of all revenue control equipment, office furnishings/equipment, ticket supply and any other operating equipment.

Equipment Maintenance is subject to change with new PARCS equipment installation and new maintenance processes will be approved with Contractor prior to PARCS equipment going live.

#### 1. Parking Revenue Control Equipment.

Contractor shall operate and maintain the City of Denver parking revenue control equipment, which includes the following:

- i. Management and financial reports showing daily, weekly and monthly revenues, access in and out of the Parking Facilities, availability of spaces, anti-passback functions, average parking duration of stay, average parking ticket value, status of access cards and other statistical information as needed.
- ii. Contractor shall keep City of Denver informed of all available upgrades and modifications to existing parking revenue control equipment.

#### 2. Parking Revenue Control Equipment Maintenance

Contractor shall perform daily preventive maintenance and regular minor maintenance on revenue control equipment in accordance with manufacturer's specifications. At a very minimum,

such work shall include the following items:

- i. Inspect and fix or replace all ticket dispensers
- ii. Inspect all clocks to be sure the times are correct
- iii. Replace broken or damaged gate arms
- iv. Inspect and fix all receipt functions computers, as necessary, to maintain a clear printout.
- v. Timing

## B. Equipment Maintenance

### 1. The Responsibility of the Contractor

- i. Maintenance of parking equipment and their systems
- ii. Preventative maintenance repairs of parking equipment and their systems
- iii. Service of all parking equipment and their systems
- iv. Maintain and service lot lighting and signage systems

### 2. The Responsibility of the City

- i. Maintain and service all life/safety (fire alarm, sprinkler, and monitoring systems).
- ii. Maintain and service carbon monoxide detection system and exhaust fans.
- iii. Maintain and service the passenger elevators, where applicable.
- iv. Maintain and service Garage camera surveillance systems.
- v. Maintain and service Garage lighting systems, where applicable.
- vi. Maintain and service heating and cooling systems (excluding minor repairs and maintenance in the Parking Office and cashier stations).
- vii. Maintain and service heaters and air conditioners (excluding minor repairs and maintenance in the Parking Office and cashier stations).
- viii. Service and repair the major electrical systems and plumbing (excluding minor repairs and maintenance in the Parking Office and cashier stations).
- ix. Inform the Contractor of repairs, modifications and other activities which may cause interruption of routine parking services.
- x. Maintain access systems (locks, keys and inventory control).

- xi. Add to or replace revenue control equipment as needed.

## **SECTION VI: REVENUE AND REPORTS.**

### **A. Collection of Revenue**

Contractor shall charge, collect and handle all parking fees and charges in strict accordance with the terms of this Agreement. All traffic entering any of the Parking Facilities will do so only via sequentially numbered tickets or authorized monthly access control device. If ACH payments will be accepted at any point (online/monthly) need to specify daily settlement and NACHA rule compliance. The accepted forms of payment shall be cash, check, credit card, and payroll deduction. City of Denver shall deliver any and all advices and documents pertaining, but not limited, to counterfeit money, dishonored checks, and deposit corrections and the like to the Contractor's Controller or its designee immediately upon receipt.

### **B. Cash Losses**

All cash losses including cashier shortages and those arising from the criminal acts of Contractor's employees or third parties shall be the responsibility of Contractor and reimbursed to the City and County of Denver.

### **C. Gross Revenues**

Gross Revenues shall mean all monies, paid or payable to Contractor for transactions made and for services rendered by Contractor under this Agreement regardless of when or where the services are rendered, whether paid or unpaid, whether on a cash or credit basis. Monies payable to the City and County of Denver shall include, but not be limited to, any and all cashier shortages and overages. Dishonored checks and, uncollected/insufficient funds amounts shall not be included in Gross Revenues.

### **D. Deposit of Gross Revenue**

Contractor shall deposit all funds collected at a frequency directed by the city in an account established by and to the credit of the City and County of Denver, or in other depository as directed in writing by the City and County of Denver.. It shall be considered that the City and County of Denver has come into possession of the deposited funds only when the bank has credited the funds to the City and County of Denver account.

### **E. Documented Revenue Controls and Revenue Enhancements**

Contractor shall maintain the minimum revenue controls and procedures set forth in this Article. Private Operator shall create and maintain forms, policies, procedures, and objective performance benchmarks necessary to provide clear and concise "chain of custody" trails. At a minimum, Contractor shall maintain documentation, in a reasonable form and format to be determined by the City and County of Denver, verifying that the following activities are routinely followed:

#### **1. Revenue Reports**

- i. Cashier (Shift) Reports- All activity of cashiers' shifts
- ii. Daily Facility Summary – Roll-up or master of all shifts for a facility
- iii. Daily Deposit Summary – Breakdown on cash bank deposits
- iv. Revenue Summary – Breakdown of revenue collected by month by facility by category of revenue (i.e. Monthly, Event, Validation, etc.)

2. Cashier Accuracy
  - i. Cashier Over/Short – Tracks revenue shortages/overages by cashier by month;
  - ii. Cashier Overring/Underring – Tracks cashier errors and performance;
  - iii. Balance Due Register – Tracks collection efforts on bad debts, such as returned checks;
  - iv. Daily Cash Audit – Reconciliation of tickets collected to cash and cash equivalents deposited.
3. Ticket Controls
  - i. Ticket Inventory – Documents tickets as they are purchased and placed in inventory;
  - ii. Ticket Loading Logs – Documenting the acquisition and installation of tickets;
  - iii. Ticket Reconciliation – Reconcile parking tickets issued to parking tickets collected;
  - iv. Ticket Summaries – Details of ticket collected by month sorted by type or increment.
4. Monthly Controls
  - i. Monthly Card Inventory – Documents Monthly Cards as they are purchased and placed into inventory;
  - ii. Monthly Card Issuance – Tracks issuance and Monthly cards;
  - iii. Monthly Card Reconciliation – Reconcile active card to billed cards.
5. Validation Controls
  - i. Validation Inventory – Documents validations as they are purchased and placed into inventory
  - ii. Validation Coupon Logs – Tracks issuance and sale of validation coupon books
  - iii. Validation Coupon Reconciliation – Reconciles coupon books sold to revenue by month

#### F. Monthly Report

Contractor shall provide, by the 15th of each month, a report summarizing all activity at each Parking Facility for the preceding month in a form and format to be approved by the City and County of Denver. This monthly report shall include a cash-based income and expense statement that shall tie to deposits and expenditures and shall identify each revenue/expense category by line item with a Month and year to date result. Contractor shall also provide a management analysis and commentary on monthly results, plus recommendations and suggestions for operational and financial improvement. Contractor shall explain in reasonable detail in the monthly report any budget variances in excess of 2%. The preparer and Contractor Facility Manager shall sign the reports. This report will be the basis for the amounts to be reimbursed to Contractor by the City and County of Denver. Contractor shall reconcile discrepancies in any of the reports within three (3) working days of discovery of the discrepancy. The City and County of Denver may, with ten (10) days written notice to Contractor, add, delete or modify the type and frequency of the periodic reports at any time.

#### G. Annual Operating Budget

Contractor shall prepare a proposed detailed annual operating budget on a form(s) provided by the City and County of Denver detailing the projected revenues, expenses, parking rates for the upcoming fiscal year. Starting with the second year of this Agreement, Contractor shall submit this report no later than January 31 of each year. The City and County of Denver, exercising reasonable judgment, shall approve or disapprove the proposed annual operating budget or portions of the categories of expenses or individual items contained in the annual operating budget.

All Unbudgeted and Unapproved expenses including Payroll and Payroll Related Expenses will not be

reimbursed unless approved in writing by the City and County of Denver prior to implementation and or purchase. The Unbudgeted and Unapproved Payroll and the resulting Payroll Related Expenses will include but not limited to, additional coverage, additional staffing, and pay rate increases other than approved annual merit increases.

#### H. Monthly Card Reconciliation Report

Every month Contractor shall perform a “Monthly Card Reconciliation Report.” Such reconciliation shall include but not be limited to an analysis of all monthly parking cards, both revenue and non-revenue producing cards, and all amounts due from such cards and reconcile Contractor operating system with its financial systems. Contractor shall submit such report to the City and County of Denver in a form approved by the City and County of Denver.

#### I. Monthly Parking Tickets Reconciliation Report.

Contractor shall reconcile parking tickets issued to parking tickets collected on a daily basis. The difference will be reported as “Missing Tickets,” which shall mean any parking ticket for which transaction data has been recorded on the cash register journal tape but Contractor cannot produce the actual ticket.

Contractor shall be responsible for all Missing Tickets in excess of 0.5% of the total cash parking tickets sold on a daily basis. In such event Contractor will be charged the maximum daily rate for each missing ticket which amount will be deducted from Contractor’s management fee. Missing tickets be adjusted for exception events that are outside Contractor’s control or are previously agreed upon as exception events. An exception event that causes ticket loss shall be documented and shall not count against the ticket loss. Examples of these exception events shall include equipment failure outside of our control, severe weather, power or communication loss, dates when gates are raised post event, and ad-hoc special requests of the theaters.

The Monthly Parking Tickets Reconciliation Report shall be based on the daily parking ticket reconciliation reports and shall include the transaction date, time, exit lane number, cashier's name transaction number and amount collected.

Contractor shall be responsible for all missing tickets in excess of 0.5% as set forth in this contract. Contractor shall be charged the maximum daily rate at the applicable City and County of Denver parking facility rate for each missing ticket and the total shall be deducted from Contractor’s management fee.

### **SECTION VII: DAMAGES**

#### A. Operational

Documented violations by the Contractor of any of the duties and requirements listed in this Scope of Work will result in the assessment of a one hundred-dollar (\$100.00) penalty, per violation, which will be deducted from the Contractor’s management fee.

#### B. Reporting

The Contractor shall provide accurate monthly reports and supporting documentation for reimbursable expenses to the City no later than the fifteenth (15th) of each calendar month and shall deliver other accurate reports no later than the agreed upon schedule of time. If the Contractor fails to provide said service level, the City shall be entitled to a credit against the monthly management fee payable to Contractor equal to the lesser of a lump sum of one hundred dollars (\$100.00)

or fees of fifty dollars (\$50.00) per page per erroneous report as fixed and agreed upon liquidated damages and not as a penalty against the Contractor for each day or fraction of a day the reports are delivered later than set forth above. The City otherwise reserves all of its legal and equitable rights with respect to any breach or default of the Management Agreement.

Repeated inaccuracies, illegibleness, or other evidence of negligent management in the distribution of reports shall constitute, in the sole discretion of the City, cause to terminate this agreement.

**C. Deposits**

The Contractor shall deposit the monies collected into designated City bank account(s) at a frequency directed by the city.

The Contractor shall monitor, maintain and keep records for the electronic pay station and cashier station change fund balances and replenish as needed. The City may provide the Contractor with change funds sufficient for each Garage(s) operation, however, it is expected that the Contractor will be responsible for providing a sufficient change fund needed to appropriately operate each pay station and cashier booth effectively. The estimated total change fund amounts for each Garage is: Denver Performing Arts Complex

\$6,000. Change fund amounts for the Garage must be approved in writing by the City.

**D. Credit Card Settlements**

The Contractor will settle credit cards daily, concurrent with closing the Garage. The Contractor will send credit card settlement reports to Denver Arts and Venues Finance and Administration within 24 hours (Monday through Friday). If cards are handled by cashiers, they shall be managed in accordance with RIDSS and card data shall not be recorded in any way. The parties agree that City is the merchant of record on all revenue control equipment and as such any credit card revenue will be deposited directly into City's bank account from the revenue control equipment.

**SECTION VIII: MAINTENANCE AND CLEANING**

**A. Overall parking garage cleanliness will be the responsibility of the Contractor.**

**B. General Guidelines**

1. The entire Garage, driveways, walkways, islands, curbs, etc., must be power washed at least once a year, unless otherwise approved by the City. The Garage washing should be done during warm weather on an on-going schedule to be approved in writing by the City.
2. The entire Garage must be power vacuum/swept at least quarterly or at the request of the City. A schedule of power sweeping must be approved by the City.
3. Clean all revenue control devices at least once per week, or as needed.

4. Clean all electric vehicle charging station devices at least once per week, or as needed.
5. Clean all Garage handrails (including supporting rails) at least once per week, or as needed.
6. Clean all elevators at least daily; this includes door tracks, walls, ceiling, floors and doors. Interior and exterior of doors to be cleaned daily or as necessary.
7. All Garage interior and exterior stairwells shall be swept, vacuumed, or wet mopped at least once per week and or as often as necessary.
8. All Garage air vent louvers and overhead piping shall be cleaned at least once per month, and/or as often as necessary.
9. The Garage cashier's booth shall be cleaned as often as necessary, inside and out to achieve a clean and professional appearance.
10. All Garage windows shall be cleaned at least once per month, and as often as necessary.
11. All walkways, islands, curb areas, and stairwells must be hand-swept at least weekly, or as needed or requested by the City. Certain areas may allow cleaning by air blower, however must be approved in writing by the City.
12. Empty all garbage cans at least twice per week, or more if needed, into a central dumpster. City provides disposal.
13. Clean all Garage signage at least once per month or as needed.
14. Daily check for oil and fuel leaks from automobiles. If oil or fuel leaks are identified, immediately place oil or fuel absorbing compound on all spots then sweep-up and remove the compound. This oil or fuel-soaked compound is now considered hazardous material and must be disposed of properly.
15. Keep all sidewalks, Garage entrances and stairwells free of any ice and/or snow.
16. Re-paint parking stall and drive lane lines at least once per year, or as needed.
17. Trash cans should be emptied daily and/or when more than 2/3 full
18. The City will plow accumulates snow on the top level of the garage and ramps leading to the top level. The Contractor may be requested to contract plowing services if City services are unavailable. It will be the responsibility of the Contractor to close level off to vehicles and pedestrians for safety as directed by the City. The use of a metal plow blade is not allowed. To de-ice top level of Garage, the Contractor will only use garage safe de-icer (Calcium Magnesium Acetate (CMA)), approved by the City. Any other use of an un-authorized de-icer may damage the concrete and may require the Contractor to make the necessary repairs at their own costs.



19. The Contractor will maintain the interior of the Parking Manager's offices, adjacent areas, and additional offices or areas as directed, to the highest degree of cleanliness and order. Office furniture and equipment will at all times be presentable and businesslike. Also, painting of walls and ceilings of same, and cleaning of all carpets and windows.
20. Inspect and clean all Garage signage at least once per week, or as needed.
21. Keep all sidewalks and pedestrian walkways free of any ice and/or snow.
22. Daily check for loose or moved parking blocks/wheel stops. If loose or moved blocks are identified, they are to be immediately replaced and secured.

A detailed maintenance/janitorial schedule including daily, weekly, monthly and annual duties will be generated by the Contractor in conjunction with the City within thirty (30) days of the contract start date. This schedule can be modified at any time with City approval. Changes must be approved in writing by the City.

## **SECTION IX: OPERATIONS**

### **A. Responsibilities**

#### **1. Contractor shall:**

- i. Provide complete operational control of whole Garages and Lots as directed by the City.
- ii. Supervise the use of the Garage by all parkers. Use of reserved spaces will be monitored.
- iii. For revenue control, the Contractor's manager will be required to provide continual attention to established revenue control procedures. The size and complexities of the Garage makes such procedures an essential part of the overall operations.
- iv. The Contractor's resident manager shall meet on a monthly basis with the City to coordinate Garage operations and to discuss the monthly financial and expenditure package.
- v. The Contractor's resident Manager, at the direction of the City, shall meet on an as needed basis with the City to coordinate any event.
- vi. Purchase and pay for all approved supplies, required under this Agreement, for the parking operation.
- vii. Provide a list of personnel, including emergency telephone numbers, shall be provided to the City, and updated as necessary.
- viii. Provide assistance to Garage customers, such as directions and minor car care (i.e., flat tire assistance, battery starting, aid in locating their vehicle)

#### **2. The City shall:**

- i. Establish and/or approve Garage operating rates and hours of operation
- ii. Pay all Garage related utilities

- iii. Appoint a designated contract administrator who shall serve as the Contractor's primary contact with the City.

## B. Monthly Parking

Contractor may sell monthly or other long-term parking spaces to potential customers and exercise adequate accounting control over access device distribution utilizing procedures approved by the City. The individual lot allocations of monthly permits sold must be approved, in advance, by the City.

Monthly parking shall be handled so that all permits/parking devices issued are verified against a list of monthly accounts in the Contractor's billing system. The common factor for verification will be: name on account, phone number, access device/permit number, License plate number and Garage access method/level.

Monthly parkers will pay in advance, unless approved by the City. Monthly accounts shall be paid by the fifth (5<sup>th</sup>) of the month and any accounts not paid by the tenth (10<sup>th</sup>) shall be deactivated unless otherwise approved by the City. Appropriate action at that time will be the cancellation of the parking device or charge for the issuing of daily/hourly parking.

Monthly parkers will be required to fill out a "Monthly Parker" contract and be familiar with the rules that apply to the contract and the Garage. The Contractor will issue all monthly permits/access devices and manage all paper or electronic applications. Deposits on monthly permits/access devices along with the amount, accounting and reporting procedures must be approved in writing by the City.

The monthly parking contract issued by the Contractor must be approved in writing by the City. The City shall have the right to edit and/or modify the parking contract, at any time, as deemed necessary.

## C. Cash Management

All currency, coins, and/or checks shall be deposited via armored courier at least once each day, Monday through Saturday. Copies of all deposit records must be maintained by the Contractor and available for review within 24 hours by the City. Any alterations to this schedule must be approved in writing by the City, in accordance with the Department of Finance Cash, Risk and Capital Funding Division Receipting Requirements for City Funds.

Locked collection canisters will be taken from each pay station machine by the Contractor's facility manager, or an authorized employee, to an authorized secure location. The Contractor will then unlock, reconcile, and deposit the revenue from the canisters into a City account via armored car service. At least two (2) authorized employees must be present during the entire collection process. The Contractor's authorized list of collection employees must be approved in advance by the City.

Deposits shall be broken down by cash, coins and checks. Monthly parking sales must be deposited on a separate deposit slip from transient and special event receipts. Bank deposit slips will be provided to the Contractor at no charge.

All deposits shall be made with a 3-part bank deposit slip. Copies of the deposit slips go to the following recipients:

1. Bank
2. Denver Arts and Venues Finance
3. Contractor File

All money and collection canisters, including spares, shall be kept locked up at all times in a secured safe. All Contractor cash counting shall be conducted in a designated locked and secure area. These coin orders are received from the bank via armored courier currently – if this continues, secure handling of coin orders should be referenced here also.

Modifications to the cash management program must be approved in writing by the City.

#### D. Audit Program

The Contractor in conjunction with the City will generate a detailed financial and operational audit program for each Garage within sixty (60) days of the execution of this Agreement. The audit program must be approved in writing by the City. Modifications to the audit program must be approved in writing by the City.

#### E. Special Policies and Procedures

##### 1. Free or Discounted Parking

A list of signatures authorized to provide free or discounted parking shall be kept on file (along with authorization letters) in the manager's office and in each cashier's booth. Authorization of free or discounted parking must be approved in writing through the City.

##### 2. Validations

Provide a parking validation program option to parkers with approval in writing by the City.

##### 3. Employee Parking

Contractor employees shall be issued free access devices and shall be recorded in the monthly billing list accordingly. While on duty, all Contractor employees can park in an approved designated area. The designated areas must be approved in writing by the City. Off-duty and other Contractor employees do not have parking privileges.

