Schedule 4 - Data Processing and Security Addendum (US Only)

Section 1 Definitions

"Affiliate" means, as to any entity, any other entity that, directly or indirectly, through one or more intermediaries, Controls, is Controlled by or is under common Control with such first entity; as used herein entity means any company, partnership, joint venture or other form of enterprise, domestic or foreign.

"Agents" means the agents, contractors, subcontractors, suppliers, vendors and representatives of Vendor. Vendor's Affiliates that perform Services under this Agreement will be considered Vendor Agents.

"AW" or "Company" means American Water Works Service Company, Inc.

"Background Technology" of a Party means all intellectual property that (a) is (i) owned by such Party, any of its Affiliates or any of its agents, contractors, subcontractors, suppliers, vendors or representatives and (ii) is in existence in electronic or written form on or prior to the Effective Date, or (b) is developed or acquired by such Party, any of its Affiliates or any of its agents, contractors, subcontractors, suppliers, vendors or representatives after the Effective Date independently of the Services.

"Claim" means any and all causes of action, claims, demands, actions, lawsuits and proceedings of every character, kind and nature.

"Company Data" means all data (a) submitted to Vendor or Vendor Agents by or on behalf of Company, (b) accessed or obtained by Vendor or Vendor Agents from Company or Company Agents, and (c) developed or produced by or on behalf of Vendor for Company in the performance of the Services, and any modification or enhancement to or replacement of any of the foregoing. Company Data does not include Systems or data of Vendor existing prior to the Effective Date, nor modifications or enhancements thereof, nor any data of any Vendor customer other than Company, nor any Vendor Background Technology or Vendor Derivative Works.

"Confidential Information" of Company or Vendor, as applicable, means all information (regardless of form) of Company and Vendor, respectively, whether disclosed to or accessed by Company or Vendor in connection with this Agreement, including with respect to Company, the existence and terms of this Agreement, all Company Data, all Personal Data; provided, however, that except to the extent otherwise provided by applicable Law, the term "Confidential Information" will not include information that (a) is independently developed by the recipient, as demonstrated by the recipient's written records, without violating the owner's rights, (b) is or becomes generally known to the public (other than through unauthorized disclosure by or through a Party), (c) is generally disclosed by the owner of such information to a third party free of any obligation of confidentiality, (d) was already known by the recipient at the time of disclosure, as demonstrated by the recipient's written records, and the recipient has no obligation of confidentiality with respect to said information other than pursuant to this Agreement or any confidentiality agreements between Company and Vendor entered into before the Effective Date with respect to said information, or (e) is rightfully received by a Party free of any obligation of confidentiality, provided that (i) such recipient has no knowledge that such information is subject to a confidentiality agreement and (ii) such information is not of a type or character that a reasonable person would have regarded it as confidential. Notwithstanding anything to the contrary, all Personal Data will always constitute Company's Confidential Information for purposes of this Agreement, even if any

Personal Data falls within any of the exceptions set forth in clauses (a) through (e) of this definition.

"Control" means: (a) the legal, beneficial, or equitable ownership, directly or indirectly, of (i) at least fifty percent (50%) of the aggregate of all voting equity interests in an entity, or (ii) equity interests having the right to at least fifty percent (50%) of the profits of an entity or, in the event of dissolution, to at least fifty percent (50%) of the assets of an entity; (b) the power to appoint, directly or indirectly, a majority of the board of directors; (c) the power to control, directly or indirectly, the management or direction of the entity, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise; (d) in the case of a partnership, the holding by an entity (or one of its Affiliates) of the position of sole general partner; or (e) the consolidation, pursuant to GAAP, of an entity into the books and records of another entity (or one of its Affiliates).

