October 8, 2018

TO: HOLDERS LIST

SUBJECT: Rail Track Inspection System
CONTRACT NO. 070973

ADDENDUM NUMBER # 02

This addendum is issued to add, remove, clarify and amend the following:

PROCUREMENT PROCESS

A. ATTACHMENT F

Addition of SaaS Technical Requirements Matrix.

PSA No: _____

ATTACHMENT F

PORT OF TACOMA SOFTWARE AS A SERVICE AGREEMENT

(Software)

This Port of Tacoma Software as a Service Agreement ("Agreement") is by and between the Port of Tacoma ("Port") (on behalf of the Northwest Seaport Alliance (NWSA)) and _____ hereby known as the "Vendor." This Agreement is effective when fully executed and approved in accordance with applicable laws, rules and regulations ("Effective Date"). This Agreement is in relation to the Software as a Service Licensing only. Any services or products necessary for Implementation will be performed or obtained in accordance with a separate Personal Services Agreement ("PSA") XXXXXX.

THE SOFTWARE AS A SERVICE AGREEMENT IS MADE IN CONJUNCTION WITH THE TERMS AND CONDITIONS SET FORTH IN THE PSA RESULTING FROM REQUEST FOR PROPOSAL ("RFP") XXXXX. IN THE EVENT OF A CONFLICT BETWEEN THIS AGREEMENT AND THE PSA, AND/OR THE RFP, THE TERMS AND CONDITIONS OF THE FOLLOWING SHALL BE CONTROLLING IN THE PRIORITY SET FORTH BELOW, WITH NUMBER 1 BEING THE MOST CONTROLLING AND NUMBER 3 BEING THE LEAST CONTROLLING:

1. SOFTWARE AS A SERVICE AGREEMENT
2. PSA
3. RFP
4. Vendor's Proposal

RECITALS

A. The Port desires to enter into this Software as a Service Agreement with Vendor to provide Hosted Software Services as described in RFP XXXXX.

B. Vendor desires and agrees to perform the Services as outlined in RFP XXXXX.

TERMS OF SERVICE

EACH PARTY ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS, AND THAT THE PERSON SIGNING ON ITS BEHALF HAS BEEN AUTHORIZED TO DO SO. THE PERSON EXECUTING THIS AGREEMENT ON VENDOR'S BEHALF REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO BIND THE VENDOR TO THESE TERMS AND CONDITIONS.

1. DEFINITIONS. The following capitalized terms shall have the following meanings whenever used in this Agreement.

1.1. "AUP" means Vendor's Acceptable Use Policy dated_____currently posted at _____.

1.2. "Acceptance" means written confirmation by the Port that the Vendor's software has met the requirements stated in RFP XXXXX and in its RFP Proposal.

1.3. "Anniversary Date" means the date that is 365 days after the Effective Date, and each anniversary thereafter of the date that is 365 days after the Effective Date, during this Agreement's Term.

1.4. "Client Data" means the data that Designated Users transmit and/or enter into the database provided as part of the Vendor's system in connection with their use of the SaaS Software pursuant to this Agreement.

1.5. "Deliverables" means the Services and all software that Vendor is required to deliver to the Port under this Agreement.

1.6. "Designated User" means Port authorized personnel who have access the Vendor's SaaS Software for business purposes.

1.7. "Documentation" means all documents, including documents that are Deliverables described in this Agreement and includes, but is not limited to, any and all operator's or user's manuals, training materials, guides, commentary, listings, requirements traceability matrices and other materials for use in conjunction with and for the operation of services that are to be delivered by the Vendor under this Agreement.

1.8. "Effective Date" means the date of the last party signature on this Agreement.

1.9. "Force Majeure Event" means neither party shall be liable or deemed to be in default for any delay in performance occasioned by unforeseeable causes beyond the contract and without the fault or negligence of the parties, including but not restricted to, acts of God or the public enemy, fires, floods, epidemics, quarantines, restrictions, strikes or labor disputes, embargoes, sabotage, cable cut not caused by Vendor, or usually severe weather; provided that in all cases of delay in performance, the Vendor shall immediately notify the Port by telephone, of such delay, and follow up such oral notice with prompt written notice detailing the cause for delay. The Vendor shall make every reasonable effort to complete performance as soon as possible. This clause does not apply to Service issues involving network outages cause by or related to a network that is not owned or controlled by the Vendor.