##### 4. Event Parking

The facility manager shall remain alert to all special events in their respective facilities and the surrounding area that may potentially impact the Garage. Special events can cause unusual traffic demands and the facility manager must staff accordingly to efficiently manage the demand of any event. Staffing and event plans must be provided to the City in advance.

##### 5. Traffic Control

The Contractor is responsible for maintaining efficient ingress and egress traffic flow within the parking facilities by directing patrons to available parking, preventing traffic delays and directing patrons away from areas that are full. This control may include closing the entire Garage when it becomes full. If the Garage becomes full, the Contractor must notify the Arts Complex Communications Center immediately. The Contractor must re-open the Garage as soon as vacancy permits. The Contractor must also notify the Arts Complex Communications Center immediately upon re-opening. The Contractor shall keep a detailed log for each Garage of full and re-open dates and times. This log shall include, at a minimum, the date and time when the Garage was full or re-opened and any pertinent notes associated with each event.

Event management plans for each Garage must be created by the Contractor and approved in

writing by the City within sixty (60) days of the Agreement start date. Modifications to the event management plans must be approved in writing by the City.

## 6. Enforcement

The City will perform primary enforcement of the Garage on a daily basis. The Contractor may provide enforcement services on as needed and determined by the City. If City determines use of Contractor Enforcement, all vehicles not properly paying for parking will be issued a Contractor violation notice that outlines a violation fee schedule for the non-paying customer to follow. The Contractor violation fee schedule needs to be approved, in advance, by the City.

## SECTION X: SECURITY

### A. Facility Security

#### 1. Keys and Combination Codes

The Contractor will exercise extreme care to assure that keys and combination codes that have been assigned to the Contractor (i.e., office and to various pieces of revenue control equipment) are restricted only to those personnel needing the keys to perform their duties properly. The Contractor will keep a log or master list of who has keys to which doors and pieces of equipment. The City must approve the list of the authorized personnel.

#### 2. General

- i. Do not prop open pedestrian or stairwell doors for any reason.
- ii. Check for one-way “free exit” from all Garage level doors, to all stairwells and then to the outside per Fire Department regulations, and that the same doors close with auto closures.
- iii. Cashier booth doors and windows to remain locked at all times, when not occupied.

### B. Security of Records

#### 1. Receipts

All receipts collected are the responsibility of the Contractor until deposited into the City’s bank account. All money collected will be kept in the locked drop safe and only a limited number of employees will have access to these funds. The list of approved employees must be approved in writing by the City. The approved employees will have access to these moneys for counting and preparation of daily bank deposits. The safe combination and the locks to the count room will be changed by the Contractor whenever an employee, having access to these areas, leaves employment of the Contractor.

#### 2. Parking Entry/Exit Tickets, Validations and Citations

The Contractor shall be responsible for protecting from theft or misuse all parking entry/exit tickets, validations, and citations collected and will be held accountable for all of these purchased items. All voided tickets must be identified with a description of the reason for which it was voided. The Contractor will provide a separate reporting category for voided tickets and process them with the daily reports. All mutilated, damaged, “found” or not regularly transacted tickets will be voided

and maintained in the same manner. All entry/exit tickets and validations will be stored in a locked area and dispensed by authorized personnel. The City must approve the list of the authorized personnel.

3. Storage of Collected Transaction Tickets

All original collected entry/exit and validation tickets will be stored by date, cashier and shift. These original transaction tickets will be stored in a manner so as to be available for inspection within 24 hours from the time of request. All transaction tickets will be stored for audit for three (3) years.

4. Filing of Charges of Destruction of Public Property

Any individual observed breaking gate arms or damaging City-owned equipment or property is to be reported to the police and charges of destruction of public property are to be filed with the police. The Contractor employees are to be trained to obtain a license plate number and description of the driver in such instances to better aid the police.

5. Filing of Accident Reports for Personal Injury to Patrons

The Contractor will prepare an accident report and obtain pictures for any injury to a patron within the Garage in conjunction with the Arts Complex security team. The report will discuss in detail the nature of the injury (accidental or assault), the specific location, parties involved, first aid administered, etc. The Contractor report will be delivered to the City within 24 hours of the incident and kept on file in the Garage office.

6. Damage to Customers' Vehicles

Any customer whose vehicle is damaged in the Garage(s) and who requests assistance is to be instructed to file an Incident Report. A copy of the incident report will be delivered to the City within 24 hours of the incident and kept on file in the Garage office.

7. Emergencies

Within thirty (30) days of the contract start date, the Contractor will be responsible to have a plan approved by the City for any emergency that a minimum will include: attempted robberies, natural disasters, injuries to employees or the public, and fires. The Contractor will ensure their employees are well trained and able to respond according to this emergency plan.

New process for security of records will be implemented when new PARCS equipment is installed.

## **SECTION XI: STAFFING AND PERSONNEL**

The Contractor shall provide qualified personnel with a professional demeanor to perform all required operational and maintenance/janitorial duties at the Garage. Contractor personnel shall always be clean and neat and shall deal with parking patrons in a prompt, polite and business-like manner. All Contractor personnel will comply with the City's and Contractor's general rules for employee conduct.

The Contractor shall always maintain adequate personnel to provide the level of service required to meet the needs of the Agreement.

No food or beverages are permitted near City-owned equipment such as fee computers, revenue control equipment, and office equipment.

A staffing plan for the Garage must be approved in writing by the City. Changes to the staffing plans must also be approved in writing by the City.

Prior to hiring, all resumes of the Contractor's management and supervisory staff supporting this Agreement must be approved in writing by the City.

Employee incentives programs must be requested in writing and approved in writing by the City. Employee incentive programs may or may not be approved pending the details of the request.

A. Management Staff:

1. Account Manager/Supervisor (portion of salary) – Available to the City 24/7
2. Bookkeeper/Supervisor (portion of salary) – Available to the City 8 a.m. – 5 p.m., Monday – Friday. It is not the intent of the City to reimburse the full salary of management staff as these services are not needed on a full-time basis, however Contractor management must spend a percentage of their time dedicated to successfully and professionally manage this contract.
3. Management Operator will present options to reduce cost with management and office personnel. Account Manager must be available on weekdays/weekends during special events. Management/Office staff is subject to change as we automate garages.

B. Uniforms

All attendants, security personnel, cashiers, maintenance personnel, and shift supervisors will wear uniforms at all times while on duty. The Contractor shall provide uniforms for employees, at no expense to the employees, except as indicated herein. Uniforms will be purchased by the Contractor and, as this is a reimbursable expense, all uniforms are the property of the City and County of Denver. Uniforms that are soiled, stained, torn, disheveled or in any way, ill-fitting or unsightly, must be replaced by the Contractor at no expense to the employee. However, employees will not be exempt from replacement or repair costs resulting from employee's acts of negligence, vandalism, or abuse of the uniform. The uniform must have the identification insignia of the Contractor as well as an employee photo identification badge. At no time will the Contractor's employees be permitted to wear any clothing or optional item which differs from the approved uniform. Uniforms must be approved in writing by the City.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

**SECTION XII: PARKING RATES AND HOURS OF OPERATION**

**A. Current Rates**

Rates are decided upon by the City. Following are the regular rates prior to COVID:

**1. Denver Performing Arts Complex Garage (1055 13th Street)**

Reg. Monthly:	\$195.00
Reserved:	\$225.00
Transient:	
Early Bird (in by 7:30am-out by 6pm)	\$9.00
0-1 hour	\$5.00
1-2 hours	\$7.00
2-5 hours	\$10.00
5-12 hours	\$16.00
12-24 hours	\$21.00
Additional 12 hours	\$21.00
Performer Pass	\$7.00
Event Pre-Pay (M-Thu after 2 p.m.)	\$12.00 (Flat)
Event Pre-Pay (Friday after 2pm - Sat & Sun All Day)	\$15.00 (Flat)

**2021 Performing Arts Garage Current COVID Rates**

< 1 hours	\$3.00
1-2 hours	
2-5 hours	\$6.00
5-12 hours	
12-4 hours	\$10.00
Early Bird	

The Contractor is expected to submit Garage rate structure recommendations, to include area rate and occupancy surveys, at a minimum of every six months to the City for review. Modifications to all Garage rate structures must be approved in writing by the City.

**B. Hours of Operation**

The hours of operation, for each individual Garage, is decided by the City. Following are the current hours of operations for the Garage:

- Denver Performing Arts Complex Garage: Open 24 hours a day, 7 days a week, 365 days a year

Facility hours of operation are subject to change, at any time, with the City’s written notice.

Exhibit B  
Fees and Proposed Budget





OPERATIONS	MONTHLY FEES	YEARLY FEES
DPAC	\$4,083.00/month	\$48,996.00/year
TOTAL FEES	\$4,083.00/month	\$48,996.00/year

As your valued partner, it has always been our intent to remain fiscally responsible in our fee. This is why **SP+** has not increased or changed the management fee in the 12 years of our partnership. We hope that **SP+** can continue to bring more and more value to our partnership with you.

ON-CALL, AS-NEEDED HOURLY RATES

Contractor Name: SP Plus Corporation

List **ALL** potential firm personnel titles/classification that may be utilized under the Agreement for on-call, as-needed services, and their respective hourly rate. Do not list names of personnel, only titles (i.e. Project Manager). Provide additional sheets as necessary.

Title/Classification	Responsibilities	Rate/Hr.
Maintenance Porter	Light duty janitorial and maintenance	\$18.00
Special Projects	Rate surveys, project management, administrative	\$31.25

Multiplier, which when multiplied by the direct labor rate yields the above hourly billing rate: 1.5.

The City will not compensate the contractor for expenses such as postage, mileage, parking, or telephone costs. Reproduction, if requested by the City, shall be reimbursed at actual cost if approved in advance by Project Manager. Such costs are, in all such instances, included in the hourly rates paid by the City. Reproduction of submittals requested by the City including such items as end-of-phase reports, drawings, bid documents, record drawing reproducibles, etc. are not included in the hourly rates, and will be itemized as a not-to-exceed reproducible expense and will be reimbursed at actual cost

SP+	DENVER PERFORMING ARTS COMPLEX GARAGE - EXPENSE BUDGET - RFP								
	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP
REVENUE									
Transient	105,000	108,150	111,395	114,736	120,473	126,497	105,000	105,000	110,250
Special Event	200,000	250,000	350,000	250,000	250,000	300,000	175,000	275,000	250,000
Performer Passes	20,000	25,000	30,000	20,000	20,000	30,000	15,000	25,000	25,000
Validation	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500	7,500
Monthly Regular	22,000	24,200	26,620	29,282	32,210	35,431	38,974	42,872	47,159
Monthly Reserved	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200
Other Revenue (Specify)									
TOTAL REVENUE	355,700	416,050	526,715	422,718	431,383	500,628	342,674	456,572	441,109
PAYROLL EXPENSES									
Salaries & Wages	23,234	23,234	23,234	23,234	23,234	23,234	23,234	23,234	23,234
FICA Contribution	1,777	1,777	1,777	1,777	1,777	1,777	1,777	1,777	1,777
City Occupational Tax	0	0	0	0	0	0	0	0	0
State Unemployment Tax	106	106	106	106	106	106	106	106	106
Federal Unemployment Tax	23	23	23	23	23	23	23	23	23
Work. Comp. Ins.	2,207	2,207	2,207	2,207	2,207	2,207	2,207	2,207	2,207
Other (Specify) Health & Pension	2,401	2,401	2,401	2,401	2,401	2,401	2,401	2,401	2,401
TOTAL PAYROLL EXPENSES	29,749	29,748	29,748	29,748	29,748	29,748	29,748	29,748	29,748
OTHER EXPENSES									
Uniforms & Laundry	75	75	75	75	75	75	75	75	75
Contract Labor	0	0	0	0	0	0	0	0	0
Power Washing & Stripping	300	300	300	300	300	300	300	300	300
Printing & Ticket	750	750	750	750	750	750	750	750	750
Telephone & Computer	640	640	640	640	640	640	640	640	640
R&M Waste Removal Snow	1,200	1,200	1,200	600	0	0	0	0	0
R&M -Sweepers/Scrub	0	0	0	0	0	0	0	19,000	0
R&M Bulding	1,750	1,750	1,750	1,750	1,750	1,750	1,750	1,750	1,750
Police - Event Traffic Direction	7,887	7,887	7,887	7,887	7,887	7,887	7,887	7,887	7,887
License & Fees	0	400	0	0	0	0	0	0	0
Office Supplies	200	200	200	200	200	200	200	200	200
Office Equipment	0	0	0	0	0	0	0	0	0
Garage Supplies	200	200	200	200	200	200	200	200	200
Data Processing Fees	976	976	976	976	976	976	976	976	976
Refunds	0	0	0	0	0	0	0	0	0
Liability Insurance	2,858	2,858	2,858	2,858	2,858	2,858	2,858	2,858	2,858
Auto Damage and Other Claims	0	0	0	0	0	0	0	0	0
Postage and Freight	5	5	5	5	5	5	5	5	5
Armored Car	0	0	0	0	0	0	0	0	0
Miscellaneous Expenses	303	303	303	303	303	303	303	303	303
Sphere IQ Admin - Optional Value Add	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
Sphere Remote - Optional Value Add	800	800	800	800	800	800	800	800	800
Sphere Analytics - Optional Value Add	550	550	550	550	550	550	550	550	550
Base Management Fee	4,083	4,083	4,083	4,083	4,083	4,083	4,083	4,083	4,083
TOTAL OTHER EXPENSES	23,576	23,977	23,577	22,977	22,377	22,377	22,377	41,377	22,377
TOTAL EXPENSES	53,325	53,725	53,325	52,725	52,125	52,125	52,125	71,125	52,125

ATTACHMENT 2

Exhibit C ACORD 101 (2008/01)

© 2008 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

Exhibit C  
(To Follow)

# CERTIFICATE OF LIABILITY INSURANCE

 DATE(MM/DD/YYYY)  
12/15/2021

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).**

<b>PRODUCER</b> Aon Risk Services Central, Inc. Chicago IL Office 200 East Randolph Chicago IL 60601 USA	<b>CONTACT NAME:</b> <table style="width: 100%;"> <tr> <td style="width: 50%;"> <b>PHONE</b>            (A/C. No. Ext): (866) 283-7122         </td> <td style="width: 50%;"> <b>FAX</b>            (A/C. No.): 800-363-0105         </td> </tr> </table> <b>E-MAIL ADDRESS:</b>	<b>PHONE</b> (A/C. No. Ext): (866) 283-7122	<b>FAX</b> (A/C. No.): 800-363-0105												
<b>PHONE</b> (A/C. No. Ext): (866) 283-7122	<b>FAX</b> (A/C. No.): 800-363-0105														
<b>INSURED</b> SP Plus Corporation Standard Parking Corporation IL 200 E Randolph Street, Suite 7700 Chicago IL 60601 USA	<table style="width: 100%;"> <tr> <th style="text-align: center;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: center;">NAIC #</th> </tr> <tr> <td>INSURER A: XL Insurance America Inc</td> <td>24554</td> </tr> <tr> <td>INSURER B: Greenwich Insurance Company</td> <td>22322</td> </tr> <tr> <td>INSURER C: AIG Specialty Insurance Company</td> <td>26883</td> </tr> <tr> <td>INSURER D: Navigators Specialty Insurance Company</td> <td>36056</td> </tr> <tr> <td>INSURER E: Illinois Union Insurance Company</td> <td>27960</td> </tr> <tr> <td>INSURER F: Endurance American Specialty Ins Co.</td> <td>41718</td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: XL Insurance America Inc	24554	INSURER B: Greenwich Insurance Company	22322	INSURER C: AIG Specialty Insurance Company	26883	INSURER D: Navigators Specialty Insurance Company	36056	INSURER E: Illinois Union Insurance Company	27960	INSURER F: Endurance American Specialty Ins Co.	41718
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: XL Insurance America Inc	24554														
INSURER B: Greenwich Insurance Company	22322														
INSURER C: AIG Specialty Insurance Company	26883														
INSURER D: Navigators Specialty Insurance Company	36056														
INSURER E: Illinois Union Insurance Company	27960														
INSURER F: Endurance American Specialty Ins Co.	41718														

**COVERAGES**
**CERTIFICATE NUMBER: 570090629010**
**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.


Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
B	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b>			RGE300120905 SIR applies per policy terms & conditions	01/01/2022	01/01/2023	EACH OCCURRENCE	\$9,000,000
	<input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	\$2,000,000
	<input checked="" type="checkbox"/> Contractual Liability Included						MED EXP (Any one person)	\$10,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						PERSONAL & ADV INJURY	\$9,000,000
	<input type="checkbox"/> POLICY <input type="checkbox"/> PKU-JECT <input checked="" type="checkbox"/> LOC						GENERAL AGGREGATE	\$15,000,000
	OTHER:						PRODUCTS - COMP/OP AGG	\$9,000,000
B	<b>AUTOMOBILE LIABILITY</b>			RAD943782005 AOS	01/01/2022	01/01/2023	COMBINED SINGLE LIMIT (Ea accident)	\$10,000,000
	<input checked="" type="checkbox"/> ANY AUTO						BODILY INJURY (Per person)	
	<input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	<input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	
	<input checked="" type="checkbox"/> GKLL \$5,000 SIR						Garagekeepers Limit	\$3,000,000
C	<input checked="" type="checkbox"/> <b>UMBRELLA LIAB</b>			66323408 SIR applies per policy terms & conditions	01/01/2022	01/01/2023	EACH OCCURRENCE	\$10,000,000
	<input type="checkbox"/> EXCESS LIAB	<input checked="" type="checkbox"/> OCCUR					AGGREGATE	\$10,000,000
	<input type="checkbox"/> RETENTION	<input type="checkbox"/> CLAIMS-MADE						
A	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b>			RWD300121005 AOS	01/01/2022	01/01/2023	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER	
A	ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	RWR300121105 RETRO	01/01/2022	01/01/2023	E.L. EACH ACCIDENT	\$1,000,000
							E.L. DISEASE-EA EMPLOYEE	\$1,000,000
							E.L. DISEASE-POLICY LIMIT	\$1,000,000

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

Re: Location - Denver Performing Arts Complex - 99352 - 1055 13th St. Denver CO 80202. City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers are included as additional insured on the above referenced policies except workers' compensation. Insurance charges will include all applicable premiums and costs, as well as retained exposure charges established by the Named Insured. 1/1/2022 - 1/1/2023 Crime & Excess Crime Pol #'s SAA50414480600 & XSC50414490600; \$5,000,000 OCCURRENCE. Crime coverage provides first party coverage against business related crime such as robbery & burglary, employee dishonesty, forgery or alteration, computer fraud, guest property, money orders, and counterfeit currency.