"Equipment" means any computer and telecommunications machines and other hardware and related equipment, including (a) mainframe, midrange, server and distributed computing equipment and associated attachments, accessories, peripheral devices, and cabling, (b) personal computers, laptop computers, terminals, workstations and personal data devices and associated attachments, accessories, printers, multi-functional printers, peripheral or network devices, and cabling, and (c) voice, data, video and wireless telecommunications and network and monitoring equipment and associated attachments, accessories, peripheral devices, cell phones and cabling, together with all documentation, corrections, modifications, upgrades, enhancements, additions, new versions, new releases and replacements thereto and thereof.

"Governmental Authority" means any federal, state, municipal, local, territorial, provincial or other governmental department, regulatory authority, judicial or administrative body, whether domestic, foreign or international.

"Law" means any declaration, decree, directive, legislative enactment, statute, order, ordinance, regulation, rule or other binding action of or by any Governmental Authority.

"Litigation Expense" means any and all attorneys' fees (including paralegal fees, investigative fees, expert witness fees, administrative costs, disbursements and all other expenses billed by the attorney), court costs and expenses, even if not recoverable by Law as court costs (including all expenses and taxes incident to arbitration, appellate, bankruptcy and post-judgment proceedings).

"Losses" means any and all damages, fines, penalties, deficiencies, remedial obligations, losses, liabilities (including settlements and judgments), awards, interest and expenses of every character, kind and nature, including Litigation Expenses.

"Malware" means any Software, Equipment or data (a) intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of any Software, Equipment or data (e.g., "viruses" or "worms"), (b) that would disable any Software, Equipment or data, or impair in any way their operation (e.g., "time bombs," "time locks" or "drop dead" devices), (c) that would permit unauthorized access to Software, Equipment or data, to cause such disablement or impairment (e.g., "traps," "access codes" or "trap door" devices), or (d) which contains any other harmful, malicious or hidden procedures, routines or mechanisms which would cause any Software, Equipment or data, to cease functioning, to damage or corrupt storage media, Software, Equipment, data or communications, or otherwise interfere with operations.

"Personal Data" means any Company Data that identifies or is capable of identifying an individual, or is otherwise defined as "personal information", "personal data", "sensitive personal data", "personally identifiable information", "personal health information", "non-public personal information" or similar terms under applicable Laws.

"Proprietary Rights" means all past, present, and future rights of the following types, which may exist or be created under the Laws of any jurisdiction in the world: (a) rights associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights, and mask works; (b) trademark and trade name rights and similar rights; (c) trade secret rights; (d) patents and industrial property rights; (e) other proprietary rights in intellectual property of every kind and nature; and (f) rights in or relating to registrations, renewals, extensions, combinations, divisions, and reissues of, and applications for, any of the rights referred to in clauses (a) through (e) of this definition.

"Security Breach" means (1) the failure by Vendor or its subcontractor(s) to properly handle, manage, store, destroy or otherwise control, or the unauthorized disclosure by Vendor or its subcontractor of: (i) Personal Data or AW PI in any format; (2) an unintentional violation of Vendor's privacy policy or misappropriation that results in the violation of any applicable data privacy laws or regulations; or (3) any other act, error, or omission by Vendor or its subcontractor in its capacity as such which is reasonably likely to result in the unauthorized disclosure of personal data.

"Services" means the services provided by Vendor to Company under any agreement to which this Data Processing and Services Addendum is attached.

"Software" means any instruction or set of instructions that are used (e.g., read, compiled, processed or manipulated) by, in or on Equipment, including APIs, source code or object code versions of applications programs, operating system software, and other programs, computer software languages and utilities, in each case, in whatever form or media, including the tangible media upon which they are recorded or printed, together with all documentation, corrections, modifications, upgrades, enhancements, additions, new versions, new releases and replacements thereto and thereof.

"Systems" means an interconnected grouping of manual or electronic processes used to perform the Services, including Equipment, Software and associated attachments, features, accessories, peripherals and cabling, together with all documentation, corrections, modifications, upgrades, enhancements, additions, new versions, new releases and replacements thereto and thereof.

"Vendor" means the party delivering Services to Company.