1.10. "Party" and "Parties" means the Port and Vendor.

1.11. "SaaS Software Application", "SaaS Solution" and "SaaS Software" mean the computer software listed on a SaaS subscription schedule to which Vendor has granted the Port access and use as part of the subscription. This includes any customization, other derivative works, upgrades, releases, fixes, patches, etc., related to the software that Vendor develops or deploys during the term of this Agreement, together with all documentation provided by or otherwise required of Vendor for any of the software, customization, other derivative works, upgrade, releases, fixes, patches, etc.

1.12. "SLA" means Port's standard service level agreement, as set forth in Exhibit B, Port of Tacoma Service Level Agreement (SLA).

1.13. "System" means the Port's access to and use of and Vendor's SaaS Software Applications and other services listed in this Agreement (Exhibit A, Licensed Software and Fee Schedule), in accordance with the terms and conditions set forth in this Agreement.

1.14. "Term" is defined in Section below.

2. THE SYSTEM.

The System is defined as the Port's access to and use of and Vendor's provision of the SaaS Software Applications and other services listed in this Agreement, in accordance with the terms and conditions set forth in this Agreement. (See Definitions, 1.13.,"System")

2.1. Use of the System. During the Term, the Port may access and use the System pursuant to the terms the Vendor's AUP.

2.2. Service Levels. Vendor shall provide the remedies listed in Exhibit B, Port of Tacoma SLA, attached hereto and incorporated herein, for any failure of the System listed in the SLA. Such remedies are Port's remedies for any failure of the System. Credits issued pursuant to the SLA apply to outstanding or future invoices and may be deducted from any final payment upon termination of this Agreement. Vendor is not required to issue refunds or to make payments against such credits under any circumstances, including without limitation after termination of this Agreement.

2.3. Application Support Hours The Vendor's application core support hours must be from 07:00 to 18:00 PST/PDT, Monday through Friday (excluding Port holidays). The Port's holidays are New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Veterans Day, Thanksgiving Day, the Day after Thanksgiving, Christmas Eve Day, and Christmas Day. For Severity Levels 1 and 2 (as documented in Exhibit B, Service Level Agreement), the Vendor must be available during non-core support hours.)

2.4. Virus Protection. The Vendor will use the most robust up-to-date virus and malware protection software and/or technology solutions available. The Vendor agrees to prevent viruses from being loaded into the SAAS Solution and into the Port's own standard IT environment through its software. If a virus is inadvertently introduced, the Vendor will take immediate and appropriate steps to reduce the effects of the virus and will notify the Port immediately upon discovery of the virus. The Port expects the Vendor to take immediate steps to respond to the virus, and for root cause analysis to be performed at a later reasonable time, i.e., within hours after the effects of the virus are reduced. Upon completion of the analysis, the results of the Vendor's root cause analysis will be shared with the Port, in writing.

2.5. Software and Hardware Updates / Patches. The Vendor is responsible for ensuring that systems, applications, database, operating systems and firewalls receive regular updates and/or patches for SaaS system high availability and protection.

2.6. Data Centers / Disaster Recovery. Any and all data centers utilized must be located within the continental United States. Data centers, server, storage and network infrastructure utilized must provide high levels of redundancy and availability. The Vendor will provide system restore/image, snapshots and backups on an hourly, daily, weekly and monthly schedule for recovery. In addition, the Vendor will ensure that network, server and storage infrastructure is actively monitored and managed for availability and performance which includes site security including but not limited to: on-premises security personnel, continuous video surveillance, screening of all people entering or exiting the premises, seismically braced server racks, high-tech fire suppression systems and round-the-clock monitoring of server operations. Disaster

Recovery and penetration testing exercises must be documented along with a plan to fix any deficiencies. The outcome of these exercises must be available to the Port upon request. All client data must be stored and remain in the continental United States.