**CERTIFICATE HOLDER**
**CANCELLATION**

City and County of Denver 201 W. Colfax Dept. 611 Denver CO 80204 USA	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  <div style="text-align: center;">  </div>
---	--

Holder Identifier : 99352

570090629010



# ADDITIONAL REMARKS SCHEDULE

Page \_ of \_

AGENCY Aon Risk Services Central, Inc.		NAMED INSURED SP Plus Corporation	
POLICY NUMBER See Certificate Number: 570090629010			
CARRIER See Certificate Number: 570090629010	NAIC CODE	EFFECTIVE DATE:	

## ADDITIONAL REMARKS

**THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,**  
**FORM NUMBER:** ACORD 25 **FORM TITLE:** Certificate of Liability Insurance

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER G: Allied World Assurance Company (US) Inc	19489
INSURER H: Everest Indemnity Insurance Company	10851
INSURER I: Great American Security Ins Co	31135
INSURER J: American Guarantee & Liability Ins Co	26247

**ADDITIONAL POLICIES** If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS	
	EXCESS LIABILITY							
D				CH22RXSZ03X3YIC \$10M xs \$10M	01/01/2022	01/01/2023	Aggregate	\$10,000,000
E				XCQG27921103007 \$15M x \$20M	01/01/2022	01/01/2023	Aggregate	\$15,000,000
F				XSC30000541304 \$15M x \$35M	01/01/2022	01/01/2023	Aggregate	\$15,000,000
G				03126674 \$10M xs \$50M	01/01/2022	01/01/2023	Aggregate	\$10,000,000
H				XC8EX00125221 \$15M xs \$60M	01/01/2022	01/01/2023	Aggregate	\$15,000,000
J				AXF565834102 \$12.5M po \$25M xs \$75M	01/01/2022	01/01/2023	Aggregate	\$12,500,000
I				EXC4137639 \$12.5M po \$25M xs \$75M	01/01/2022	01/01/2023	Aggregate	\$12,500,000
							Each Occurrence	\$12,500,000

Exhibit D  
(To Follow)



TO: All Users of the City and County of Denver Prevailing Wage Schedules

FROM: Ryland Feno, OHR Compensation and Classification

DATE: March 18, 2021

SUBJECT: Latest Update to Prevailing Wage Schedules

Please find an attachment to this memorandum of all the current Office of Human Resources Prevailing Wage Schedules issued in accordance with the City and County of Denver's Revised Municipal Code, Section 20-76(c). This schedule does not include the Davis-Bacon rates. The Davis-Bacon wage rates will continue to be published separately as they are announced.

Modification No. 157  
Publication Date: March 18, 2021  
(12 pages)

Unless otherwise specified in this document, apprentices shall be permitted only if they are employed pursuant to, and individually registered in a bona fide apprenticeship program registered with the U.S. Department of Labor. The employer and the individual apprentice must be registered in a program, which has received prior approval by the U.S. Department of Labor. Any employer who employs an apprentice and is found to be in violation of this provision shall be required to pay said apprentice the full journeyman scale.

Attachments as listed above.

Office of Human Resources  
201 W. Colfax Ave. Dept. 412 | Denver, CO 80202  
p: 720.913.5751 | f: 720.913.5720  
[www.denvergov.org/humanresources](http://www.denvergov.org/humanresources)



**APPLIANCE MECHANIC****Effective Date: 02-18-21**

Last Revision: 05-16-19

\*OHR pulled the wages in February of 2021 and data has remained the same so there is no recommendation to change the base wage or fringes.

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Appliance Mechanic	\$23.21	\$7.22

Plus 10% shift differential for regularly scheduled hours worked between 6:00 p.m. and 6:00 a.m.

The Appliance Mechanic installs, services and repairs stoves, refrigerators, dishwashing machines, exercise equipment and other electrical household or commercial appliances, using hand tools, test equipment and following wiring diagrams and manufacturer's specifications. Responsibilities include: connects appliance to power source and test meters, such as wattmeter, ammeter, or voltmeter, observes readings on meters and graphic recorders, examines appliance during operating cycle to detect excess vibration, overheating, fluid leaks and loose parts, and disassembles appliances and examines mechanical and electrical parts. Additional duties include: traces electrical circuits, following diagram and locates shorts and grounds, using ohmmeter, calibrates timers, thermostats and adjusts contact points, and cleans and washes parts, using wire brush, buffer, and solvent to remove carbon, grease and dust. Replaces worn or defective parts, such as switches, pumps, bearings, transmissions, belts, gears, blowers and defective wiring, repairs and adjusts appliance motors, reassembles appliance, adjusts pulleys and lubricates moving parts, using hand tools and lubricating equipment.

Note: This position does not perform installations done at new construction.

**BUILDING ENGINEER****Effective Date: 09-17-20**

Last Revision: 08-15-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Building Engineer	\$32.50	\$8.29

This classification of work is responsible for operating, monitoring, maintaining/repairing the facilities mechanical systems to ensure peak performance of the systems. This includes performing P.M. and repair work of the building mechanical systems, inspecting, adjusting, and monitoring the building automation and life safety systems, contacting vendors and place order replacement parts, responding to customer service requests and performing maintenance/repairs I tenant or public spaces, performing routine P.M. i.e. light plumbing and electrical repairs, ballast lamp and tube replacement, operating mechanical systems both on site and via a remote laptop computer, maintaining inventory of spare parts and tools, painting and cleaning mechanical equipment and machine rooms, etc.

**CONVEYANCE SYSTEM MAINTENANCE SERIES****Effective Date: 11-19-20****Last Revision: 09-19-19**

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Entry-Support Mechanic	\$22.65	\$7.15
Machinery Maintenance Mechanic	\$27.66	\$7.73
Controls System Technician	\$30.11	\$8.01

Plus 10% shift differential for regularly scheduled hours worked between 6:00 p.m. and 6:00 a.m.

This classification was previously listed as Baggage Handling System Maintenance. The title of the series has been changed to be inclusive of other types of similar work.

**Entry Support Mechanic**

The Entry Support Mechanic (ESM) applies basic mechanical knowledge to perform maintenance and operational tasks on a conveyance system. Under supervision of a Machinery Maintenance Mechanic (MMM) or Control Systems Technician (CRO), the ESM performs cleaning, routine inspections, preventive, corrective and emergency maintenance based on an established maintenance program. The ESM clears jams and faults and may physically move items during failures.

**Machinery Maintenance Mechanic**

The Machinery Maintenance Mechanic (MMM) applies advanced mechanical knowledge to perform maintenance and operational tasks on a conveyance system. Performs cleaning of all parts of the system, routine inspections, preventive maintenance, corrective maintenance, and emergency maintenance within the system based on an established maintenance program. The MMM shall inspect all equipment for proper operation and performance including but not limited to conveyors, lifts, diverters and automatic tag readers. The MMM troubleshoots, repairs, replaces, and rebuilds conveyor components including but not limited to; motors, gearboxes, bearings, rollers, sheaves, hydraulic systems, conveyor belting, clutch brakes, tools, independent carrier systems, and other complex devices using basic hand tools, power tools, welders and specialized tools. The MMM may assist the Control Systems Technician (CST) with clearing electrical faults and electrical repairs. The MMM reads and interprets manufacturers' maintenance manuals, service bulletins, technical data, engineering data, and other specifications to determine feasibility and method of repairing or replacing malfunctioning or damaged components. The MMM clears jams and faults in the system and may physically move items during failures. The MMM will operate a Central Monitoring Facility/Control Room, these duties include; using multiple computer systems for monitoring the system and running reports, communicating faults in the system using a radio and telephone, and communicating with stakeholders. The MMM performs on-site training of ESM.

**Controls System Technician**

The Control Systems Technician (CST) applies advanced technical knowledge to perform maintenance and operational tasks on a conveyance system. Performs all duties assigned to an MMM in addition to the following routine inspections, preventive maintenance, corrective maintenance, and emergency maintenance of complex components within the system based on an established maintenance program. The CST is responsible for resolving difficult controls, electrical and mechanical problems. The CST troubleshoots, repairs, replaces, and rebuilds complex electro-mechanical systems and conveyor components including but not limited to; programmable logic controllers, input and output modules, electrical switches, variable frequency drives, 110V AC and 24V DC controls devices, automatic tag readers, electrical control panels, 110V - 480V AC components and motors, gearboxes, bearings, rollers, sheaves, hydraulic systems, conveyor belting, clutch brakes, tools, independent carrier systems, and other complex devices using basic hand tools, power tools, welders and specialized mechanical and electrical tools. The CST reads and interprets manufacturers' maintenance manuals, service bulletins, technical data, engineering data, and other specifications to determine feasibility and method of repairing or replacing malfunctioning or damaged components. The CST clears mechanical, electrical and controls faults, jams and may physically move items during failures. The CST performs on-site training and competency evaluations of MMM and ESM.

Note: Incumbents must possess an Electrician's license when work warrants.

**CUSTODIANS****Effective Date: 12-17-20**

Last Revision: 12-19-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Custodian I	\$16.43	\$6.18 (Single) \$8.02 (Children) \$7.74 (2-party) \$10.15 (Family)
Custodian II	\$16.78	\$6.24 (Single) \$8.08 (Children) \$7.80 (2-party) \$10.21 (Family)

**Benefits and Overtime**

Parking	With valid receipt from approved parking lot, employees are reimbursed the actual monthly cost of parking.
RTD Bus Pass	Employer will provide employees with the Bus Pass or pay (\$0.23) per hour for travel differential.
Shift Differential	2nd shift (2:30 p.m.-10:30 p.m.): \$.50/hour 3rd shift (10:31 p.m.-6:30 a.m.): \$1.00/hour
Overtime	Time worked in excess of seven and one-half (7 ½) hours in one (1) day or in excess of thirty-seven and one-half (37 ½) hours in one week shall constitute overtime and shall be paid for at the rate of time and one-half (1 ½) at the employee's basic straight time hourly rate of pay.
Lunch	Any employee working seven and a half (7.5) hours in a day is entitled to a thirty (30) minute paid lunch.
Note	The Career Service Board in their public hearing on March 15, 2007 approved to amend prevailing wages paid to the Custodian as follows: "All contractors shall provide fringe benefits or cash equivalent at not less than the single rate amount. Contractors who offer health insurance shall provide an employer contribution to such insurance of not less than the 2-party or family rate for any employee who elects 2-party or family coverage. Contractors who offer such coverage will be reimbursed for their employer contributions at the above rates under any City contract incorporating this wage specification."

**Custodian I**

Any employee performing general clean-up duties using equipment that does not require special training: i.e., dust mopping, damp mopping, vacuuming, emptying trash, spray cleaning, washing toilets, sinks, walls, cleaning chairs, etc.

**Custodian II**

Any employee performing specialized cleaning duties requiring technical training and the use of heavy and technical equipment, i.e., heavy machine operators, floor strippers and waxers, carpet shampooers, spray buffing, re-lamping, mopping behind machines, high ladder work, chemical stripping and finishing of stainless steel.

**DIA OIL & GAS****Effective Date:** 03-18-21

Last Revision: 04-16-20

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Derrick Hand/Roustabout	\$15.94	\$6.38
Electrician	\$26.44	\$7.59
Mechanic	\$26.55	\$7.60
Pipefitter	\$27.10	\$7.67
Rig/Drill Operator	\$23.80	\$7.29
Truck Driver	\$24.32	\$7.35

**Heavy Equipment Mechanic (Mechanic)**

The Heavy Equipment Mechanic analyzes malfunctions and repairs, rebuilds and maintains power equipment, such as cranes, power shovels, scrapers, paving machines, motor graders, trench-digging machines, conveyors, bulldozers, dredges, pumps, compressors and pneumatic tools. This worker operates and inspects machines or equipment to diagnose defects, dismantles and reassembles equipment, using hoists and hand tools, examines parts for damage or excessive wear, using micrometers and gauges, replaces defective engines and subassemblies, such as transmissions, and tests overhauled equipment to insure operating efficiency. The mechanic welds broken parts and structural members, may direct workers engaged in cleaning parts and assisting with assembly and disassembly of equipment, and may repair, adjust and maintain mining machinery, such as stripping and loading shovels, drilling and cutting machines, and continuous mining machines.

**Pipefitter**

The Pipefitter, Maintenance installs or repairs water, steam, gas or other types of pipe and pipefitting. Work involves most of the following: laying out work and measuring to locate position of pipe from drawings or other written specifications, cutting various sizes of pipe to correct lengths with chisel and hammer, oxyacetylene torch or pipe-cutting machines, threading pipe with stocks and dies. This person is responsible for bending pipe by hand-driven or power-driven machines, assembling pipe with couplings and fastening pipe to hangers, making standard shop computations relating to pressures, flow and size of pipe required; and making standard tests to determine whether finished pipes meet specifications. In general, the work of the Maintenance Pipefitter requires rounded training and experience usually acquired through a formal apprenticeship or equivalent training and experience.

**Well Driller (Rig/Drill Operator)**

This incumbent sets up and operates portable drilling rig (machine and related equipment) to drill wells, extends stabilizing jackscrews to support and level drilling rig, moves levers to control power-driven winch that raises and extends telescoping mast. This person bolts trusses and guy wires to raise mast and anchors them to machine frame and stakes, and assembles drilling tools, using hand tools or power tools. The Well Driller moves levers and pedals to raise tools into vertical drilling position and lowers well casing (pipe that shores up walls of well) into well bore, using winch, moves levers and pedals and turns hand wells to control reciprocating action of machine and to drive or extract well casing.

**Laborer (Derrick Hand/Roustabout)**

The Laborer performs tasks that require mainly physical abilities and effort involving little or no specialized skill or prior work experience. The following tasks are typical of this occupation: The Laborer loads and unloads trucks, and other conveyances, moves supplies and materials to proper location by wheelbarrow or hand truck; stacks materials for storage or binning, collects refuse and salvageable materials, and digs, fills, and tamps earth excavations, The Laborer levels ground using pick, shovel, tamper and rake, shovels concrete and snow; cleans culverts and ditches, cuts tree and brush; operates power lawnmowers, moves and arranges heavy pieces of office and household furniture, equipment, and appliance, moves heavy pieces of automotive, medical engineering, and other types of machinery and equipment, spreads sand and salt on icy roads and walkways, and picks up leaves and trash.

**Truckdriver**

Straight truck, over 4 tons, usually 10 wheels. The Truckdriver drives a truck to transport materials, merchandise, equipment, or workers between various types of establishments such as: manufacturing plants, freight depots, warehouses, wholesale and retail establishments, or between retail establishments and customers' houses or places of business. This driver may also load or unload truck with or without helpers, make minor mechanical repairs, and keep truck in good working order.

**ELEVATOR MECHANIC**

Effective 1-18-2018, the Elevator Mechanic classification will utilize the base pay and fringe benefits for the Elevator Mechanic classification under the Davis Bacon [Building Wage Determination](#).

**FINISHER & JOURNEYMAN**

TILE, MARBLE AND TERRAZZO

**Effective Date:** 11-19-20

**Last Revision:** 06-20-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Finisher	\$23.20	\$8.46
Journeyman	\$29.15	\$8.46

Effective May 1, 2008, Local Union 7 of Colorado combined three classes of Finishers, Floor Grinders, and Base Grinders into Finisher using one pay schedule.

Tile Setter: Applies to workers who apply tile to floors, walls, ceilings, stair treads, promenade roof decks, garden walks, swimming pools and all places where tiles may be used to form a finished surface for practical use, sanitary finish or decorative purpose.

**FIRE EXTINGUISHER REPAIRER**

**Effective Date:** 07-16-20

**Last Revision:** 07-19-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Fire Extinguisher Repairer	\$20.72	\$6.93

The Fire Extinguisher Repairer performs the following duties: repairs and tests fire extinguishers in repair shops and in establishments, such as factories, homes, garages, and office buildings, using hand tools and hydrostatic test equipment, this repairer dismantles extinguisher and examines tubing, horns, head gaskets, cutter disks, and other parts for defects, and replaces worn or damaged parts. Using hand tools, this repairer cleans extinguishers and recharges them with materials, (such as soda water and sulfuric acid, carbon tetrachloride, nitrogen or patented solutions); tests extinguishers for conformity with legal specifications using hydrostatic test equipment and may install cabinets and brackets to hold extinguishers.

**FUEL HANDLER SERIES****Effective Date: 12-17-20****Last Revision: 10-17-19**

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Fuel Facility Maintenance Technician	\$21.50	\$7.02
Fuel Facility Operator	\$23.41	\$7.24
Fuel Facility Electrician	\$26.44	\$7.59
Fuel Distribution System Mechanic	\$30.74	\$8.09
Lead Fuel Distribution System Mechanic	\$32.14	\$8.25

Plus 10% shift differential for hours worked between 6:00 p.m. and 6:00 a.m.

**Fuel Facility Maintenance Technician**

Under the supervision of Maintenance Manager and or Lead Mechanic, maintain the fuel systems. Position does not limit, segregate, or classify that an employee would not be subject to perform those duties and responsibilities within a stated contract classification. To properly identify the requirements of those duties and responsibilities within a contract classification, it may be required to review these job descriptions which identify those essential functions.

**Fuel Facility Operator**

Receives, stores, transfers, and issues fuel. Performs various testing procedures and documentation on fuel samples. Gauges tanks for water, temperature and fuel levels. Performs temperature and gravity testing for correct weight of fuel. Checks pumping systems for correct operating pressure or unusual noises. Inspects fuel receiving, storage, and distribution facilities to detect leakage, corrosion, faulty fittings, and malfunction of mechanical units, meters, and gauges such as distribution lines, float gauges, piping valves, pumps, and roof sumps. Operates a 24-hour control center; operates various computer equipment to determine potential equipment failure, leak and cathodic protection systems, pump failure, and emergency fuel shutoff systems. Monitors quality of fuel and drains excess condensation from fuel sumps and underground fuel pits. Inspects fuel tank farm for such items as leaks, low pressure, and unauthorized personnel. Performs general housekeeping and grounds maintenance for terminal, pipeline and dock areas, including fuel pits and valve vault cleaning and pump out activities. May connect lines, grounding wires, and loading and off-loading arms of hoses to pipelines. May assist Fuel Distribution System Mechanics by preparing work areas. Maintains record of inspections, observations and test results.

**Fuel Facility Electrician**

Performs preventative, routine, and emergency maintenance repairs on a variety of mechanical, electrical, HVAC systems, pneumatic control systems, electronic systems, and generators.

**Fuel Distribution System Mechanic**

Maintains and repairs fuel storage and distribution systems, equipment and filtration systems, and differential pressure valves. Corrects leakage, corrosion, faulty fittings, and malfunction of mechanical units, meters, and gauges such as distribution lines, float gauges, piping valves, pumps, and roof sumps. Inspects electrical wiring, switches, and controls for safe-operating condition, grounding, and adjustment; may make minor repairs. Lubricates and repacks valves. Lubricates pumps, replaces gaskets, and corrects pumping equipment misalignment. May clean strainers and filters, service water separators, and check meters for correct delivery and calibration. Overhauls system components such as pressure regulating valves and excess valves. Disassembles, adjusts, aligns, and calibrates gauges and meters or replaces them. Removes and installs equipment such as filters and piping to modify system or repair and replace system component. Cleans fuel tanks and distribution lines. Removes corrosion and repaints surfaces. Overhauls vacuum and pressure vents, floating roof seals, hangers, and roof sumps. Some positions maintain fuel-servicing equipment such as hydrant and tanker trucks. Maintains record of inspections and repairs and other related paperwork as required.

**Lead Fuel Distribution System Mechanic**

Performs lead duties such as making and approving work assignments and conducting on-the-job training as well as performing the various tasks performed by the Mechanic classification.