"Vendor Derivative Works" means any modifications, upgrades or enhancements to, or derivative works of, Vendor's Background Technology or Vendor Owned Materials.

"Vendor Owned Materials" means the Materials that are owned, acquired or developed by or on behalf of Vendor, Vendor's Affiliates or Vendor Agents, excluding in each case the Work Product, and used in connection with the Services, but including the Software specified as such in the Statements of Work.

Section 2 Record Retention.

Vendor will maintain complete and accurate records sufficient to document the performance of the Services and invoicing of fees (collectively, "Contract Records"). Vendor will retain Contract Records in accordance with generally accepted accounting principles ("GAAP") during the Term and for at least three (3) years after termination.

Section 3 Audits

3.1 Company Audits.

(a) With at least five (5) days advance notice to Vendor, an accounting firm selected by Company ("Company Auditor") may examine the books and records of Vendor solely for the purposes of verifying compliance with this Agreement. Company shall maintain such information in confidence, provided such information may be admitted into evidence in connection with any legal action relating to the collection by Company of any fees or payments hereunder. If the results of the audit or inspection reveal that Company has overpaid by five percent (5%) or more of the fees and payments due and owing to Vendor, then Vendor shall bear the reasonable expenses of such audit and inspection. All overpayment amounts identified by such audit shall be reimbursed immediately to Company.

(b) Company Auditors will not be given access to (i) the information of Vendor that is not related to Company or the Services, (ii) Vendor locations that are not related to Company or the Services, or (iii) Vendor's internal expenses, except to the extent such expenses are the basis upon which Company is charged or are necessary to calculate the applicable fees.

3.2 Vendor Controls.

At all times during the Term and continuing thereafter until the completion of the audit of Company's financial statements for Company's fiscal year during which this Agreement expires or is terminated, Vendor will, and will cause Vendor Agents to:

(a) maintain in effect the controls, operations and systems that are sufficient for Company to comply with its obligations under the Sarbanes-Oxley Act ("SOX");

(b) On an annual basis each calendar year during the Term, Vendor will engage, at its cost and expense, a nationally-recognized auditor to conduct an end-to-end audit of the systems used by Vendor or its service providers with respect to its provision of the Services, in accordance with SSAE 16 or its successor standard, and have such auditor issue a Type II Audit Report. Upon AW's request at any time, Vendor will provide AW with a copy of the then-current Audit Report. To the extent the Audit Report identifies any material deficiencies that adversely affect the Software, Systems, or Services, Vendor shall notify AW in writing and shall, at its sole cost and expense, promptly evaluate and, as appropriate, develop and implement a remediation plan in order to resolve such identified material deficiencies.

(c) generally cooperate with Company Auditors in any other way that Company or Company Auditors may reasonably request to enable Company to comply, and Company Auditors to evaluate whether Company complies, with SOX as it relates to the Services, Software, or Systems;

Section 4 BC/DR Plan.

(a) At all times during the Term, Vendor will maintain and comply with a commercially reasonable business continuity and disaster recovery plan for the Services (the "BC/DR Plan"). Vendor will exercise and test (and re-test as necessary) at least once annually the operability of the BC/DR Plan to confirm that the BC/DR Plan is fully operational, and will update the BC/DR Plan to reflect any changes or lessons learned as a result of any exercise, test or recovery from an actual incident. The parties agree that the BC/DR plan shall be solely the responsibility of (and under the control of) Vendor. Vendor will provide a non-confidential summary of the BC/DR Plan to Company upon request.

(b) Upon the occurrence of any business interruption, disaster or Force Majeure (as such term may be defined under the agreement to which this Addendum attached) event, Vendor will implement the BC/DR Plan in accordance with its terms and provide the services described therein. The occurrence of a business interruption, disaster or Force Majeure event will not relieve Vendor of its obligation to implement the BC/DR Plan and provide the services described therein. In the event of a business interruption, disaster or Force Majeure event, Vendor will not increase the fees or charge Company usage or other charges in addition to the fees.