2.7. Documentation: The Port may reproduce and use the documentation solely as necessary to support Designated Users' use of the System.

2.8. Designated System Revisions. The Port recognizes the Vendor may revise System features and functions at any time. If any such revision to the System materially reduces features or functionality mutually agreed upon by the Parties, the Port may within 30 days of notice of the revision terminate this Agreement without cause. If any such revision to the SLA materially reduces service levels mutually agreed upon by the Parties, the Port may within 30 days of notice of revision terminate this Agreement without cause.

3. SYSTEM FEES. The Port shall pay Vendor the fee set forth in Exhibit A, Licensed Software and Fee Schedule, attached hereto and incorporated herein.

3.1. Implementation Schedule. For purposes of a first time set-up and/or implementation for the Port, Vendor will provide a schedule for the implementation, including the milestones that must be met and hard dates by which the milestones must be met.

3.2. Milestone Payments. Payment for first time implementation for the Port will be tied to successful completion of milestones associated with hard dates or deadlines. A payment schedule is provided in Exhibit A, Licensed Software and Fee Schedule.

4. CYBERSECURITY AND CLIENT DATA PRIVACY.

4.1. Cybersecurity. All solution components, including code base, application, servers, web servers, databases, data at rest and in motion, and network infrastructure including firewalls, are developed, configured and maintained using industry standard cybersecurity best practices in accordance with NIST Special Publication 800-53r4 (or successor publications). For the web servers, the Vendor will use SSL certificate to secure connectivity for users. The Vendor will maintain a documented Security Plan that it will supply to the Port upon request. The Vendor will undergo Security Vulnerability Audits annually, and supply audit reports to the Port upon request. Once the Security Vulnerability Audit is completed, the Vendor will create a remediation plan and implement the plan to address any failed areas. Within five (5) business days, the Port will receive a copy of the Vendor's remediation plan. The Vendor will notify the Port immediately of any security breach of the Vendor's SaaS infrastructure or unauthorized access to the Port's data; will work immediately and without interruption to resolve the breach and the vulnerability; and will provide the Port with a copy of an incident review.

4.2. Use of Client Data. Unless it receives the Port's prior written consent, Vendor: (a) shall not access, process, or otherwise use Client Data other than as necessary to facilitate the System; and (b) shall not grant any third party access to Client Data, including without limitation Vendor's other customers. Notwithstanding the foregoing, Vendor may disclose Client Data as required by applicable law or by proper legal or governmental authority. Vendor shall give the Port prompt notice of any such legal or governmental demand and reasonably cooperate with the

Port in any effort to seek a protective order or otherwise to contest such required disclosure.

4.3. Protection of Client Data Stored Within the SaaS Solution. The Port's confidential information, sensitive data and/or personally identifiable information may be stored within the SaaS Software. The Port requires that the Vendor understand that (1) the Port owns its own data, (2) the Vendor will provide protection against the release or transfer of that data, (3) the Vendor is required to notify the Port within two (2) hours of any breach and will provide the Port with the specific steps that will be taken if a security breach occurs or is suspected.

4.4. Data Encryption. Vendor shall ensure that all data transfers, i.e., data moving or data at rest, will be encrypted. For data in transit, the Vendor will ensure encryption with 256-bit encryption and Transport Layer Security (TLS) and file-level encryption will be performed via Transparent Data Encryption (TDE). In order to ensure client anonymity, the Vendor will encrypt the database names. Data at rest will have a robust encryption method in place to encrypt all Client data elements. In addition, the Vendor will encrypt all user passwords with a form-based system login and store all encrypted user passwords in a secure database.

4.5. Records Retention. Until the expiration of six years after the term of this Agreement, Vendor agrees to maintain accurate records of all work done in providing services specified by this Agreement, including the Port's client data hosted, stored, or maintained by Vendor, and to deliver such records to the Port upon termination of this Agreement or otherwise as requested by the Port.