**FURNITURE MOVERS**

Moving, Storage and Cartage Workers

**Effective Date:** 11-19-20

Last Revision: 10-17-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Laborer/Helper	\$17.36	\$6.54
Furniture Driver/Packer	\$18.44	\$6.67
Lead Furniture Mover	\$19.28	\$6.76

**GLYCOL FACILITY****Effective Date:** 07-16-20

Last Revision: 06-20-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
De-icing Facility Operator	\$27.77	\$7.74
Maintenance Mechanic	\$27.64	\$7.73
Glycol Plant Specialist	\$17.36	\$6.54

**De-icing Facility Operator**

The De-icing Facility Operator is responsible for the safe and efficient daily operation of all aircraft de-icing fluid equipment to include: mechanical vapor recompression (concentrators), distillation, polishing, distribution, and collection systems as well as daily routine chores to include: operating and controlling all facility machines and equipment associates with the aircraft deicing fluid system (ADS). Operate electrical motors, pumps and valves to regulate flow, add specific amounts of chemicals such as hydrochloric acid or sodium hydroxide to fluid(s) for adjustment as required, turn valves, change filters/activated carbon, and clean tanks as needed to optimize productivity. Monitor panel boards/HMI/PLC's, adjust control flow rates, repairs, and lubricate machinery and equipment using hand powered tools. Test fluids to determine quality controlling methods. Record data as necessary and maintain good housekeeping of the facility.

**Maintenance Mechanic**

The position of the Machinery Maintenance Mechanic will be primarily responsible for the routine maintenance and repairs of all facility equipment. Responsible for repairs to machinery and mechanical equipment, examine machines and mechanic equipment to diagnose source of trouble, dismantling or partly dismantling machines and performing repairs that mainly involve the use of hand tools in scraping and fitting parts, replacing broken or defective parts with items obtained from stock, ordering replacement parts, sending parts to a machine shop or equivalent for major repairs, preparing specific written specifications for repairs, SOP's for minor repairs, reassembly of machines and mechanical equipment, and making any necessary adjustments to all equipment for operational optimization.

**Glycol Plant Specialist/Material Handling Laborer**

The Material Handling Laborer is responsible for the safe and efficient daily documentation/recording of all ADF processors, distillation and polishing systems, as well as the distribution and collection system. Performing physical tasks to transport and/or store materials or fluids. Duties involve one or more of the following: manually loading or unloading trucks, tankers, tanks, totes, drums, pallets, unpacking, placing items on storage bins or proper locations. Utilizing hand carts, forklift, or wheelbarrow. Completing daily fluid inventory, to include tank measuring and completing fluid accountability records. Responsible for the overall facility housekeeping and general cleanliness. Escort vehicles and tankers in and out of the facility, change out filters as required on all systems, take samples and test for quality control and document the findings.

**PARKING ELECTRONICS TECHNICIAN****Effective Date: 09-17-20**

Last Revision: 10-17-19

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Parking Electronics Technician	\$26.54	\$7.60

Plus 10% shift differential for regularly scheduled hours worked between 6:00 p.m. and 6:00 a.m.

This classification of work installs, modifies, troubleshoots, repairs and maintains revenue control equipment at manned and unmanned parking entrance and exit gates. Replaces consumable items such as tickets, printer ribbons, and light bulbs. Replaces modules and related equipment as needed to repair existing equipment, modify applications, or resolve unusual problems. Troubleshoots, tests, diagnoses, calibrates, and performs field repairs. Performs preventive maintenance such as inspection, testing, cleaning, lubricating, adjusting and replacing of serviceable parts to prevent equipment failure for electromechanical control to minimize repair problems and meet manufacturers' specifications.

**PEST CONTROLLER****Effective Date: 07-16-20**

Last Revision: 07-19-19

\*OHR pulled the wages in July of 2020 and data has remained the same so there is no recommendation to change the base wage or fringes.

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Pest Controller	\$20.41	\$6.90

The Pest Controller sprays chemical solutions or toxic gases and sets mechanical traps to kill pests that infest buildings and surrounding areas, fumigates rooms and buildings using toxic gases, sprays chemical solutions or dusts powders in rooms and work areas, places poisonous paste or bait and mechanical traps where pests are present; may clean areas that harbor pests, using rakes, brooms, shovels, and mops preparatory to fumigating; and may be required to hold State license

**QUALITY CONTROL & ASSURANCE TECHNICIAN****Effective Date: 03-18-21**

Last Revision: 04-16-20

<b><u>Classification</u></b>	<b><u>Base Wage/Hour</u></b>	<b><u>Fringes/Hour</u></b>
Quality Control & Assurance Technician	\$25.35	\$7.47

The Quality Control & Assurance Technician provides support to Inland Technologies operations by independently performing standard analysis on samples related to the manufacture of spent de-icing fluid to a 99% recycled glycol product and waste water discharge. The Quality Control and Assurance Technician will continually look at ways to improve products and processes to exceed customer quality demands and decrease operational costs.



**SIGN ERECTOR****Effective Date: 01-21-21**

Last Revision: 03-15-18

**Classification**

Sign Erector

**Base Wage/Hour**

\$21.09

**Fringes/Hour**

\$6.31

This classification of work erects, assembles, and/or maintains signs, sign structures and/or billboards using various tools. Erects pre-assembled illuminated signs on buildings or other structures according to sketches, drawings, or blueprints. Digs and fills holes, places poles. Bolts, screws. or nails sign panels to sign post or frame. Replaces or repairs damaged or worn signs. May use welding equipment when installing sign. This classification is not a licensed electrician and therefore cannot make connections to power sources (i.e., provide exit lighting).

**TREE TRIMMERS****Effective Date: 09-17-20**

Last Revision: 09-19-19

**Classification**

Tree Trimmer

**Base Wage/Hour**

\$21.30

**Fringes/Hour**

\$7.00

This classification of work trims, removes, and applies insecticides to trees and shrubbery including trimming dead, diseased, or broken limbs from trees utilizing rope and saddle, chain, handsaw and other related equipment common to the care of trees and shrubs. Removes limbs, branches and other litter from the work area, observes safety rules, inspects and identifies tree diseases and insects of the area distinguishing beneficial insects and environmental stress, takes samples from diseased or insect infested trees for lab analysis, operates a wide variety of heavy and power equipment in trimming and removing trees and shrubbery i.e. mobile aerial tower unit, tandem trucks, loaders, chipper, etc., maintains all equipment.

**WINDOW CLEANER****Effective Date: 12-17-20**

Last Revision: 05-21-20

**Classification**

Window Cleaner

**Base Wage/Hour**

\$26.74

**Fringes/Hour**

\$9.53 (Employee)

\$11.37 (Children)

\$11.09 (2-party)

\$13.50 (Family)

**Benefits/Overtime**

Parking	The Company shall reimburse the cost of parking (per month) to employees furnishing a monthly parking receipt from the approved parking lot. The Employer shall reimburse employees for parking expenses from other parking lots up to the amount reimbursed for DIA Employee Parking Lot upon the submission of a monthly parking receipt. Only (1) one receipt per month.
Shift Differential	Employees working on the night shift shall be awarded a shift differential of \$0.85 per hour worked.  Note: All wage increases become effective on the first day of the first full pay period following the above dates.
Overtime	One and one-half (1½) times the basic rate of pay in excess of 7.5 hours worked per day or 37.5 hours worked per week.
Lunch	Any employee working seven and a half (7.5) hours in a day is entitled to a thirty (30) minute paid lunch.
Lead Work	\$1.75 per hour above highest paid employee under supervision
High Work	\$1.85 per hour (21 feet or more from ground (base) to top of surface/structure being cleaned)
Training	\$0.25 per hour
ECOPASS	Company will provide an ECOPASS to all bargaining unit employees beginning January 1, 2009.



**TO:** All Users of the City and County of Denver Prevailing Wage Schedules  
**FROM:** Ryland Feno, Classification & Compensation Technician II  
**DATE:** January 04, 2021  
**SUBJECT:** Latest Change to Prevailing Wage Schedules

Please be advised prevailing wage rates for some building, heavy, highway, and residential construction trades have not been updated by the United States Department of Labor (DOL) since March 1, 2002. The Career Service Board, in their meeting held on April 21, 2011, approved the use of the attached supplemental wage rates until prevailing wage rates for these classifications of work are again published by the United States Department of Labor in accordance with the Davis-Bacon Act.

The effective date for this publication will be **Friday, January 01, 2021** and applies to the City and County of Denver for **HIGHWAY CONSTRUCTION PROJECTS** in accordance with the Denver Revised Municipal Code, Section 20-76(c).

General Wage Decision No. CO20210009  
Superseded General Decision No. CO20200009  
Modification No. 0  
Publication Date: 01/01/2021  
(6 pages)

Unless otherwise specified in this document, apprentices shall be permitted only if they are employed pursuant to and individually registered in a bona fide apprenticeship program registered with the U.S. Department of Labor (DOL). The employer and the individual apprentice must be registered in a program which has received prior approval by the DOL. Any employer who employs an apprentice and is found to be in violation of this provision shall be required to pay said apprentice the full journeyman scale.

Attachments as listed above.

**\*Career Service Board approved to adjust all Davis Bacon classifications under \$13.00 to comply with the city's minimum wage. The effective date is August 15, 2019. See page 7 for reference.**

Office of Human Resources  
201 W. Colfax Ave. Dept. 412 | Denver, CO 80202  
p: 720.913.5751 | f: 720.913.5720  
[www.denvergov.org/humanresources](http://www.denvergov.org/humanresources)

"General Decision Number: CO20210009 01/01/2021

Superseded General Decision Number: CO20200009

State: Colorado

Construction Type: Highway

Counties: Denver and Douglas Counties in Colorado.

#### HIGHWAY CONSTRUCTION PROJECTS

Note: Under Executive Order (EO) 13658, an hourly minimum wage of \$10.95 for calendar year 2021 applies to all contracts subject to the Davis-Bacon Act for which the contract is awarded (and any solicitation was issued) on or after January 1, 2015. If this contract is covered by the EO, the contractor must pay all workers in any classification listed on this wage determination at least \$10.95 per hour (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in calendar year 2021. If this contract is covered by the EO and a classification considered necessary for performance of work on the contract does not appear on this wage determination, the contractor must pay workers in that classification at least the wage rate determined through the conformance process set forth in 29 CFR 5.5(a)(1)(ii) (or the EO minimum wage rate, if it is higher than the conformed wage rate). The EO minimum wage rate will be adjusted annually. Please note that this EO applies to the above-mentioned types of contracts entered into by the federal government that are subject to the Davis-Bacon Act itself, but it does not apply to contracts subject only to the Davis-Bacon Related Acts, including those set forth at 29 CFR 5.1(a)(2)-(60). Additional information on contractor requirements and worker protections under the EO is available at [www.dol.gov/whd/govcontracts](http://www.dol.gov/whd/govcontracts).

Modification Number	Publication Date
0	01/01/2021

\* CARP9901-008 11/01/2019

	Rates	Fringes
CARPENTER (Form Work Only).....	\$ 26.50	10.32

-----  
ELEC0068-016 03/01/2011

	Rates	Fringes
TRAFFIC SIGNALIZATION:		
Traffic Signal Installation		
Zone 1.....	\$ 26.42	4.75%+8.68
Zone 2.....	\$ 29.42	4.75%+8.68

#### TRAFFIC SIGNAL INSTALLER ZONE DEFINITIONS

Zone 1 shall be a 35 mile radius, measured from the following addresses in each of the following cities:  
 Colorado Springs - Nevada & Bijou  
 Denver - Ellsworth Avenue & Broadway  
 Ft. Collins - Prospect & College  
 Grand Junction - 12th & North Avenue  
 Pueblo - I-25 & Highway 50  
 All work outside of these areas shall be paid Zone 2 rates.

-----  
 ENGI0009-008 05/01/2018

	Rates	Fringes
POWER EQUIPMENT OPERATOR:		
(3)-Hydraulic Backhoe (Wheel Mounted, under 3/4 yds), Hydraulic Backhoe (Backhoe/Loader combination), Drill Rig Caisson (smaller than Watson 2500 and similar), Loader (up to and including 6 cu. yd.).....	\$ 28.25	10.70
(3)-Loader (under 6 cu. yd.) Denver County.....	\$ 28.25	10.70
(3)-Motor Grader (blade- rough) Douglas County.....	\$ 28.25	10.70
(4)-Crane (50 tons and under), Scraper (single bowl, under 40 cu. yd).....	\$ 28.40	10.70
(4)-Loader (over 6 cu. yd) Denver County.....	\$ 28.40	10.70
(5)-Drill Rig Caisson (Watson 2500 similar or larger), Crane (51-90 tons), Scraper (40 cu.yd and over),.....	\$ 28.57	10.70
(5)-Motor Grader (blade- finish)		

Douglas County.....	\$ 28.57	10.70
(6)-Crane (91-140 tons).....	\$ 29.55	10.70

---

SUCO2011-004 09/15/2011

	Rates	Fringes
CARPENTER (Excludes Form Work)...	\$ 19.27	5.08
CEMENT MASON/CONCRETE FINISHER		
Denver.....	\$ 20.18	5.75
Douglas.....	\$ 18.75	3.00
ELECTRICIAN (Excludes Traffic Signal Installation).....	\$ 35.13	6.83
FENCE ERECTOR (Excludes Link/Cyclone Fence Erection).....	\$ 13.02	3.20
GUARDRAIL INSTALLER.....	\$ 12.89	3.20
HIGHWAY/PARKING LOT STRIPING:Painter		
Denver.....	\$ 12.62	3.21
Douglas.....	\$ 13.89	3.21
IRONWORKER, REINFORCING (Excludes Guardrail Installation).....	\$ 16.69	5.45
IRONWORKER, STRUCTURAL (Includes Link/Cyclone Fence Erection, Excludes Guardrail Installation).....	\$ 18.22	6.01
LABORER		
Asphalt Raker.....	\$ 16.29	4.25
Asphalt Shoveler.....	\$ 21.21	4.25
Asphalt Spreader.....	\$ 18.58	4.65
Common or General		
Denver.....	\$ 16.76	6.77
Douglas.....	\$ 16.29	4.25
Concrete Saw (Hand Held)....	\$ 16.29	6.14
Landscape and Irrigation....	\$ 12.26	3.16
Mason Tender- Cement/Concrete		
Denver.....	\$ 16.96	4.04
Douglas.....	\$ 16.29	4.25
Pipelayer		
Denver.....	\$ 13.55	2.41
Douglas.....	\$ 16.30	2.18
Traffic Control (Flagger)...	\$ 9.55	3.05

Traffic Control (Sets Up/Moves Barrels, Cones, Install Signs, Arrow Boards and Place Stationary Flags) (Excludes Flaggers).....	\$ 12.43	3.22
PAINTER (Spray Only).....	\$ 16.99	2.87
POWER EQUIPMENT OPERATOR:		
Asphalt Laydown		
Denver.....	\$ 22.67	8.72
Douglas.....	\$ 23.67	8.47
Asphalt Paver		
Denver.....	\$ 24.97	6.13
Douglas.....	\$ 25.44	3.50
Asphalt Roller		
Denver.....	\$ 23.13	7.55
Douglas.....	\$ 23.63	6.43
Asphalt Spreader.....	\$ 22.67	8.72
Backhoe/Trackhoe		
Douglas.....	\$ 23.82	6.00
Bobcat/Skid Loader.....	\$ 15.37	4.28
Boom.....	\$ 22.67	8.72
Broom/Sweeper		
Denver.....	\$ 22.47	8.72
Douglas.....	\$ 22.96	8.22
Bulldozer.....	\$ 26.90	5.59
Concrete Pump.....	\$ 21.60	5.21
Drill		
Denver.....	\$ 20.48	4.71
Douglas.....	\$ 20.71	2.66
Forklift.....	\$ 15.91	4.68
Grader/Blade		
Denver.....	\$ 22.67	8.72
Guardrail/Post Driver.....	\$ 16.07	4.41
Loader (Front End)		
Douglas.....	\$ 21.67	8.22
Mechanic		
Denver.....	\$ 22.89	8.72
Douglas.....	\$ 23.88	8.22
Oiler		
Denver.....	\$ 23.73	8.41
Douglas.....	\$ 24.90	7.67
Roller/Compactor (Dirt and Grade Compaction)		
Denver.....	\$ 20.30	5.51
Douglas.....	\$ 22.78	4.86
Rotomill.....	\$ 16.22	4.41
Screed		
Denver.....	\$ 22.67	8.38
Douglas.....	\$ 29.99	1.40

Tractor.....	\$ 13.13	2.95
--------------	----------	------

## TRAFFIC SIGNALIZATION:

## Groundsman

Denver.....	\$ 17.90	3.41
Douglas.....	\$ 18.67	7.17

## TRUCK DRIVER

## Distributor

Denver.....	\$ 17.81	5.82
Douglas.....	\$ 16.98	5.27

## Dump Truck

Denver.....	\$ 15.27	5.27
Douglas.....	\$ 16.39	5.27

Lowboy Truck.....	\$ 17.25	5.27
-------------------	----------	------

Mechanic.....	\$ 26.48	3.50
---------------	----------	------

## Multi-Purpose Specialty &amp;

## Hoisting Truck

Denver.....	\$ 17.49	3.17
Douglas.....	\$ 20.05	2.88

## Pickup and Pilot Car

Denver.....	\$ 14.24	3.77
Douglas.....	\$ 16.43	3.68

Semi/Trailer Truck.....	\$ 18.39	4.13
-------------------------	----------	------

Truck Mounted Attenuator...	\$ 12.43	3.22
-----------------------------	----------	------

## Water Truck

Denver.....	\$ 26.27	5.27
Douglas.....	\$ 19.46	2.58

---

WELDERS - Receive rate prescribed for craft performing  
operation to which welding is incidental.

=====

**Office of Human Resources  
Supplemental Rates  
(Specific to the Denver Projects)  
Revised 08/21/2019)**

<b>Classification</b>		<b>Base</b>	<b>Fringe</b>
Guard Rail Installer		\$13.00	\$3.20
Highway Parking Lot Striping: Painter		\$13.00	\$3.21
Ironworker (Ornamental)		\$26.05	\$12.00
Laborer	Removal of Asbestos	\$21.03	\$8.55
Laborer (Landscape & Irrigation)		\$13.00	\$3.16
Laborer: Traffic Control (Flagger)		\$13.00	\$3.05
Laborer: Stationary Flags( excludes Flaggers)		\$13.00	\$3.22
Line Construction	Lineman, Gas Fitter/Welder	\$36.88	\$9.55
	Line Eq Operator/Line Truck Crew	\$25.74	\$8.09
Millwright		\$28.00	\$10.00
Pipefitter		\$30.45	\$12.85
Plumber		\$30.19	\$13.55
Power Equipment Operator (Tunnels Above and Below Ground, shafts and raises):	Group 1	\$25.12	\$10.81
	Group 2	\$25.47	\$10.85
	Group 3	\$25.57	\$10.86
	Group 4	\$25.82	\$10.88
	Group 5	\$25.97	\$10.90
	Group 6	\$26.12	\$10.91
	Group 7	\$26.37	\$10.94
Power Equipment Operator	Group 1	\$22.97	\$10.60
	Group 2	\$23.32	\$10.63
	Group 3	\$23.67	\$10.67
	Group 4	\$23.82	\$10.68
	Group 5	\$23.97	\$10.70
	Group 6	\$24.12	\$10.71
	Group 7	\$24.88	\$10.79
Truck Driver	Group 1	\$18.42	\$10.00
	Group 2	\$19.14	\$10.07
	Group 3	\$19.48	\$10.11
	Group 4	\$20.01	\$10.16
	Group 5	\$20.66	\$10.23
	Group 6	\$21.46	\$10.31
Truck Driver: Truck Mounted Attenuator		\$13.00	\$3.22

Go to <http://www.denvergov.org/Auditor> to view the Prevailing Wage Clarification Document for a list of complete classifications used.