Section 5 Data and Confidentiality

5.1 Protection of Data

5.1.1 Data Ownership. AW shall be, for all purposes hereof and as between Vendor and AW, the sole and exclusive owner of any information or data supplied by AW and/or an Affiliate of AW or created in connection with Vendor's performance of Services hereunder, including, but not limited to all Personal Data, proprietary data, information and records, customer information, prospect information, all internal financial information and projections, and all billing, pricing, personnel, salary, and insurance information, of or relating to AW and its Affiliates (collectively, "**AW Data**"). Except as expressly provided herein and as necessary to performance hereunder, Vendor and its employees, agents and subcontractors shall not have any rights in or to the AW Data in any form or any information derived from or in connection with the AW Data.

5.2 Data Protection.

5.2.1 If, in connection with this Agreement or performance hereunder, Vendor receives, is exposed to, uses, discloses or processes Personal Data on behalf of AW or its Affiliates (including the outputs from such processing), Vendor shall: (a) process such Personal Data only pursuant to the written instructions of AW (or, with AW's prior written approval, those of AW's Affiliates); (b) implement appropriate technical and organizational measures to protect such Personal Data from and against any accidental or unlawful destruction or any accidental loss, alteration, unauthorized disclosure, use or access, including, but not limited to, in connection with any transmission of such Personal Data over a public or private network, and from and against all other unlawful forms of processing, access, use and disclosure; (c) except where instructed otherwise by AW in writing, make all reasonable efforts to delete such Personal Data after a reasonable time, given the purposes for which they are held, unless it is appropriate to keep such data longer as a matter of Law; (d) not use or further disclose such Personal Data to any person except as required or permitted by this Agreement or with the prior written consent of AW; (e) not process such Personal Data except to the extent reasonably necessary for performance of Vendor's Services under this Agreement. In all events and circumstances in which Vendor uses, discloses or processes Personal Data on behalf of AW, Vendor shall (and AW specifically instructs Vendor to), in such use, disclosure or processing of such Personal Data, take only such steps as are reasonably necessary for performance pursuant to this Agreement and take all such steps as are consistent

and in accordance and compliance with the provisions of this Agreement and all applicable Laws and regulations of all relevant jurisdictions; and (f) unless otherwise agreed, not process or store any Personal Data in jurisdiction(s) outside of the United States. For avoidance of doubt, Personal Data includes CCPA Personal Information as defined in Section 5.4.1. AW or its Affiliates, as the case may be, shall be the sole and exclusive owner of Personal Data, regardless of whether such data is delivered to Vendor by, or on behalf of AW or an Affiliate.

5.2.2 Files that contain AW Data should be encrypted by Vendor at rest and in transit, regardless if stored on a server, desktop, laptop, or other device or media, and regardless of the transfer mechanism or endpoint (including, without limitation, to a designated FTP site).

5.2.3 A Security Breach must be reported to AW Security Operations – ITS for data security incidents and AW Operations Security for any security breach involving physical security. Security Breaches are to be reported to AW Security Hot-line 1-866-801-1123, Option 4. Any Security Breach must be reported within twenty-four (24) hours of Vendor's awareness that such Breach has occurred.

5.2.4 To the extent a Security Breach is attributable to Vendor, Vendor shall bear (a) the expenses incurred by Vendor in complying with its legal obligations relating to such Security Breach and (b) in addition to any other damages for which Vendor may be liable for under this Agreement, the following expenses incurred by AW in responding to such breach, to the extent applicable: (i) the expense of providing legally required notice to affected individuals; (ii) the expense of providing legally required notice to governmental authorities, credit bureaus, and other required entities; (iii) the expense of providing affected individuals with credit monitoring services for a specific period not to exceed twelve (12) months; and (v) the expense of any other measures required under applicable Law. Notwithstanding the foregoing, the parties agree that the reference to "expenses" in this section shall not apply to any such costs, including fines or penalties, assessed as a result of any contributory action or inaction by AW, AW's Affiliates, or third parties under AW's control.