4.6. Risk of Exposure. The Port recognizes and agrees that hosting data online involves risks of unauthorized disclosure or exposure and that, in accessing and using the System, the Port assumes such risks. Vendor warrants that it will make all commercially available efforts to ensure that Client Data will not be exposed or disclosed through errors or the actions of third parties. The Vendor must ensure that it has performed all commercially available efforts to protect the Port's client data in accordance with Section 2. The System, and Section 2.5 Cybersecurity.

4.7. Data Accuracy. Vendor shall have no responsibility or liability for the accuracy of data uploaded to the System by the Port, including without limitation Client Data and any other data uploaded by Designated Users.

4.8. SSAE16 Audits. During the term of this Agreement, and so long as SSAE16 remains a current and industry standard auditing standard, Vendor agrees to annually undertake an audit in accord with the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements No. 16 or a successor standard ("SSAE16") with respect to the services offered in Exhibit A. Upon the Port's request, and no more than annually, Vendor agrees to provide a copy of its then-current SSAE16 audit report for the Port's review. Additionally, the Port requires the Vendor to perform an annual Cybersecurity Vulnerability assessment performed at the same intervals as the audit and the findings relating to Port's SaaS system will be shared with the Port.

5. THE PORT'S RESPONSIBILITIES & RESTRICTIONS.

5.1. Acceptable Use. The Port shall comply with the AUP identified in Section 1.1. The Port shall not:

(a) use the System for service bureau or time-sharing purposes or in any other way allow third parties to exploit the System; (b) provide System passwords or other log-in information to any third party; (c) share non-public System features or content with any third party, subject to the Port's obligations set forth in Section 11.10; or (d) access the System in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the System, or to copy any ideas, features, functions or graphics of the System. In the event that it suspects any breach of the requirements of this Section 5.1, including without limitation by Designated Users, Vendor will immediately notify the Port of any breach for unauthorized use.

5.2. Unauthorized Access. The Port shall take reasonable steps to prevent unauthorized access to the System, including without limitation by protecting its passwords and other log-in information. The Port shall notify Vendor immediately of any known or suspected unauthorized use of the System or breach of its security and shall use best efforts to stop said breach.

5.3. Designated Users & System Access. The Port is responsible and liable for: (a) Designated Users' use of the System, including without limitation unauthorized Designated User conduct and any User conduct that would violate the AUP or the requirements of this Agreement applicable to the Port; and (b) any use of the System through Port's account, whether authorized or unauthorized, except to the extent said use is performed by persons or entities not employed by or affiliated with the Port.

6. INTELLECTUAL PROPERTY (IP).

6.1. IP Rights to the System. Vendor retains all right, title, and interest in and to the System, including without limitation all software used to provide the System and all graphics, user interfaces, logos, and trademarks reproduced through the System. This Agreement does not grant the Port any intellectual property license or rights in or to the System or any of its components, except to the extent this Agreement provides the Port with the right to use the System as expressly provided herein. The Port recognizes that the System and its components are protected by copyright and other laws.

7. CONFIDENTIAL INFORMATION. "Confidential Information": Pursuant to this Agreement, Vendor may collect, or the Port may disclose to Vendor, financial, personnel or other information that the Port regards as proprietary or confidential ("Confidential Information"). Confidential Information shall belong solely to the Port. Vendor shall use such Confidential Information only in the performance of its services under this Agreement and shall not disclose Confidential Information or any advice given by it to the Port to any third party, except with the Port's prior written consent or under a valid order of a court or governmental agency of competent jurisdiction and then only upon timely notice to the Port. The Port may require that Vendor's officers, employees, agents or sub-vendors agree in writing to the obligations contained in this section. Confidential Information shall be returned to the Port upon termination of this Agreement. The confidentiality obligation contained in this section shall survive termination of this Agreement. Confidential Information shall not include data or information that: (a) is or was in the possession of Vendor before being furnished by the Port, provided that such information or other data is not known by Vendor to be subject to another confidentiality agreement with or other obligation of secrecy to the Port; (b) becomes generally available to the public other than as a result of disclosure by Vendor, or; (c) becomes available to Vendor on a non-confidential basis from a source other than the Port, provided that such source is not known by Vendor to be subject to a confidentiality agreement

with or other obligation of secrecy to the Port.