**TO:** All Users of the City and County of Denver Prevailing Wage Schedules  
**FROM:** Ryland Feno, Classification & Compensation Technician II  
**DATE:** March 08, 2021  
**SUBJECT:** Latest Change to Prevailing Wage Schedules

The effective date for this publication will be **Friday, March 05, 2021** and applies to the City and County of Denver for **HEAVY CONSTRUCTION PROJECTS** in accordance with the Denver Revised Municipal Code, Section 20-76(c).

General Wage Decision No. CO20210002  
Superseded General Decision No. CO20200002  
Modification No. 1  
Publication Date: 03/05/2021  
(6 pages)

Unless otherwise specified in this document, apprentices shall be permitted only if they are employed pursuant to and individually registered in a bona fide apprenticeship program registered with the U.S. Department of Labor (DOL). The employer and the individual apprentice must be registered in a program which has received prior approval by the DOL. Any employer who employs an apprentice and is found to be in violation of this provision shall be required to pay said apprentice the full journeyman scale.

Attachments as listed above.

**\*Career Service Board approved to adjust all Davis Bacon classifications under \$13.00 to comply with the city's minimum wage. The effective date is August 15, 2019. See page 7 for reference.**

Office of Human Resources  
201 W. Colfax Ave. Dept. 412 | Denver, CO 80202  
p: 720.913.5751 | f: 720.913.5720  
[www.denvergov.org/humanresources](http://www.denvergov.org/humanresources)

"General Decision Number: CO20210002 03/05/2021

Superseded General Decision Number: CO20200002

State: Colorado

Construction Type: Heavy

Counties: Adams, Arapahoe, Boulder, Broomfield, Denver, Douglas, El Paso, Jefferson, Larimer, Mesa, Pueblo and Weld Counties in Colorado.

#### HEAVY CONSTRUCTION PROJECTS

Note: Under Executive Order (EO) 13658, an hourly minimum wage of \$10.95 for calendar year 2021 applies to all contracts subject to the Davis-Bacon Act for which the contract is awarded (and any solicitation was issued) on or after January 1, 2015. If this contract is covered by the EO, the contractor must pay all workers in any classification listed on this wage determination at least \$10.95 per hour (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in calendar year 2021. If this contract is covered by the EO and a classification considered necessary for performance of work on the contract does not appear on this wage determination, the contractor must pay workers in that classification at least the wage rate determined through the conformance process set forth in 29 CFR 5.5(a)(1)(ii) (or the EO minimum wage rate, if it is higher than the conformed wage rate). The EO minimum wage rate will be adjusted annually. Please note that this EO applies to the above-mentioned types of contracts entered into by the federal government that are subject to the Davis-Bacon Act itself, but it does not apply to contracts subject only to the Davis-Bacon Related Acts, including those set forth at 29 CFR 5.1(a)(2)-(60). Additional information on contractor requirements and worker protections under the EO is available at [www.dol.gov/whd/govcontracts](http://www.dol.gov/whd/govcontracts).

Modification Number	Publication Date
0	01/01/2021
1	03/05/2021

ASBE0028-001 07/01/2019

Rates

Fringes

Asbestos Workers/Insulator  
(Includes application of  
all insulating materials,

protective coverings,  
 coatings and finishings to  
 all types of mechanical  
 systems).....\$ 32.98 14.73

-----  
 BRCO0007-004 01/01/2019

ADAMS, ARAPAHOE, BOULDER, BROOMFIELD, DENVER, DOUGLAS,  
 JEFFERSON AND WELD COUNTIES

	Rates	Fringes
BRICKLAYER.....	\$ 29.52	10.48

-----  
 BRCO0007-006 05/01/2018

EL PASO AND PUEBLO COUNTIES

	Rates	Fringes
BRICKLAYER.....	\$ 25.88	10.34

-----  
 ELEC0012-004 06/01/2019

PUEBLO COUNTY

	Rates	Fringes
ELECTRICIAN		
Electrical contract over		
\$1,000,000.....	\$ 27.50	12.50+3%
Electrical contract under		
\$1,000,000.....	\$ 24.85	12.50+3%

-----  
 ELEC0068-001 06/01/2020

ADAMS, ARAPAHOE, BOULDER, BROOMFIELD, DENVER, DOUGLAS,  
 JEFFERSON, LARIMER, AND WELD COUNTIES

	Rates	Fringes
ELECTRICIAN.....	\$ 38.00	16.97

-----  
 ELEC0111-001 09/01/2020

	Rates	Fringes
Line Construction:		
Groundman.....	\$ 22.04	24.25%+6.80
Line Equipment Operator.....	\$ 35.61	24.25%+6.80

Lineman and Welder.....\$ 49.45      24.25%+6.80

-----  
ELEC0113-002 06/01/2020

EL PASO COUNTY

	Rates	Fringes
ELECTRICIAN.....	\$ 33.25	3%+15.75

-----  
ELEC0969-002 06/01/2019

MESA COUNTY

	Rates	Fringes
ELECTRICIAN. ....	\$ 25.20	10.06

-----  
ENGI0009-001 05/01/2020

	Rates	Fringes
Power equipment operators:		
Blade: Finish.....	\$ 30.37	11.15
Blade: Rough.....	\$ 30.37	11.15
Bulldozer.....	\$ 30.37	11.15
Cranes: 50 tons and under..	\$ 30.20	11.15
Cranes: 51 to 90 tons.....	\$ 30.47	11.15
Cranes: 91 to 140 tons....	\$ 31.55	11.15
Cranes: 141 tons and over...	\$ 33.67	11.15
Forklift.....	\$ 29.67	11.15
Mechanic.....	\$ 30.53	11.15
Oiler.....	\$ 29.29	11.15
Scraper: Single bowl under 40 cubic yards.....	\$ 30.20	11.15
Scraper: Single bowl, including pups 40 cubic yards and over and tandem bowls.....	\$ 30.37	11.15
Trackhoe.....	\$ 30.20	11.15

-----  
IRON0024-003 11/01/2020

	Rates	Fringes
IRONWORKER, STRUCTURAL.....	\$ 32.00	12.01
Structural		

-----  
LABO0086-001 05/01/2009

	Rates	Fringes
--	-------	---------

## Laborers:

Pipelayer.....	\$ 18.68	6.78
----------------	----------	------

-----  
PLUM0003-005 06/01/2020ADAMS, ARAPAHOE, BOULDER, BROOMFIELD, DENVER, DOUGLAS,  
JEFFERSON, LARIMER AND WELD COUNTIES

	Rates	Fringes
PLUMBER.....	\$ 43.63	16.67

-----  
PLUM0058-002 07/01/2018

EL PASO COUNTY

	Rates	Fringes
Plumbers and Pipefitters.....	\$ 32.75	14.85

-----  
PLUM0058-008 07/01/2018

PUEBLO COUNTY

	Rates	Fringes
Plumbers and Pipefitters.....	\$ 32.75	14.85

-----  
PLUM0145-002 07/01/2016

MESA COUNTY

	Rates	Fringes
Plumbers and Pipefitters.....	\$ 35.17	11.70

-----  
\* PLUM0208-004 01/01/2021ADAMS, ARAPAHOE, BOULDER, BROOMFIELD, DENVER, DOUGLAS,  
JEFFERSON, LARIMER AND WELD COUNTIES

	Rates	Fringes
PIPEFITTER.....	\$ 39.10	13.77

-----  
SHEE0009-002 07/01/2019

	Rates	Fringes
Sheet metal worker.....	\$ 34.62	17.95

-----  
 TEAM0455-002 07/01/2020

	Rates	Fringes
Truck drivers:		
Pickup.....	\$ 22.66	4.42
Tandem/Semi and Water.....	\$ 23.29	4.42

-----  
 SUCO2001-006 12/20/2001

	Rates	Fringes
BOILERMAKER.....	\$ 17.60	
Carpenters:		
Form Building and Setting...	\$ 16.97	2.74
All Other Work.....	\$ 15.14	3.37
Cement Mason/Concrete Finisher...	\$ 17.31	2.85
IRONWORKER, REINFORCING.....	\$ 18.83	3.90
Laborers:		
Common.....	\$ 11.22	2.92
Flagger.....	\$ 8.91	3.80
Landscape.....	\$ 12.56	3.21
Painters:		
Brush, Roller & Spray.....	\$ 15.81	3.26
Power equipment operators:		
Backhoe.....	\$ 16.36	2.48
Front End Loader.....	\$ 17.24	3.23
Skid Loader.....	\$ 15.37	4.41

-----  
 WELDERS - Receive rate prescribed for craft performing  
 operation to which welding is incidental.  
 =====

**Office of Human Resources  
Supplemental Rates  
(Specific to the Denver Projects)  
(Supp #74, Revised: 08-21-2019)**

<b>Classification</b>		<b>Base</b>	<b>Fringe</b>
Ironworker	Ornamental	\$24.80	\$10.03
Laborer	Group 1	\$18.18	\$8.27
	Group 2	\$21.59	\$8.61
Laborer (Common)		\$13.00	\$2.92
Laborer (Flagger)		\$13.00	\$3.80
Laborer (Landscape)		\$13.00	\$3.21
Laborer (Janitor)	Janitor/Yardmen	\$17.68	\$8.22
Laborer (Asbestos)	Removal of Asbestos	\$21.03	\$8.55
Laborer (Tunnel)	Group 1	\$18.53	\$8.30
	Group 2	\$18.63	\$8.31
	Group 3	\$19.73	\$8.42
	Group 4	\$21.59	\$8.61
	Group 5	\$19.68	\$8.42
Line Construction	Lineman, Gas Fitter/Welder	\$36.88	\$9.55
	Line Eq Operator/Line Truck Crew	\$25.74	\$8.09
Millwright		\$28.00	\$10.00
Power Equipment Operator	Group 1	\$22.97	\$10.60
	Group 2	\$23.32	\$10.63
	Group 3	\$23.67	\$10.67
	Group 4	\$23.82	\$10.68
	Group 5	\$23.97	\$10.70
	Group 6	\$24.12	\$10.71
	Group 7	\$24.88	\$10.79
Power Equipment Operator (Tunnels above and below ground, shafts and raises):	Group 1	\$25.12	\$10.81
	Group 2	\$25.47	\$10.85
	Group 3	\$25.57	\$10.86
	Group 4	\$25.82	\$10.88
	Group 5	\$25.97	\$10.90
	Group 6	\$26.12	\$10.91
	Group 7	\$26.37	\$10.94
Truck Driver	Group 1	\$18.42	\$10.00
	Group 2	\$19.14	\$10.07
	Group 3	\$19.48	\$10.11
	Group 4	\$20.01	\$10.16
	Group 5	\$20.66	\$10.23
	Group 6	\$21.46	\$10.31

Go to <http://www.denvergov.org/Auditor> to view the Prevailing Wage Clarification Document for a list of complete classifications used.

Exhibit E  
DSBO Forms





## DIVISION OF SMALL BUSINESS OPPORTUNITY (DSBO) COMMITMENT TO MWBE PARTICIPATION

*This page must be completed by all Bidders/Proposers to indicate their commitment towards satisfying the MWBE participation goal. The commitment will be incorporated into the contract and thereby the selected Bidder/Proposer's will be held to that commitment. (Please check the appropriate box):*

### COMPLETE IF YOU ARE A NON MWBE PRIME:

☒ The City and County of Denver has specified a 5 % MWBE Participation goal on this project. The Bidder/Proposer is committed to meeting 5 % MWBE Participation on the contract.

### COMPLETE IF YOU ARE A MWBE PRIME:

☐ The City and County of Denver has specified a \_\_\_\_\_ % MWBE Participation goal on this project. The Bidder/Proposer is a certified MWBE with the City and County of Denver and is committed to meeting \_\_\_\_\_ % MWBE Participation on the contract.

### COMPLETE IF YOU ARE UNABLE TO MEET PROJECT GOAL:

☐ The City and County of Denver has specified a \_\_\_\_\_ % MWBE Participation goal on this project. The Bidder/Proposer is unable to meet this project goal but is committed to a \_\_\_\_\_ % MWBE Participation on the contract. The Bidder/Proposer must make adequate good faith efforts to meet this goal in order to be deemed responsive. The Bidder/Proposer must submit a detailed statement and documentation of their good faith efforts. Award of the contract will be conditioned on meeting the requirements of this section, in accordance of Chapter 28 of the D.R.M.C. to the Division of Small Business Opportunity.

The undersigned Bidder/Proposer hereby agrees and understands that they must comply with their MWBE commitments in this project in conformity with the Requirements, Terms, and Conditions of this MWBE Procurement/Contract Language.

Bidder/Proposer (Name of Firm): SP Plus Corporation

Firm's Representative: DANE LYON

Title: Regional Manager

Signature (Firm's Representative): [Signature] Date: 11/30/21

Address: 1801 California St. Ste 2775

City: Denver State: CO Zip: 80204

Phone: 303-638-7112 Email: DLYON@spplus.com

Exhibit F  
(To Follow)



**Payment Card Industry (PCI)  
Data Security Standard  
Self-Assessment Questionnaire D  
and Attestation of Compliance for  
Service Providers**

---

**SAQ-Eligible Service Providers**

**For use with PCI DSS Version 3.2.1**

June 2018



## Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1</i> .
July 2015	3.1	1.1	Updated to remove references to “best practices” prior to June 30, 2015, and remove the PCI DSS v2 reporting option for Requirement 11.3.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2</i> .
January 2017	3.2	1.1	Updated version numbering to align with other SAQs
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1</i> .



## Table of Contents

<b>Document Changes .....</b>	<b>ii</b>
<b>Before You Begin.....</b>	<b>iv</b>
<b>PCI DSS Self-Assessment Completion Steps .....</b>	<b>iv</b>
<b>Understanding the Self-Assessment Questionnaire .....</b>	<b>iv</b>
<i>Expected Testing .....</i>	<i>v</i>
<b>Completing the Self-Assessment Questionnaire .....</b>	<b>v</b>
<b>Guidance for Non-Applicability of Certain, Specific Requirements.....</b>	<b>v</b>
<i>Understanding the difference between Not Applicable and Not Tested.....</i>	<i>vi</i>
<b>Legal Exception .....</b>	<b>vi</b>
<b>Section 1: Assessment Information .....</b>	<b>1</b>
<b>Section 2: Self-Assessment Questionnaire D for Service Providers .....</b>	<b>9</b>
<b>Build and Maintain a Secure Network and Systems .....</b>	<b>9</b>
<i>Requirement 1: Install and maintain a firewall configuration to protect data .....</i>	<i>9</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....</i>	<i>14</i>
<b>Protect Cardholder Data .....</b>	<b>20</b>
<i>Requirement 3: Protect stored cardholder data.....</i>	<i>20</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks.....</i>	<i>28</i>
<b>Maintain a Vulnerability Management Program .....</b>	<b>30</b>
<i>Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.....</i>	<i>30</i>
<i>Requirement 6: Develop and maintain secure systems and applications.....</i>	<i>32</i>
<b>Implement Strong Access Control Measures.....</b>	<b>41</b>
<i>Requirement 7: Restrict access to cardholder data by business need to know.....</i>	<i>41</i>
<i>Requirement 8: Identify and authenticate access to system components .....</i>	<i>43</i>
<i>Requirement 9: Restrict physical access to cardholder data .....</i>	<i>50</i>
<b>Regularly Monitor and Test Networks.....</b>	<b>58</b>
<i>Requirement 10: Track and monitor all access to network resources and cardholder data .....</i>	<i>58</i>
<i>Requirement 11: Regularly test security systems and processes.....</i>	<i>65</i>
<b>Maintain an Information Security Policy .....</b>	<b>73</b>
<i>Requirement 12: Maintain a policy that addresses information security for all personnel .....</i>	<i>73</i>
<b>Appendix A: Additional PCI DSS Requirements.....</b>	<b>82</b>
<i>Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.....</i>	<i>82</i>
<i>Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.....</i>	<i>84</i>
<i>Appendix A3: Designated Entities Supplemental Validation (DESV).....</i>	<i>85</i>
<b>Appendix B: Compensating Controls Worksheet.....</b>	<b>86</b>
<b>Appendix C: Explanation of Non-Applicability.....</b>	<b>87</b>
<b>Appendix D: Explanation of Requirements Not Tested .....</b>	<b>88</b>
<b>Section 3: Validation and Attestation Details .....</b>	<b>89</b>





## Before You Begin

SAQ D for Service Providers applies to all service providers defined by a payment brand as being SAQ-eligible.

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. See the guidance below for information about the exclusion of certain, specific requirements.

### PCI DSS Self-Assessment Completion Steps

1. Confirm that your environment is properly scoped.
2. Assess your environment for compliance with PCI DSS requirements.
3. Complete all sections of this document:
  - Section 1 (Parts 1 & 2 of the AOC) – Assessment Information and Executive Summary
  - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ D)
  - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
4. Submit the SAQ and Attestation of Compliance (AOC), along with any other requested documentation—such as ASV scan reports—to the payment brand, or other requester.

### Understanding the Self-Assessment Questionnaire

The questions contained in the “PCI DSS Question” column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS <i>(PCI Data Security Standard Requirements and Security Assessment Procedures)</i>	<ul style="list-style-type: none"> <li>• Guidance on Scoping</li> <li>• Guidance on the intent of all PCI DSS Requirements</li> <li>• Details of testing procedures</li> <li>• Guidance on Compensating Controls</li> </ul>
SAQ Instructions and Guidelines documents	<ul style="list-style-type: none"> <li>• Information about all SAQs and their eligibility criteria</li> <li>• How to determine which SAQ is right for your organization</li> </ul>
<i>PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms</i>	<ul style="list-style-type: none"> <li>• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires</li> </ul>

These and other resources can be found on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.



## Expected Testing

The instructions provided in the “Expected Testing” column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

## Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company’s status regarding that requirement. **Only one response should be selected for each question.**

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
<b>Yes</b>	The expected testing has been performed, and all elements of the requirement have been met as stated.
<b>Yes with CCW</b> (Compensating Control Worksheet)	<p>The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.</p> <p>All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ.</p> <p>Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.</p>
<b>No</b>	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
<b>N/A</b> (Not Applicable)	<p>The requirement does not apply to the organization’s environment. (See <i>Guidance for Non-Applicability of Certain, Specific Requirements</i> below for examples.)</p> <p>All responses in this column require a supporting explanation in Appendix C of the SAQ.</p>
<b>Not Tested</b>	<p>The requirement was not included for consideration in the assessment, and was not tested in any way. (See <i>Understanding the difference between Not Applicable and Not Tested</i> below for examples of when this option should be used.)</p> <p>All responses in this column require a supporting explanation in Appendix D of the SAQ.</p>

## Guidance for Non-Applicability of Certain, Specific Requirements

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. Similarly, an organization that does not store any cardholder data electronically at any time would not need to validate requirements related to secure storage of cardholder data (for example, Requirement 3.4).



Examples of requirements with specific applicability include:

- The questions specific to securing wireless technologies (for example, Requirements 1.2.3, 2.1.1, and 4.1.1) only need to be answered if wireless is present anywhere in your network. Note that Requirement 11.1 (use of processes to identify unauthorized wireless access points) must still be answered even if you don't use wireless technologies in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- The questions specific to application development and secure coding (Requirements 6.3 and 6.5) only need to be answered if your organization develops its own custom applications.
- The questions for Requirements 9.1.1 and 9.3 only need to be answered for facilities with "sensitive areas" as defined here: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data.