5.2.5 If a Party discovers or is notified of a breach or potential breach of the obligations of confidentiality set forth in this Section 5 and such breach or potential breach results in the unauthorized possession, use or knowledge, or attempt thereof of the other Party's Confidential Information, the Party by or through whom the unauthorized possession, use or knowledge, or attempt thereof occurred shall: (a) promptly notify the other Party of any unauthorized possession, use or knowledge, or attempt thereof, of the other Party's Confidential Information by any person or entity that may become known to such Party; (b) promptly furnish to the other Party full details of the unauthorized possession, use or knowledge, or attempt thereof; (c) assist the other Party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge, or attempt thereof, of Confidential Information; (d) timely cooperate with the other Party in any litigation and investigation against third parties deemed necessary by the other Party to protect its Proprietary Rights; and (e) promptly use its commercially reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge, or attempt thereof, of Confidential Information. For avoidance of doubt, Confidential Information that is Personal Data shall also be subject to obligations associated with a Security Breach.

5.2.6 Without limiting its obligations under Section 5.2.3 – Section 5.2.5, Vendor agrees to maintain reasonable security (consistent with the standards applied by CCPA and other applicable Law) of PI (as defined in Section 5.4.1) and Confidential Information, and agrees to notify AW of any actual, suspected or alleged Security Breach that has resulted, or may result in, a compromise

to the confidentiality, integrity, or availability of PI or any Confidential Information within twenty-four (24) hours after detection. Upon identification of a Security Breach, Vendor will:

5.2.6.1 Cooperate fully with AW in investigating and responding to the Security Breach;

5.2.6.2 Identify AW PI (as defined in Section 5.4.1) and Personal Data affected;

5.2.6.3 Immediately take steps to contain the Security Breach and preserve evidence for any necessary investigation;

5.2.6.4 Complete a thorough forensic investigation of the Security Breach, consistent with industry best practices, and share with AW the results of all investigations, which will include, but not be limited to: (1) a full description of the circumstances surrounding the Incident; (2) a description of the evidence reviewed and analysis completed; (3) identification of the incident's root cause, if determined; (4) a determination of whether any AW PI or Personal Data was accessed or acquired without authorization;

5.2.6.5 Permit AW, or its designated agent, to conduct an investigation at its cost, during normal business hours upon prior written notice of not less than 3 business days, and in a manner that does not unduly interfere with the Vendor's operations, of the Security Breach;

5.2.6.6 Cooperate with AW as reasonably necessary to facilitate compliance with any applicable Laws; and

5.2.6.7 Indemnify and hold AW harmless from any Claims, Losses, or damages of any nature whatsoever, including reasonable attorneys' fees, arising from or relating to such Security Breach, except to the extent it if determined to be attributable to AW.

5.2.7 Vendor shall maintain a privacy policy during the duration of the Agreement consistent with the requirements of Law (including, without limitation CCPA, as defined in Section 5.4).

5.2.8 Vendor warrants that any Systems on which Personal Data may reside are free of and do not contain any code or mechanism that collects information or asserts control of the Systems without AW's or Vendor's consent, or which may restrict legitimate access to the Personal Data. Vendor further warrants that it will not introduce via any means, any Malware, spyware, adware, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to Personal Data, or which may restrict the legitimate access to or use of the Personal Data.

5.2.9 At least once per year, Vendor shall conduct audits of the information technology and information security controls for all facilities used in performance of Services under this Agreement, including, without limitation, obtaining a network-level vulnerability assessment and penetration testing performed by a recognized third-party audit firm based on the recognized industry best practices. Upon AW's written request once annually, Vendor shall make available to AW for review its SOC2 Type 2 audit summary (or its successor attestations) and any reports relating to ISC/ICE 27001/27002, and summaries regarding network-level vulnerability assessment and penetration testing. AW shall treat such audit reports as Vendor's Confidential Information under the Agreement. Any exceptions noted on the SOC 2 (or successor attestations) report will be promptly addressed with the development and implementation of a corrective action plan by Vendor.