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

### ***Understanding the difference between Not Applicable and Not Tested***

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the wireless example above, for an organization to select "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, the organization would first need to confirm that there are no wireless technologies used in their cardholder data environment (CDE) or that connect to their CDE. Once this has been confirmed, the organization may select "N/A" for those specific requirements,

If a requirement is completely excluded from review without any consideration as to whether it *could* apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.
- An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that requires assessment of PCI DSS Requirements 2, 3 and 4.
- A service provider organization might offer a service which covers only a limited number of PCI DSS requirements—for example, a physical storage provider may only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment.

### **Legal Exception**

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.





## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

### Part 1. Service Provider and Qualified Security Assessor Information

#### Part 1a. Service Provider Organization Information

Company Name:	SP Plus Corporation	DBA (doing business as):	SP+ parking management services for the City of Denver Garages and Lots Location # 05129 / 99352		
Contact Name:	Bob Kohler	Title:	VP, Regional Manager III		
Telephone:	303-292-0212	E-mail:	BKohler@spplus.com		
Business Address:	1055 13 <sup>th</sup> St	City:	Denver		
State/Province:	CO	Country:	USA	Zip:	80204-2156
URL:	spplus.com				

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		Zip:	
URL:					



## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) assessed:		Parking Management Services
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input checked="" type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.



## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) not assessed:

Type of service(s) not assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

#### Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

### Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

SP+ is not involved with managing the storing, processing or transmitting credit card data; this process is managed by the vendor in their service agreement with the City who holds the Merchant ID.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

SP+ staff provides physical security to credit card processing equipment, operates access controls to the facility and assists customers with regular use of the card reading equipment if needed, and would alert the vendor and City if staff detected a physical security incident involving credit cards were occur at one of the facilities.

### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Parking Lot	1	Denver, CO, USA




## Part 2. Executive Summary *(continued)*

### Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

### Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

SkiData (est. October 2023 transition), Amano McGann (current), Verifone handhelds and mobile POS card-reading equipment, with computer servers supporting the pay stations in parking facilities.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation.)*

☒ Yes ☐ No

### Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?

☐ Yes ☒ No



<b>If Yes:</b>	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	



## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers *(continued)*

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

☐ Yes ☒ No

#### **If Yes:**

Name of service provider:	Description of services provided:

**Note:** Requirement 12.8 applies to all entities in this list.



## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the SAQ.
- **Partial** – One or more sub-requirements of that Requirement were marked as “Not Tested” or “Not Applicable” in the SAQ.
- **None** – All sub-requirements of that Requirement were marked as “Not Tested” and/or “Not Applicable” in the SAQ.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the SAQ
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

<b>Name of Service Assessed:</b>		6/24/2022		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for the firewalls at these locations.</b>
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for the systems configuration at these locations.</b>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for credit card data storage or transmission at these locations.</b>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>SP+ is not responsible for encryption configuration at these locations, and will not transmit credit card data in plaintext on our messaging systems.</b>
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for antivirus at these locations.</b>
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for patching or vulnerabilities at these locations.</b>
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for user system access at these locations.</b>
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for user system access at these locations.</b>



Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Physical media and video cameras not used re: credit cards at these locations.</b>
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for logs or audit trails at these locations.</b>
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not responsible for IT Security controls at these locations.</b>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SP+ is not a shared hosting provider.</b>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SSL / Early TLS is not used at these locations.</b>





## Section 2: Self-Assessment Questionnaire D for Service Providers

**Note:** The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Self-assessment completion date: 6/24/2022

### Build and Maintain a Secure Network and Systems

#### Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1	Are firewall and router configuration standards established and implemented to include the following:						
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	<ul style="list-style-type: none"> <li>Review documented process.</li> <li>Interview personnel.</li> <li>Examine network configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	<ul style="list-style-type: none"> <li>Review current network diagram.</li> <li>Examine network configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a process to ensure the diagram is kept current?	<ul style="list-style-type: none"> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	<ul style="list-style-type: none"> <li>Review current dataflow diagram.</li> <li>Examine network configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a process to ensure the diagram is kept current?	<ul style="list-style-type: none"> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	<ul style="list-style-type: none"> <li>Review firewall configuration standards.</li> <li>Observe network configurations to verify that a firewall(s) is in place.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is the current network diagram consistent with the firewall configuration standards?	<ul style="list-style-type: none"> <li>Compare firewall configuration standards to current network diagram.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.1.5	Are groups, roles, and responsibilities for logical management of network components assigned and documented in the firewall and router configuration standards?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.1.6	(a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.1.7	(a) Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are firewall and router rule sets reviewed at least every six months?	<ul style="list-style-type: none"> <li>Examine documentation from firewall reviews.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:  <b>Note:</b> An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.						



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.2.1	(a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.2.2	Are router configuration files secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Examine router configuration files and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	<ul style="list-style-type: none"> <li>Review firewall and router configuration standards.</li> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:						
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	<ul style="list-style-type: none"> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	<ul style="list-style-type: none"> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3.3	Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network? (For example, block traffic originating from the internet with an internal address.)	<ul style="list-style-type: none"> <li>Examine firewall and router configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	▪ Examine firewall and router configurations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3.5	Are only established connections permitted into the network?	▪ Examine firewall and router configurations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3.6	Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?	▪ Examine firewall and router configurations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3.7	(a) Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet?  <b>Note:</b> Methods to obscure IP addressing may include, but are not limited to: <ul style="list-style-type: none"> <li>• Network Address Translation (NAT)</li> <li>• Placing servers containing cardholder data behind proxy servers/firewalls,</li> <li>• Removal or filtering of route advertisements for private networks that employ registered addressing,</li> <li>• Internal use of RFC1918 address space instead of registered addresses.</li> </ul>	▪ Examine firewall and router configurations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is any disclosure of private IP addresses and routing information to external entities authorized?	▪ Examine firewall and router configurations. ▪ Interview personnel.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.4	(a) Is personal firewall software (or equivalent functionality) installed and active on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE?	<ul style="list-style-type: none"> <li>Review policies and configuration standards.</li> <li>Examine mobile and/or employee-owned devices.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is the personal firewall software (or equivalent functionality) configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?	<ul style="list-style-type: none"> <li>Review policies and configuration standards.</li> <li>Examine mobile and/or employee-owned devices.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.5	Are security policies and operational procedures for managing firewalls: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network?  <i>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).</i>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine vendor documentation.</li> <li>Observe system configurations and account settings.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review vendor documentation.</li> <li>Examine system configurations and account settings.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:						
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review vendor documentation.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are default SNMP community strings on wireless devices changed at installation?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review vendor documentation.</li> <li>Interview personnel.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are default passwords/passphrases on access points changed at installation?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.1.1 (cont.)	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review vendor documentation.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(e) Are other security-related wireless vendor defaults changed, if applicable?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review vendor documentation.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2	(a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?  <i>Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> <li>Review system configuration standards.</li> <li>Review industry-accepted hardening standards.</li> <li>Review policies and procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are system configuration standards applied when new systems are configured?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.2 (cont.)	(d) Do system configuration standards include all of the following: <ul style="list-style-type: none"> <li>– Changing of all vendor-supplied defaults and elimination of unnecessary default accounts?</li> <li>– Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?</li> <li>– Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?</li> <li>– Implementing additional security features for any required services, protocols or daemons that are considered to be insecure?</li> <li>– Configuring system security parameters to prevent misuse?</li> <li>– Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review system configuration standards.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.1	(a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?  <i>For example, web servers, database servers, and DNS should be implemented on separate servers.</i>	<ul style="list-style-type: none"> <li>▪ Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	<ul style="list-style-type: none"> <li>▪ Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	<ul style="list-style-type: none"> <li>Review configuration standards.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	<ul style="list-style-type: none"> <li>Review configuration standards</li> <li>Interview personnel.</li> <li>Examine configuration settings.</li> <li>Compare enabled services, etc. to documented justifications.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.3	Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?	<ul style="list-style-type: none"> <li>Review configuration standards.</li> <li>Examine configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.4	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	<ul style="list-style-type: none"> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are common system security parameters settings included in the system configuration standards?	<ul style="list-style-type: none"> <li>Review system configuration standards.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are security parameter settings set appropriately on system components?	<ul style="list-style-type: none"> <li>Examine system components.</li> <li>Examine security parameter settings.</li> <li>Compare settings to system configuration standards.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.5	(a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	<ul style="list-style-type: none"> <li>Examine security parameters on system components.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are enabled functions documented and do they support secure configuration?	<ul style="list-style-type: none"> <li>Review documentation.</li> <li>Examine security parameters on system components.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.2.5 (cont.)	(c) Is only documented functionality present on system components?	<ul style="list-style-type: none"> <li>Review documentation.</li> <li>Examine security parameters on system components.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.3	Is non-console administrative access encrypted as follows:						
	(a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	<ul style="list-style-type: none"> <li>Examine system components.</li> <li>Examine system configurations.</li> <li>Observe an administrator log on.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	<ul style="list-style-type: none"> <li>Examine system components.</li> <li>Examine services and files.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	<ul style="list-style-type: none"> <li>Examine system components.</li> <li>Observe an administrator log on.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	<ul style="list-style-type: none"> <li>Examine system components.</li> <li>Review vendor documentation.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.4	(a) Is an inventory maintained for systems components that are in scope for PCI DSS, including a list of hardware and software components and a description of function/use for each?	<ul style="list-style-type: none"> <li>Examine system inventory.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is the documented inventory kept current?	<ul style="list-style-type: none"> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.5	Are security policies and operational procedures for managing vendor defaults and other security parameters: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.6	<p>If you are a shared hosting provider, are your systems configured to protect each entity's (your customers') hosted environment and cardholder data?</p> <p><i>See Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers for specific requirements that must be met.</i></p>	<ul style="list-style-type: none"> <li>Complete Appendix A1 testing procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



## Protect Cardholder Data

### Requirement 3: Protect stored cardholder data

PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
3.1	Are data-retention and disposal policies, procedures, and processes implemented as follows:					
(a)	Is data storage amount and retention time limited to that required for legal, regulatory, and/or business requirements?  ▪ Review data retention and disposal policies and procedures. ▪ Interview personnel.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(b)	Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, and/or business reasons?  ▪ Review policies and procedures. ▪ Interview personnel. ▪ Examine deletion mechanism.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(c)	Are there specific retention requirements for cardholder data? <i>For example, cardholder data needs to be held for X period for Y business reasons.</i>  ▪ Review policies and procedures. ▪ Interview personnel. ▪ Examine retention requirements.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(d)	Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?  ▪ Review policies and procedures. ▪ Interview personnel. ▪ Observe deletion processes.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(e)	Does all stored cardholder data meet the requirements defined in the data-retention policy?  ▪ Examine files and system records.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.2	(a) For issuers and/or companies that support issuing services and store sensitive authentication data, is there a documented business justification for the storage of sensitive authentication data?  ▪ Review policies and procedures. ▪ Interview personnel. ▪ Review documented business justification.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.2 (cont.)	(b) For issuers and/or companies that support issuing services and store sensitive authentication data: Is the data secured?	<ul style="list-style-type: none"> <li>Examine data stores and system configuration files.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) For all other entities: Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine system configurations.</li> <li>Examine deletion processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):						
3.2.1	<p>The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization?</p> <p><i>This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</i></p> <p><b>Note:</b> In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</p> <ul style="list-style-type: none"> <li>The cardholder's name,</li> <li>Primary account number (PAN),</li> <li>Expiration date, and</li> <li>Service code</li> </ul> <p>To minimize risk, store only these data elements as needed for business.</p>	<ul style="list-style-type: none"> <li>Examine data sources including:               <ul style="list-style-type: none"> <li>Incoming transaction data</li> <li>All logs</li> <li>History files</li> <li>Trace files</li> <li>Database schema</li> <li>Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	<ul style="list-style-type: none"> <li>Examine data sources including:               <ul style="list-style-type: none"> <li>– Incoming transaction data</li> <li>– All logs</li> <li>– History files</li> <li>– Trace files</li> <li>– Database schema</li> <li>– Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	<ul style="list-style-type: none"> <li>Examine data sources including:               <ul style="list-style-type: none"> <li>– Incoming transaction data</li> <li>– All logs</li> <li>– History files</li> <li>– Trace files</li> <li>– Database schema</li> <li>– Database contents</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.3	<p>Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN?</p> <p><b>Note:</b> This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.</p>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review roles that need access to displays of full PAN.</li> <li>Examine system configurations.</li> <li>Observe displays of PAN.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
3.4 Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches? <ul style="list-style-type: none"> <li>One-way hashes based on strong cryptography (hash must be of the entire PAN)</li> <li>Truncation (hashing cannot be used to replace the truncated segment of PAN)</li> <li>Index tokens and pads (pads must be securely stored)</li> <li>Strong cryptography with associated key management processes and procedures.</li> </ul> <p><b>Note:</b> It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.</p>	<ul style="list-style-type: none"> <li>Examine vendor documentation.</li> <li>Examine data repositories.</li> <li>Examine removable media.</li> <li>Examine audit logs, including payment application logs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.4.1 If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows: <p><b>Note:</b> This requirement applies in addition to all other PCI DSS encryption and key management requirements.</p>						
(a) Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?	<ul style="list-style-type: none"> <li>Examine system configurations.</li> <li>Observe the authentication process.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(b) Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.4.1 (cont.)	(c) Is cardholder data on removable media encrypted wherever stored?  <i><b>Note:</b> If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.</i>	<ul style="list-style-type: none"> <li>Examine system configurations.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.5	Are keys used to secure stored cardholder data protected against disclosure and misuse as follows:  <i><b>Note:</b> This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.</i>						
3.5.1	<i>For service providers only:</i> Is a documented description of the cryptographic architecture maintained that includes: <ul style="list-style-type: none"> <li>Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date,</li> <li>Description of the key usage for each key,</li> <li>Inventory of any HSMs and other SCDs used for key management?</li> </ul>	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Review documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.5.2	Is access to cryptographic keys restricted to the fewest number of custodians necessary?	<ul style="list-style-type: none"> <li>Examine user access lists.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.5.3	<p>Are secret and private cryptographic keys used to encrypt/decrypt cardholder data stored in one (or more) of the following forms at all times?</p> <ul style="list-style-type: none"> <li>Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key</li> <li>Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)</li> <li>As at least two full-length key components or key shares, in accordance with an industry-accepted method.</li> </ul> <p><b>Note:</b> It is not required that public keys be stored in one of these forms.</p>	<ul style="list-style-type: none"> <li>Review documented procedures.</li> <li>Examine system configurations and key storage locations, including for key-encrypting keys.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.5.4	Are cryptographic keys stored in the fewest possible locations?	<ul style="list-style-type: none"> <li>Examine key-storage locations.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6	(a) Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) <i>For service providers only:</i> If keys are shared with customers for transmission or storage of cardholder data, is documentation provided to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with requirements 3.6.1 through 3.6.8 below?	<ul style="list-style-type: none"> <li>Review documentation provided to customers.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are key-management processes and procedures implemented to require the following:						
3.6.1	Do cryptographic key procedures include the generation of strong cryptographic keys?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Observe key-generation procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.6.2	Do cryptographic key procedures include secure cryptographic key distribution?	<ul style="list-style-type: none"> <li>Review key management procedures.</li> <li>Observe the key-distribution method.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6.3	Do cryptographic key procedures include secure cryptographic key storage?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Observe the method for secure storage of keys.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6.4	Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57)?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6.5	(a) Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Do cryptographic key procedures include replacement of known or suspected compromised keys?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes, and not used for encryption operations?	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
3.6.6 If manual clear-text key-management operations are used, do cryptographic key procedures include split knowledge and dual control of cryptographic keys as follows: <ul style="list-style-type: none"> <li>Do split knowledge procedures require that key components are under the control of at least two people who only have knowledge of their own key components?</li> </ul> AND <ul style="list-style-type: none"> <li>Do dual control procedures require that at least two people are required to perform any key management operations and no one person has access to the authentication materials (for example, passwords or keys) of another?</li> </ul> <p><b>Note:</b> Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.</p>	<ul style="list-style-type: none"> <li>Review key-management procedures.</li> <li>Interview personnel and/or.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6.7 Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys?	<ul style="list-style-type: none"> <li>Review procedures.</li> <li>Interview personnel and/or</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.6.8 Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities?	<ul style="list-style-type: none"> <li>Review procedures.</li> <li>Review documentation or other evidence.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.7 Are security policies and operational procedures for protecting stored cardholder data: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



#### Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
4.1	(a) Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?  <i>Note: Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).</i>	<ul style="list-style-type: none"> <li>Review documented standards.</li> <li>Review policies and procedures.</li> <li>Review all locations where CHD is transmitted or received.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are only trusted keys and/or certificates accepted?	<ul style="list-style-type: none"> <li>Observe inbound and outbound transmissions.</li> <li>Examine keys and certificates.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	<ul style="list-style-type: none"> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	<ul style="list-style-type: none"> <li>Review vendor documentation.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(e) For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?  <i>For example, for browser-based implementations:</i> <ul style="list-style-type: none"> <li>"HTTPS" appears as the browser Universal Record Locator (URL) protocol, and</li> <li>Cardholder data is only requested if "HTTPS" appears as part of the URL.</li> </ul>	<ul style="list-style-type: none"> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	<ul style="list-style-type: none"> <li>Review documented standards.</li> <li>Review wireless networks.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.2	(a) Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Review outbound transmissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Are security policies and operational procedures for encrypting transmissions of cardholder data: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Maintain a Vulnerability Management Program

### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	<ul style="list-style-type: none"> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	<ul style="list-style-type: none"> <li>Review vendor documentation.</li> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	<ul style="list-style-type: none"> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	Are all anti-virus mechanisms maintained as follows:						
	(a) Are all anti-virus software and definitions kept current?	<ul style="list-style-type: none"> <li>Examine policies and procedures.</li> <li>Examine anti-virus configurations, including the master installation.</li> <li>Examine system components.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are automatic updates and periodic scans enabled and being performed?	<ul style="list-style-type: none"> <li>Examine anti-virus configurations, including the master installation.</li> <li>Examine system components.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	<ul style="list-style-type: none"> <li>Examine anti-virus configurations.</li> <li>Review log retention processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
5.3	<p>Are all anti-virus mechanisms:</p> <ul style="list-style-type: none"> <li>Actively running?</li> <li>Unable to be disabled or altered by users?</li> </ul> <p><b>Note:</b> Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.</p>	<ul style="list-style-type: none"> <li>Examine anti-virus configurations.</li> <li>Examine system components.</li> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<p>Are security policies and operational procedures for protecting systems against malware:</p> <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



### Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.1	<p>Is there a process to identify security vulnerabilities, including the following:</p> <ul style="list-style-type: none"> <li>Using reputable outside sources for vulnerability information?</li> <li>Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities?</li> </ul> <p><b>Note:</b> Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.</p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.</p>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.2 (cont.)	(b) Are critical security patches installed within one month of release?  <b>Note:</b> Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine system components.</li> <li>Compare list of security patches installed to recent vendor patch lists.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.3	(a) Are software- development processes based on industry standards and/or best practices?	<ul style="list-style-type: none"> <li>Review software development processes.</li> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is information security included throughout the software-development life cycle?	<ul style="list-style-type: none"> <li>Review software development processes.</li> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)?	<ul style="list-style-type: none"> <li>Review software development processes.</li> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) Do software development processes ensure the following at 6.3.1 - 6.3.2:						
6.3.1	Are development, test, and/or custom application accounts, user IDs, and passwords removed before applications become active or are released to customers?	<ul style="list-style-type: none"> <li>Review software development processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
6.3.2 Is all custom code reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes as follows): <ul style="list-style-type: none"> <li>Are code changes reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices?</li> <li>Do code reviews ensure code is developed according to secure coding guidelines?</li> <li>Are appropriate corrections implemented prior to release?</li> <li>Are code review results reviewed and approved by management prior to release?</li> </ul> <p><b>Note:</b> This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</p>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Examine recent changes and change records.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4	Are change control processes and procedures followed for all changes to system components to include the following:					
6.4.1	(a) Are development/test environments separate from the production environment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is access control in place to enforce the separation between the development/test environments and the production environment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<ul style="list-style-type: none"> <li>Review change control processes and procedures.</li> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.3	Are production data (live PANs) <b>not</b> used for testing or development?	<ul style="list-style-type: none"> <li>Review change control processes and procedures.</li> <li>Observe processes.</li> <li>Interview personnel.</li> <li>Examine test data.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.4	Are test data and accounts removed from system components before the system becomes active / goes into production?	<ul style="list-style-type: none"> <li>Review change control processes and procedures.</li> <li>Observe processes.</li> <li>Interview personnel.</li> <li>Examine production systems.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.5	(a) Are change-control procedures documented and require the following? <ul style="list-style-type: none"> <li>Documentation of impact</li> <li>Documented change control approval by authorized parties</li> <li>Functionality testing to verify that the change does not adversely impact the security of the system</li> <li>Back-out procedures</li> </ul>	<ul style="list-style-type: none"> <li>Review change control processes and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are the following performed and documented for all changes:						
6.4.5.1	Documentation of impact?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.5.2	Documented approval by authorized parties?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.5.3	(a) Functionality testing to verify that the change does not adversely impact the security of the system?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.5.4	Back-out procedures?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.4.6	Upon completion of a significant change, are all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable?	<ul style="list-style-type: none"> <li>Trace changes to change control documentation.</li> <li>Examine change control documentation.</li> <li>Interview personnel.</li> <li>Observe affected systems or networks.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.5	(a) Do software-development processes address common coding vulnerabilities?	<ul style="list-style-type: none"> <li>Review software-development policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are developers trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Examine training records.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:  <b>Note:</b> The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.						
6.5.1	Do coding techniques address injection flaws, particularly SQL injection?  <b>Note:</b> Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.2	Do coding techniques address buffer overflow vulnerabilities?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.3	Do coding techniques address insecure cryptographic storage?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.4	Do coding techniques address insecure communications?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.5.5	Do coding techniques address improper error handling?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.6	Do coding techniques address all "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
For web applications and application interfaces (internal or external), are applications developed based on secure coding guidelines to protect applications from the following additional vulnerabilities:							
6.5.7	Do coding techniques address cross-site scripting (XSS) vulnerabilities?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.8	Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.9	Do coding techniques address cross-site request forgery (CSRF)?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6.5.10	Do coding techniques address broken authentication and session management?	<ul style="list-style-type: none"> <li>Examine software-development policies and procedures.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
<p>6.6 For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying <i>either</i> of the following methods?</p> <ul style="list-style-type: none"> <li>Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: <ul style="list-style-type: none"> <li>At least annually</li> <li>After any changes</li> <li>By an organization that specializes in application security</li> <li>That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment</li> <li>That all vulnerabilities are corrected</li> <li>That the application is re-evaluated after the corrections</li> </ul> </li> </ul> <p><b>Note:</b> This assessment is not the same as the vulnerability scans performed for Requirement 11.2.</p> <p>– OR –</p> <ul style="list-style-type: none"> <li>Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows: <ul style="list-style-type: none"> <li>Is situated in front of public-facing web applications to detect and prevent web-based attacks.</li> <li>Is actively running and up to date as applicable.</li> <li>Is generating audit logs.</li> <li>Is configured to either block web-based attacks, or generate an alert that is immediately investigated.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Review documented processes.</li> <li>Interview personnel.</li> <li>Examine records of application security assessments.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.7	Are security policies and operational procedures for developing and maintaining secure systems and applications: <ul style="list-style-type: none"> <li>▪ Documented</li> <li>▪ In use</li> <li>▪ Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review security policies and operational procedures.</li> <li>▪ Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





## Implement Strong Access Control Measures

### Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:						
	<ul style="list-style-type: none"> <li>Is there a written policy for access control that incorporates the following? <ul style="list-style-type: none"> <li>Defining access needs and privilege assignments for each role</li> <li>Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities,</li> <li>Assignment of access based on individual personnel's job classification and function</li> <li>Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Examine written access control policy.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.1.1	Are access needs for each role defined, including: <ul style="list-style-type: none"> <li>System components and data resources that each role needs to access for their job function?</li> <li>Level of privilege required (for example, user, administrator, etc.) for accessing resources?</li> </ul>	<ul style="list-style-type: none"> <li>Examine roles and access need.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.1.2	Is access to privileged user IDs restricted as follows: <ul style="list-style-type: none"> <li>To least privileges necessary to perform job responsibilities?</li> <li>Assigned only to roles that specifically require that privileged access?</li> </ul>	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Interview management.</li> <li>Review privileged user IDs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.1.3	Is access assigned based on individual personnel's job classification and function?	<ul style="list-style-type: none"> <li>Interview management.</li> <li>Review user IDs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
7.1.4	Is documented approval by authorized parties required, specifying required privileges?	<ul style="list-style-type: none"> <li>Review user IDs.</li> <li>Compare with documented approvals.</li> <li>Compare assigned privileges with documented approvals.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.2	Is an access control system(s) in place for system components to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:						
7.2.1	Is the access control system(s) in place on all system components?	<ul style="list-style-type: none"> <li>Review vendor documentation.</li> <li>Examine configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.2.2	Is the access control system(s) configured to enforce privileges assigned to individuals based on job classification and function?	<ul style="list-style-type: none"> <li>Review vendor documentation.</li> <li>Examine configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.2.3	Does the access control system(s) have a default "deny-all" setting?	<ul style="list-style-type: none"> <li>Review vendor documentation.</li> <li>Examine configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7.3	Are security policies and operational procedures for restricting access to cardholder data: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Examine security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


**Requirement 8: Identify and authenticate access to system components**

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.1	Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:						
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.2	Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled such that user IDs are implemented only as authorized (including with specified privileges)?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine privileged and general user IDs and associated authorizations.</li> <li>Observe system settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.3	Is access for any terminated users immediately deactivated or removed?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine terminated users accounts.</li> <li>Review current access lists.</li> <li>Observe returned physical authentication devices.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.4	Are inactive user accounts either removed or disabled within 90 days?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Observe user accounts.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.5	(a) Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Interview personnel.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are third-party remote access accounts monitored when in use?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.1.6	(a) Are repeated access attempts limited by locking out the user ID after no more than six attempts?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) <i>For service providers only:</i> Are non-consumer customer passwords temporarily locked-out after not more than six invalid access attempts?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review documentation.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.7	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.1.8	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? <ul style="list-style-type: none"> <li>Something you know, such as a password or passphrase</li> <li>Something you have, such as a token device or smart card</li> <li>Something you are, such as a biometric</li> </ul>	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Observe authentication processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2.1	(a) Is strong cryptography used to render all authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Review vendor documentation.</li> <li>Examine system configuration settings.</li> <li>Observe password files.</li> <li>Observe data transmissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.2.1 (cont.)	(b) <i>For service providers only:</i> Is strong cryptography used to render all non-consumer customers' authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components?	<ul style="list-style-type: none"> <li>Observe password files.</li> <li>Observe data transmissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2.2	Is user identity verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)?	<ul style="list-style-type: none"> <li>Review authentication procedures.</li> <li>Observe personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2.3	(a) Are user password parameters configured to require passwords/passphrases meet the following? <ul style="list-style-type: none"> <li>A minimum password length of at least seven characters</li> <li>Contain both numeric and alphabetic characters</li> </ul> Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	<ul style="list-style-type: none"> <li>Examine system configuration settings to verify password parameters.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) <i>For service providers only:</i> Are non-consumer customer passwords required to meet the following minimum length and complexity requirements? <ul style="list-style-type: none"> <li>A minimum password length of at least seven characters</li> <li>Contain both numeric and alphabetic characters</li> </ul>	<ul style="list-style-type: none"> <li>Review customer/user documentation.</li> <li>Observe internal processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2.4	(a) Are user passwords/passphrases changed at least once every 90 days?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) <i>For service providers only:</i> Are non-consumer customer passwords required to be changed periodically, and are non-consumer customers given guidance as to when, and under what circumstances, passwords must change.	<ul style="list-style-type: none"> <li>Review customer/user documentation.</li> <li>Observe internal processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.2.5	(a) Must an individual submit a new password/passphrase that is different from any of the last four passwords/passphrases he or she has used?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Sample system components.</li> <li>Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) <i>For service providers only:</i> Are new, non-consumer customer passwords required to be different from any of the last four passwords used?	<ul style="list-style-type: none"> <li>Review customer/user documentation.</li> <li>Observe internal processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.2.6	Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?	<ul style="list-style-type: none"> <li>Review password procedures.</li> <li>Examine system configuration settings.</li> <li>Observe security personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.3	<p>Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication, as follows:</p> <p><b>Note:</b> Multi-factor authentication requires that a minimum of two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.</p>						
8.3.1	Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access?	<ul style="list-style-type: none"> <li>Examine system configurations.</li> <li>Observe administrator logging into CDE.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.3.2	Is multi-factor authentication incorporated for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network?	<ul style="list-style-type: none"> <li>Examine system configurations.</li> <li>Observe personnel connecting remotely.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.4	(a) Are authentication policies and procedures documented and communicated to all users?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review distribution method.</li> <li>Interview personnel.</li> <li>Interview users.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Do authentication policies and procedures include the following? <ul style="list-style-type: none"> <li>Guidance on selecting strong authentication credentials</li> <li>Guidance for how users should protect their authentication credentials</li> <li>Instructions not to reuse previously used passwords</li> <li>Instructions that users should change passwords if there is any suspicion the password could be compromised</li> </ul>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Review documentation provided to users.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: <ul style="list-style-type: none"> <li>Generic user IDs and accounts are disabled or removed;</li> <li>Shared user IDs for system administration activities and other critical functions do not exist; and</li> <li>Shared and generic user IDs are not used to administer any system components?</li> </ul>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine user ID lists.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.5.1	<p><i>For service providers only.</i> Do service providers with remote access to customer premises (for example, for support of POS systems or servers) use a unique authentication credential (such as a password/passphrase) for each customer?</p> <p><b>Note:</b> This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.</p>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.6	<p>Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), is the use of these mechanisms assigned as follows?</p> <ul style="list-style-type: none"> <li>Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts</li> <li>Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access</li> </ul>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Examine system configuration settings and/or physical controls.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
8.7	Is all access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:					
(a)	Is all user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(b)	Is user direct access to or queries to of databases restricted to database administrators?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(c)	Are application IDs only able to be used by the applications (and not by individual users or other processes)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8.8	Are security policies and operational procedures for identification and authentication: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


**Requirement 9: Restrict physical access to cardholder data**

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	<ul style="list-style-type: none"> <li>Observe physical access controls.</li> <li>Observe personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.1	(a) Are either video cameras or access control mechanisms (or both) in place to monitor individual physical access to sensitive areas?  <i>Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Observe physical monitoring mechanisms.</li> <li>Observe security features.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are either video cameras or access control mechanisms (or both) protected from tampering or disabling?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview security personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?	<ul style="list-style-type: none"> <li>Review data retention processes.</li> <li>Observe data storage.</li> <li>Interview security personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.1.2	Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?  <i>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Observe locations.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.1.3	Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Observe devices.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.2	(a) Are procedures developed to easily distinguish between onsite personnel and visitors, which include: <ul style="list-style-type: none"> <li>Identifying onsite personnel and visitors (for example, assigning badges),</li> <li>Changing access requirements, and</li> <li>Revoking terminated onsite personnel and expired visitor identification (such as ID badges)</li> </ul> <i>For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> <li>Observe identification methods (e.g. badges).</li> <li>Observe visitor processes.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors?	<ul style="list-style-type: none"> <li>Observe identification methods.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is access to the badge system limited to authorized personnel?	<ul style="list-style-type: none"> <li>Observe physical controls and access controls for the badge system.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3	Is physical access to sensitive areas controlled for onsite personnel, as follows: <ul style="list-style-type: none"> <li>Is access authorized and based on individual job function?</li> <li>Is access revoked immediately upon termination</li> <li>Upon termination, are all physical access mechanisms, such as keys, access cards, etc., returned or disabled?</li> </ul>	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Examine access control lists.</li> <li>Observe onsite personnel.</li> <li>Compare lists of terminated employees to access control lists.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.4	Is visitor identification and access handled as follows:						
9.4.1	Are visitors authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Observe visitor processes including how access is controlled.</li> <li>Interview personnel.</li> <li>Observe visitors and badge use.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.2	(a) Are visitors identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel?	<ul style="list-style-type: none"> <li>Observe badge use of personnel and visitors.</li> <li>Examine identification.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do visitor badges or other identification expire?	<ul style="list-style-type: none"> <li>Observe process.</li> <li>Examine identification.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.3	Are visitors asked to surrender the badge or other identification before leaving the facility or at the date of expiration?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Observe visitors leaving facility.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.4	(a) Is a visitor log in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine the visitor log.</li> <li>Observe visitor processes.</li> <li>Examine log retention.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine the visitor log.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is the visitor log retained for at least three months?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Examine visitor log retention.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?  <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures for physically securing media.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.5.1	Is the location where media back-ups are stored reviewed at least annually to confirm storage is secure?	<ul style="list-style-type: none"> <li>Review policies and procedures for reviewing offsite media locations.</li> <li>Interview security personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	<ul style="list-style-type: none"> <li>Review policies and procedures for distribution of media.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Do controls include the following:						
9.6.1	Is media classified so the sensitivity of the data can be determined?	<ul style="list-style-type: none"> <li>Review policies and procedures for media classification.</li> <li>Interview security personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Examine media distribution tracking logs and documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Examine media distribution tracking logs and documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.7	Is strict control maintained over the storage and accessibility of media?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.7.1	(a) Are inventory logs of all media properly maintained?	<ul style="list-style-type: none"> <li>Examine inventory logs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are periodic media inventories conducted at least annually?	<ul style="list-style-type: none"> <li>Examine inventory logs.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	<ul style="list-style-type: none"> <li>Review periodic media destruction policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a periodic media destruction policy that defines requirements for the following? <ul style="list-style-type: none"> <li>Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.</li> <li>Storage containers used for materials that are to be destroyed must be secured.</li> <li>Cardholder data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).</li> </ul>	<ul style="list-style-type: none"> <li>Review periodic media destruction policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Is media destruction performed as follows:						
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Examine procedures.</li> <li>Observe processes.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	<ul style="list-style-type: none"> <li>Examine security of storage containers.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9.8.2	Is cardholder data on electronic media rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media), so that cardholder data cannot be reconstructed?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.9	<p>Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?</p> <p><b>Note:</b> This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.</p>						
	(a) Do policies and procedures require that a list of such devices be maintained?	▪ Review policies and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	▪ Review policies and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	▪ Review policies and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1	(a) Does the list of devices include the following? <ul style="list-style-type: none"> <li>– Make, model of device</li> <li>– Location of device (for example, the address of the site or facility where the device is located)</li> <li>– Device serial number or other method of unique identification</li> </ul>	▪ Examine the list of devices.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is the list accurate and up to date?	▪ Observe devices and device locations and compare to list.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	▪ Interview personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.9.2	<p>(a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?</p> <p><b>Note:</b> Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.</p>	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe inspection processes and compare to defined processes.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are personnel aware of procedures for inspecting devices?	<ul style="list-style-type: none"> <li>Interview personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?						
	<p>(a) Do training materials for personnel at point-of-sale locations include the following?</p> <ul style="list-style-type: none"> <li>Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.</li> <li>Do not install, replace, or return devices without verification.</li> <li>Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).</li> <li>Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).</li> </ul>	<ul style="list-style-type: none"> <li>Review training materials.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.9.3 (cont.)	(b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	<ul style="list-style-type: none"> <li>Interview personnel at POS locations.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.10	Are security policies and operational procedures for restricting physical access to cardholder data: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Examine security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Regularly Monitor and Test Networks

### Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.1	(a) Are audit trails enabled and active for system components?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview system administrator.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is access to system components linked to individual users?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview system administrator.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:						
10.2.1	All individual user accesses to cardholder data?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2.2	All actions taken by any individual with root or administrative privileges?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2.3	Access to all audit trails?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2.4	Invalid logical access attempts?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.2.6	Initialization, stopping, or pausing of the audit logs?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.2.7	Creation and deletion of system-level objects?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3	Are the following audit trail entries recorded for all system components for each event:						
10.3.1	User identification?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3.2	Type of event?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3.3	Date and time?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3.4	Success or failure indication?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3.5	Origination of event?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identity or name of affected data, system component, or resource?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe audit logs.</li> <li>Examine audit log settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.4	Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current?  <b>Note:</b> One example of time synchronization technology is Network Time Protocol (NTP).	<ul style="list-style-type: none"> <li>Review time configuration standards and processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.4.1	Are the following processes implemented for critical systems to have the correct and consistent time:						
	(a) Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?	<ul style="list-style-type: none"> <li>Review time configuration standards and processes.</li> <li>Examine time-related system parameters.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?	<ul style="list-style-type: none"> <li>Review time configuration standards and processes.</li> <li>Examine time-related system parameters.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Do systems receive time only from designated central time server(s)?	<ul style="list-style-type: none"> <li>Review time configuration standards and processes.</li> <li>Examine time-related system parameters.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.4.2	Is time data is protected as follows:	<ul style="list-style-type: none"> <li>Examine system configurations and time-synchronization settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(a) Is access to time data restricted to only personnel with a business need to access time data?						
	(b) Are changes to time settings on critical systems logged, monitored, and reviewed?	<ul style="list-style-type: none"> <li>Examine system configurations and time-synchronization settings and logs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.4.3	Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock).  <i>Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).</i>	<ul style="list-style-type: none"> <li>Examine system configurations.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.5	Are audit trails secured so they cannot be altered, as follows:						
10.5.1	Is viewing of audit trails limited to those with a job-related need?	<ul style="list-style-type: none"> <li>Interview system administrators.</li> <li>Examine system configurations and permissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	<ul style="list-style-type: none"> <li>Interview system administrators.</li> <li>Examine system configurations and permissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	<ul style="list-style-type: none"> <li>Interview system administrators.</li> <li>Examine system configurations and permissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?	<ul style="list-style-type: none"> <li>Interview system administrators.</li> <li>Examine system configurations and permissions.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	<ul style="list-style-type: none"> <li>Examine settings, monitored files, and results from monitoring activities.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows?  <b>Note:</b> Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.						
10.6.1	(a) Are written policies and procedures defined for reviewing the following at least daily, either manually or via log tools? <ul style="list-style-type: none"> <li>All security events</li> <li>Logs of all system components that store, process, or transmit CHD and/or SAD</li> <li>Logs of all critical system components</li> <li>Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are the above logs and security events reviewed at least daily?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.6.2	(a) Are written policies and procedures defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy?	<ul style="list-style-type: none"> <li>Review security policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are reviews of all other system components performed in accordance with organization’s policies and risk management strategy?	<ul style="list-style-type: none"> <li>Review risk assessment documentation.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.6.3	(a) Are written policies and procedures defined for following up on exceptions and anomalies identified during the review process?	<ul style="list-style-type: none"> <li>Review security policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is follow up to exceptions and anomalies performed?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.7	(a) Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?	<ul style="list-style-type: none"> <li>Review security policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are audit logs retained for at least one year?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Examine audit logs.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are at least the last three months' logs immediately available for analysis?	<ul style="list-style-type: none"> <li>Interview personnel.</li> <li>Observe processes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.8	<i>For service providers only:</i> Is a process implemented for the timely detection and reporting of failures of critical security control systems as follows:						
	(a) Are processes implemented for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"> <li>Firewalls</li> <li>IDS/IPS</li> <li>FIM</li> <li>Anti-virus</li> <li>Physical access controls</li> <li>Logical access controls</li> <li>Audit logging mechanisms</li> <li>Segmentation controls (if used)</li> </ul>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Does the failure of a critical security control result in the generation of an alert?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.8.1	For service providers only: Are failures of any critical security controls responded to in a timely manner, as follows:						
	(a) Are processes for responding to critical security control failures defined and implemented, and include: <ul style="list-style-type: none"> <li>Restoring security functions</li> <li>Identifying and documenting the duration (date and time start to end) of the security failure</li> <li>Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause</li> <li>Identifying and addressing any security issues that arose during the failure</li> <li>Implementing controls to prevent cause of failure from reoccurring</li> <li>Resuming monitoring of security controls?</li> </ul>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are failures in critical security controls documented, including: <ul style="list-style-type: none"> <li>Identification of cause(s) of the failure, including root cause</li> <li>Duration (date and time start and end) of the security failure</li> <li>Details of the remediation required to address the root cause?</li> </ul>	<ul style="list-style-type: none"> <li>Examine records of security control failures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.9	Are security policies and operational procedures for monitoring all access to network resources and cardholder data: <ul style="list-style-type: none"> <li>Documented</li> <li>In use</li> <li>Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>Review security policies and operational procedures.</li> <li>Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>