5.3 No Implied Rights or Licenses. Except as expressly set forth in this Agreement, nothing in this Agreement shall be deemed to grant to a Party, by implication, estoppel or otherwise, license rights, ownership rights or any other intellectual property or other Proprietary Rights in any resources or other property (including intellectual property) that is owned, licensed, leased, acquired or otherwise obtained by the other Party or any Affiliate of the other Party.

5.4 CCPA Compliance

5.4.1 Vendor represents, warrants, covenants and agrees that it (i) is, and will maintain its status as, a "service provider" as defined by the California Consumer Privacy Act, as well as in the California Attorney General implementing regulations (collectively "CCPA") and will comply with all of its obligations related thereto under the CCPA, and its obligations under other applicable Laws and this Agreement; (ii) will not "sell" AW "personal information" (as those terms are defined under the CCPA), which includes any personal information processed by Vendor in performing the Services for AW ("CCPA Personal Information" or "AW PI"); (iii) acknowledges that AW is the owner and controller of the AW PI and it will process AW PI solely as and when directed by AW for AW's designated business purposes; and (iv) will not retain, use, or disclose AW PI other than for AW's business purposes, and will not retain, use, or disclose AW PI for any commercial purpose other than providing the Services specified in the Agreement; (v) will maintain reasonable security of the AW PI consistent with the standards of reasonableness applicable to the CCPA and all other applicable Laws; (vi) will reasonably cooperate with AW's responses to consumer rights requests, and at minimum promptly facilitate AW's ability to identify, retrieve, copy and/or delete specific PI of specific data subjects; and (vii) will promptly convey any data subject rights requests regarding AW PI it receives to AW and will not itself respond to such requests. Vendor hereby certifies that it understands the restrictions in this Section 5.4 and will at all times comply with such restrictions.

5.4.2 Vendor shall not assign, delegate, of subcontract any of its rights or obligations concerning AW PI, or otherwise disclose AW PI, to any other party, without AW approval, and then only (a) for the purpose of performing the Services for AW; and (b) as permitted by applicable Law. If any such disclosure is approved, Vendor shall obtain contractual commitments with the subcontractor or other recipient of AW PI that are substantially similar to those imposed on Vendor hereunder.

5.4.3 It is understood and agreed that the CCPA has an effective date of January 1, 2020, that the CCPA remains subject to amendment and to implementing regulations that have not yet been finalized, and that other state legislatures and the U.S. Congress are considering enacting similar laws ("New Privacy Laws"). Accordingly, Vendor agrees to implement such additional policies in order for AW to comply with New Privacy Laws, (including, without limitation, providing CCPA-required commitments and certification), and undertaking reasonable commitments to otherwise address New Privacy Laws. AW and Vendor will work together in good faith to amend this Agreement in order for AW to comply with the CCPA and applicable New Privacy Laws, if necessary. If the parties cannot agree to reach an amendment regarding additional compliance commitments within thirty (30) days, either party may terminate the Agreement, subject to a transition period designated by AW which shall not exceed one hundred eight (180) days during which Vendor will continue to provide the Services and assist in transitioning the Services to a new vendor at its then-current rates, and AW shall only be responsible for fees and costs on a pro rata basis through the post-transition termination date.

5.4.4 Vendor agrees to defend (if requested by AW), indemnify and hold AW harmless from and against third party Claims resulting from any breach of its representation, warranties, covenants or obligations under this Section 5.4 by Vendor (to the extent caused by Vendor).