**Requirement 11: Regularly test security systems and processes**

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.1	(a) Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?  <i>Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.</i>	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Does the methodology detect and identify any unauthorized wireless access points, including at least the following? <ul style="list-style-type: none"> <li>WLAN cards inserted into system components;</li> <li>Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and</li> <li>Wireless devices attached to a network port or network device.</li> </ul>	<ul style="list-style-type: none"> <li>Evaluate the methodology.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?	<ul style="list-style-type: none"> <li>Examine output from recent wireless scans.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?	<ul style="list-style-type: none"> <li>Examine configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.1.1	Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?	<ul style="list-style-type: none"> <li>Examine inventory records.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.1.2	(a) Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?	<ul style="list-style-type: none"> <li>Examine incident response plan (see Requirement 12.10).</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is action taken when unauthorized wireless access points are found?	<ul style="list-style-type: none"> <li>Interview responsible personnel.</li> <li>Inspect recent wireless scans and related responses.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.2	<p>Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows:</p> <p><b>Note:</b> Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.</p> <p>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</p>						
11.2.1	(a) Are quarterly internal vulnerability scans performed?	<ul style="list-style-type: none"> <li>Review scan reports.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Does the quarterly internal scan process address all "high risk" vulnerabilities and include rescans to verify all "high-risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved?	<ul style="list-style-type: none"> <li>Review scan reports.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.2.1 (cont.)	(c) Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Interview personnel.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.2.2	(a) Are quarterly external vulnerability scans performed? <b>Note:</b> Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	▪ Review results from the four most recent quarters of external vulnerability scans.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	▪ Review results of each external quarterly scan and rescan.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?	▪ Review results of each external quarterly scan and rescan.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.2.3	(a) Are internal and external scans, and rescans as needed, performed after any significant change? <b>Note:</b> Scans must be performed by qualified personnel.	▪ Examine and correlate change control documentation and scan reports.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Does the scan process include rescans until: – For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS, – For internal scans, a passing result is obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	▪ Review scan reports.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Interview personnel.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.3	<p>Does the penetration-testing methodology include the following?</p> <ul style="list-style-type: none"> <li>Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)</li> <li>Includes coverage for the entire CDE perimeter and critical systems</li> <li>Includes testing from both inside and outside the network</li> <li>Includes testing to validate any segmentation and scope-reduction controls</li> <li>Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5</li> <li>Defines network-layer penetration tests to include components that support network functions as well as operating systems</li> <li>Includes review and consideration of threats and vulnerabilities experienced in the last 12 months</li> <li>Specifies retention of penetration testing results and remediation activities results</li> </ul>	<ul style="list-style-type: none"> <li>Examine penetration-testing methodology.</li> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.3.1	(a) Is <i>external</i> penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	<ul style="list-style-type: none"> <li>Examine scope of work.</li> <li>Examine results from the most recent external penetration test.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<ul style="list-style-type: none"> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.3.2	(a) Is <i>internal</i> penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	<ul style="list-style-type: none"> <li>Examine scope of work.</li> <li>Examine results from the most recent internal penetration test.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<ul style="list-style-type: none"> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	<ul style="list-style-type: none"> <li>Examine penetration testing results.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.3.4	If segmentation is used to isolate the CDE from other networks:						
	(a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?	<ul style="list-style-type: none"> <li>Examine segmentation controls.</li> <li>Review penetration-testing methodology.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Does penetration testing to verify segmentation controls meet the following? <ul style="list-style-type: none"> <li>Performed at least annually and after any changes to segmentation controls/methods.</li> <li>Covers all segmentation controls/methods in use.</li> <li>Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.</li> </ul>	<ul style="list-style-type: none"> <li>Examine results from the most recent penetration test.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<ul style="list-style-type: none"> <li>Interview responsible personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question	Expected Testing	Response (Check one response for each question)				
		Yes	Yes with CCW	No	N/A	Not Tested
11.3.4.1	For service providers only: If segmentation is used:					
(a)	Is PCI DSS scope confirmed by performing penetration tests on segmentation controls at least every six months and after any changes to segmentation controls/methods?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(b)	Does penetration testing cover all segmentation controls/methods in use?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(c)	Does penetration testing verify that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(d)	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.4	(a) Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: - At the perimeter of the cardholder data environment, and - At critical points in the cardholder data environment.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(c) Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.5	<p>(a) Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?</p> <p><i>Examples of files that should be monitored include:</i></p> <ul style="list-style-type: none"> <li>• System executables</li> <li>• Application executables</li> <li>• Configuration and parameter files</li> <li>• Centrally stored, historical or archived, log, and audit files</li> <li>• Additional critical files determined by entity (for example, through risk assessment or other means)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Observe system settings and monitored files.</li> <li>▪ Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<p>(b) Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly?</p> <p><b>Note:</b> For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).</p>	<ul style="list-style-type: none"> <li>▪ Observe system settings and monitored files.</li> <li>▪ Review results from monitoring activities.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	<ul style="list-style-type: none"> <li>▪ Examine system configuration settings.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.6	Are security policies and operational procedures for security monitoring and testing: <ul style="list-style-type: none"> <li>▪ Documented</li> <li>▪ In use</li> <li>▪ Known to all affected parties?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine security policies and operational procedures.</li> <li>▪ Interview personnel.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>





## Maintain an Information Security Policy

### Requirement 12: Maintain a policy that addresses information security for all personnel

**Note:** For the purposes of Requirement 12, “personnel” refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the entity’s site or otherwise have access to the company’s site cardholder data environment.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	<ul style="list-style-type: none"> <li>Review the information security policy.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	<ul style="list-style-type: none"> <li>Review the information security policy.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.2	(a) Is an annual risk assessment process implemented that: <ul style="list-style-type: none"> <li>Identifies critical assets, threats, and vulnerabilities, and</li> <li>Results in a formal, documented analysis of risk?</li> </ul> <i>Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.</i>	<ul style="list-style-type: none"> <li>Review annual risk assessment process.</li> <li>Interview personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?	<ul style="list-style-type: none"> <li>Review risk assessment documentation.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following:  <b>Note:</b> Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.						



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.3.1	Explicit approval by authorized parties to use the technologies?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Authentication for use of the technology?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	A list of all such devices and personnel with access?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Acceptable uses of the technologies?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Acceptable network locations for the technologies?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.7	List of company-approved products?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.3.10	(a) For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need?  <i>Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.</i>	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?	<ul style="list-style-type: none"> <li>Review usage policies.</li> <li>Interview responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	<ul style="list-style-type: none"> <li>Review information security policy and procedures.</li> <li>Interview a sample of responsible personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4.1	<i>For service providers only.</i> Have executive management established responsibility for the protection of cardholder data and a PCI DSS compliance program, as follows:						
	(a) Has executive management assigned overall accountability for maintaining the entity's PCI DSS compliance?	<ul style="list-style-type: none"> <li>Examine documentation.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Has executive management defined a charter for the PCI DSS compliance program and communication to executive management?	<ul style="list-style-type: none"> <li>Examine PCI DSS charter.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5	(a) Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?	<ul style="list-style-type: none"> <li>Review information security policy and procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are the following information security management responsibilities formally assigned to an individual or team:						



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.5.1	Establishing, documenting, and distributing security policies and procedures?	▪ Review information security policy and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	▪ Review information security policy and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	▪ Review information security policy and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.4	Administering user accounts, including additions, deletions, and modifications?	▪ Review information security policy and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.5	Monitoring and controlling all access to data?	▪ Review information security policy and procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	▪ Review security awareness program.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do security awareness program procedures include the following:						
12.6.1	(a) Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)?  <i>Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.</i>	▪ Review security awareness program. ▪ Review security awareness program procedures. ▪ Review security awareness program attendance records.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are personnel educated upon hire and at least annually?	▪ Examine security awareness program procedures and documentation.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Have employees completed awareness training and are they aware of the importance of cardholder data security?	▪ Interview personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.6.2	Are personnel required to acknowledge at least annually that they have read and understood the security policy and procedures?	<ul style="list-style-type: none"> <li>Examine security awareness program procedures and documentation.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.7	<p>Are potential personnel (see definition of “personnel” above) screened prior to hire to minimize the risk of attacks from internal sources?</p> <p><i>Examples of background checks include previous employment history, criminal record, credit history and reference checks.</i></p> <p><b>Note:</b> For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</p>	<ul style="list-style-type: none"> <li>Interview Human Resource department management.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:						
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	<ul style="list-style-type: none"> <li>Review policies and procedures.</li> <li>Observe processes.</li> <li>Review list of service providers.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.8.2	<p>Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?</p> <p><b>Note:</b> The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</p>	<ul style="list-style-type: none"> <li>Observe written agreements.</li> <li>Review policies and procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Review policies and procedures and supporting documentation.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Review policies and procedures and supporting documentation.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	<ul style="list-style-type: none"> <li>Observe processes.</li> <li>Review policies and procedures and supporting documentation.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.9	<p><i>For service providers only.</i> Do service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?</p> <p><b>Note:</b> The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</p>	<ul style="list-style-type: none"> <li>Review service provider's policies and procedures.</li> <li>Observe templates used for written agreements.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:						
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	<ul style="list-style-type: none"> <li>Review the incident response plan.</li> <li>Review incident response plan procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Does the plan address the following, at a minimum:						
	– Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	<ul style="list-style-type: none"> <li>Review incident response plan procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	– Specific incident response procedures?	<ul style="list-style-type: none"> <li>Review incident response plan procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	– Business recovery and continuity procedures?	<ul style="list-style-type: none"> <li>Review incident response plan procedures.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question			Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.10.1(b) (cont.)	– Data backup processes?	▪ Review incident response plan procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	– Analysis of legal requirements for reporting compromises?	▪ Review incident response plan procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	– Coverage and responses of all critical system components?	▪ Review incident response plan procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	– Reference or inclusion of incident response procedures from the payment brands?	▪ Review incident response plan procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.2	Is the plan reviewed and tested at least annually, including all elements listed in Requirement 12.10.1?	▪ Review incident response plan procedures. ▪ Interview responsible personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	▪ Observe processes. ▪ Review policies. ▪ Interview responsible personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.4	Is appropriate training provided to staff with security breach response responsibilities?	▪ Observe processes. ▪ Review incident response plan procedures. ▪ Interview responsible personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.5	Are alerts from security monitoring systems included in the incident response plan?	▪ Observe processes. ▪ Review incident response plan procedures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.6	Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	▪ Observe processes. ▪ Review incident response plan procedures. ▪ Interview responsible personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.11	For service providers only: Are reviews performed at least quarterly to confirm personnel are following security policies and operational procedures, as follows:						
	(a) Do reviews cover the following processes: <ul style="list-style-type: none"> <li>– Daily log reviews</li> <li>– Firewall rule-set reviews</li> <li>– Applying configuration standards to new systems</li> <li>– Responding to security alerts</li> <li>– Change management processes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine policies and procedures for performing quarterly reviews.</li> <li>▪ Interview personnel.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are reviews performed at least quarterly?	<ul style="list-style-type: none"> <li>▪ Interview personnel.</li> <li>▪ Examine records of reviews.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.11.1	For service providers only: Is documentation of the quarterly review process maintained to include: <ul style="list-style-type: none"> <li>– Documenting results of the reviews</li> <li>– Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program</li> </ul>	<ul style="list-style-type: none"> <li>▪ Examine documentation from the quarterly reviews.</li> </ul>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Appendix A: Additional PCI DSS Requirements

### Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
A1	<p>Is each entity's (that is, a merchant, service provider, or other entity) hosted environment and data protected, per A1.1 through A1.4 as follows:</p> <p><i>A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.</i></p> <p><b>Note:</b> Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.</p>						
A1.1	<p>Does each entity run processes that have access to only that entity's cardholder data environment, and are these application processes run using the unique ID of the entity?</p> <p><i>For example:</i></p> <ul style="list-style-type: none"> <li>No entity on the system can use a shared web server user ID.</li> <li>All CGI scripts used by an entity must be created and run as the entity's unique user ID</li> </ul>	<ul style="list-style-type: none"> <li>Examine system configurations and related unique IDs for hosted entities.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
A1.2	<p>Are each entity's access and privileges restricted to its own cardholder data environment as follows:</p> <p>(a) Are the user IDs for application processes not privileged users (root/admin)?</p> <p>(b) Does each entity have read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.)?</p> <p><b>Important:</b> An entity's files may not be shared by group.</p>	<ul style="list-style-type: none"> <li>Examine system configurations for application user IDs.</li> <li>Examine system configurations and file permissions for hosted entities.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
A1.2 (cont.)	(c) Do all entities' users not have write access to shared system binaries?	▪ Examine system configurations and file permissions for shared system binaries.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(d) Is viewing of log entries restricted to the owning entity?	▪ Examine system configurations and file permissions for viewing log entries.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(e) Are restrictions in place for the use of these system resources? – Disk space, – Bandwidth, – Memory, – CPU  <i>This ensures that each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows).</i>	▪ Examine system configurations and file permissions for use of: Disk space Bandwidth Memory CPU	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
A1.3	(a) Are logging and audit trails enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10?	▪ Examine log settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	(b) Is logging enabled as follows, for each merchant and service provider environment as follows:						
	– Logs are enabled for common third-party applications?	▪ Examine log settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	– Logs are active by default?	▪ Examine log settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	– Logs are available for review by the owning entity?	▪ Examine log settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	– Log locations are clearly communicated to the owning entity?	▪ Examine log settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
A1.4	Are written policies and processes enabled to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider?	▪ Review written policies and procedures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



## Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
A2.1	<p>For POS POI terminals (<b>at the merchant or payment-acceptance location</b>) using SSL and/or early TLS: Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS</p> <p><b>Note:</b> This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.</p>	<ul style="list-style-type: none"> <li>Review documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
A2.2	<p>For service providers only: Is there a formal Risk Mitigation and Migration Plan in place for all service provider connection points to POS POI terminals that use SSL and/or early TLS (as referred to in A2.1), that includes:</p> <ul style="list-style-type: none"> <li>Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;</li> <li>Risk assessment results and risk reduction controls in place;</li> <li>Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;</li> <li>Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;</li> <li>Overview of migration project plan to replace SSL/early TLS at a future date?</li> </ul>	<ul style="list-style-type: none"> <li>Review the documented Risk Mitigation and Migration Plan.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
A2.3	<p>For service providers only: Is there a secure service offering in place?</p>	<ul style="list-style-type: none"> <li>Examine system configurations and supporting documentation.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



### ***Appendix A3: Designated Entities Supplemental Validation (DESV)***

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.



## Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where “YES with CCW” was checked.

**Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

### Requirement Number and Definition:

	Information Required	Explanation
<b>1. Constraints</b>	List constraints precluding compliance with the original requirement.	
<b>2. Objective</b>	Define the objective of the original control; identify the objective met by the compensating control.	
<b>3. Identified Risk</b>	Identify any additional risk posed by the lack of the original control.	
<b>4. Definition of Compensating Controls</b>	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
<b>5. Validation of Compensating Controls</b>	Define how the compensating controls were validated and tested.	
<b>6. Maintenance</b>	Define process and controls in place to maintain compensating controls.	



## Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
<i>Example:</i>	
3.4	Cardholder data is never stored electronically
Requirement 1	SP+ is not responsible for and does not have access to modify the firewall configurations at these locations.
Requirement 2	SP+ is not responsible for and does not have access to modify the credit card systems configuration at these locations.
Requirement 3	SP+ is not responsible for and does not have access to credit card data storage or the ability to modify how it is transmitted at these locations.
Requirement 4	SP+ is not responsible for and does not have access to modify the encryption configuration used for credit cards at these locations.
Requirement 5	SP+ is not responsible for and does not have access to modify the antivirus software used to protect credit card systems at these locations.
Requirement 6	SP+ is not responsible for and does not have access to install patches or run vulnerability assessments at these locations.
Requirements 7 and 8	SP+ is not responsible for and does not have access to manage user IDs and permissions on the credit card equipment at these locations.
9.1.1	Video cameras are not used to specifically monitor credit card equipment at these locations.
9.5 - 9.8	Credit card data is not normally stored or written on physical media at these locations.
Requirement 10	SP+ is not responsible for and does not have access to system logs and audit trails for the credit card equipment at these locations.
Requirement 11	SP+ is not responsible for and does not have access to the IT security controls protecting the credit card equipment at these locations.
A1	SP+ is not a shared hosting provider.
A2	SSL / Early TLS is not used at these locations.

*If the "Not Tested" column was checked in the questionnaire, use this worksheet to explain why the related requirement was not reviewed as part of the assessment.*

[illegible]





## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (6/24/2022).

Based on the results documented in the SAQ D noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: **(check one)**:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby (<i>SP Plus Corporation</i>) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

**(Check all that apply)**

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version (3.2.1), was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



### Part 3. PCI DSS Validation *(continued)*

#### Part 3a. Acknowledgement of Status *(continued)*

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment. |
| <input type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor ( <i>ASV Name</i> ).   |

#### Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑

Date: 6/24/2022

Service Provider Executive Officer Name: Christopher Ratliff

Title: SVP, Digital Info & Technology

#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

Signature of Duly Authorized Officer of QSA Company ↑

Date:

Duly Authorized Officer Name:

QSA Company:

#### Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

Davis Lentz, ISA 805-079 - Assistance with PCI Review

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