5.5 General Confidentiality Obligations.

All Confidential Information will be protected from unauthorized use and disclosure by the receiving Party by using the same degree of care as such Party employs to avoid unauthorized use and disclosure of its own confidential information of a similar nature (but in no event less than reasonable care). Neither Party will use or reproduce the Confidential Information of the other Party except as necessary to perform, receive, or use the Services. Neither Party will disclose, publish, release, transfer or otherwise make available Confidential Information of the other Party in any form to, or for the use or benefit of, any entity, except as expressly permitted by this Agreement or with the disclosing Party's prior approval, to be given in the disclosing Party's sole discretion. Each of Company and Vendor will, however, be permitted to disclose relevant aspects of the other's Confidential Information to its officers, directors, employees, agents, professional advisors (including attorneys, bankers and consultants), contractors, subcontractors, suppliers, vendors and representatives, and to the officers, directors, employees, agents, professional advisors, contractors, subcontractors, suppliers, vendors and representatives of its Affiliates (collectively, "Permitted Parties"), in each case to the extent that such disclosure is not restricted under any applicable agreements or any Laws and to the extent that such disclosure is necessary for the performance of its duties and obligations under this Agreement or the determination, preservation or exercise of its rights and remedies under this Agreement or under Law; provided that the receiving Party will take all reasonable measures to ensure that Confidential Information of the other Party is not used, disclosed or duplicated in contravention of the terms of this Agreement by any of the receiving Party's Permitted Parties. The receiving Party will be liable for any act or omission by a Permitted Party to whom it has disclosed the other Party's Confidential Information which act or omission constitutes a breach of the obligations under this Section. The terms of this Section will not restrict any disclosure required by any competent Governmental Authority (provided that the receiving Party will give prompt notice to the other Party of such requirement and cooperate, upon the other Party's request, in obtaining a protective order with respect to such information).

5.6 Return of Confidential Information.

Upon request by Company, Vendor will (a) promptly provide to Company all or any part of Company's Confidential Information, and (b) securely and permanently erase or destroy all or any part of Company's Confidential Information in Vendor's or any Vendor Agents' possession or control in accordance with then-current generally accepted industry standards. Upon Company's request, Vendor will certify to Company that Vendor and each applicable Vendor Agent has complied with the immediately preceding sentence in a notice signed by an officer of Vendor and each applicable Vendor Agent. Company may identify to Vendor any part of Company's Confidential Information that is subject to a litigation hold or is otherwise not to be unilaterally erased or destroyed by Vendor, and Vendor will refrain from erasing or destroying such Confidential Information and will maintain such Confidential Information in accordance with Company's instructions. Vendor will not withhold any of Company's Confidential Information as a means of resolving any dispute.

5.7 PCI Compliance.

5.7.1 If Vendor is providing payments solutions to Company, Vendor agrees to utilize and will continue to utilize a PCI compliant payment processing service provider and shall, together with and through its contracted payment processing service provider, perform the Services in compliance with the PCI DSS, and hereby acknowledges its responsibility for the security of any Cardholder Data or Sensitive Authentication Data (as such terms are defined in the PCI DSS) that

it processes in connection with this Agreement. In the event Vendor switches payment processing service providers during the Term or brings payment processing services in-house, Vendor shall ensure such new payment processing service provider or in-house processing remains compliant with the obligations of this Agreement. Vendor will perform all tasks, assessments, reviews, penetration tests, scans and other activities required under the PCI DSS Merchants or Service Providers, as applicable (including any compliance guidance issued by the PCI Security Standards Council or its subordinate bodies), or otherwise to validate its compliance with the PCI DSS as it relates to the system elements and portions of cardholder data environment (as such terms are defined in the PCI DSS) for which Vendor is responsible (the "PCI Environment").

5.7.2 Vendor will ensure that (i) all Software used to perform the Services that process, store or transmit card-holder data will comply with the requirements of the most current published version of the Payment Application Data Security Standard, and (ii) such Software, and all enhancements thereto, remain "Validated Payment Applications" as determined by the PCI Security Standards Council.

5.7.3 obtain Payment Card Industry (PCI) certification from a Qualified Security Assessor (QSA) for each facility from which the Services are provided (whether the Services are provided by Vendor or a Vendor Agent). Each Vendor PCI certificate will be completed annually. The PCI certification must be from a QSA.