7.1. Non-disclosure. The Port may require a Non-Disclosure Agreement to be signed by the Vendor and its employees.

7.2. Termination & Return. Upon termination of this Agreement, the Vendor shall return all copies of the Port's data within 5 business days or certify, in writing, the destruction thereof.

7.3. Retention of Rights. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. The Parties will retain all right, title, and interest in and to all their Confidential Information.

8. REPRESENTATIONS & WARRANTIES.

8.1. From Vendor. Vendor represents and warrants that it is the owner of the System and of each and every component thereof, or the recipient of a valid license thereto, and that it has and will maintain the full power and authority to grant the rights granted in this Agreement without the further consent of any third party. In the event of a breach of the warranty in this Section, Vendor, at its own expense, will promptly take the following actions: (a) secure for the Port the right to continue using the System; (b) replace or modify the System to make it noninfringing; or (c) terminate the infringing features of the Service and refund to the Port any prepaid fees for such features, in proportion to the portion of the Term left after such termination. In conjunction with Port's right to terminate for breach where applicable, the preceding sentence states Vendor's sole obligation and liability, and Port's sole remedy, for breach of the warranty in this Section and for potential or actual intellectual property infringement by the System.

8.2. Warranty Period. For the period of one (1) year (Warranty Period), the SaaS Software supplied to the Port shall conform to the Acceptance criteria set forth in the RFP XXXXX and the Vendor's RFP Response and shall be free from error or defect that materially impairs their use.

8.3. Warranty Use. All services and SaaS Software supplied by the Vendor to the Port shall be provided to the Port free and clear of any and all restrictions on or conditions all liens, claims, mortgages, security interests, liabilities and encumbrances of any kind.

9. INDEMNIFICATION.

9.1. Save Harmless. The Vendor shall defend, indemnify and hold the Port harmless from any and all liability, claims, damages, costs, expenses, and actions, including reasonable attorney's fees, to the extent caused by or arising from the negligent or wrongful acts or omissions under this Agreement of the Vendor, its employees, agents, or subcontractors, that cause death or bodily injury, or damage to property, or arising out of a failure to comply with any state or federal statute, law, regulations or act.

10. Term & Termination.

10.1. Term. The term of this Agreement (the "Term") shall commence on the Effective Date and continue for a period of ____. By mutual agreement, this Agreement may be renewed, under the existing terms and conditions, for a period of successive one (1) year periods, not to exceed X years.

10.2. Termination for Convenience. The Port may terminate this Agreement at any time for government convenience upon 30 days' advance written notice. On the date of termination, the Port shall pay the Vendor any outstanding undisputed fees for Services not yet performed.

10.3. Effects of Termination. Upon termination of this Agreement, the Port shall cease all use of the System and delete, destroy, or return all copies of the documentation in its possession or control, subject to the Port's obligations to retain and/or disclose records pursuant to applicable law. The Vendor will return all client data within 5 business days via the last back-up copy of the system database. The following provisions will survive termination or expiration of this Agreement: (a) any obligation of the Port to pay fees incurred before termination; (b) Articles and Sections *IP*, *Confidential Information*, and *Limitation of Liability*.

11. MISCELLANEOUS.

11.1. Independent Contractors. The parties are independent contractors and will so represent themselves in all regards. Neither party is the agent of the other, and neither may make commitments on the other's behalf. The parties agree that no Vendor employee or contractor will be an employee of The Port.

11.2. Notices. Vendor may send notices pursuant to this Agreement to the following Port representative ____, at the following e-mail address:_____ , and such notices will be deemed received 24 hours after they are sent. The Port may send notices pursuant to this Agreement to _____, and such notices will be deemed received 24 hours after they are sent.

11.3. Assignment & Successors. Vendor may not assign this Agreement or any of its rights or obligations hereunder without Port's express written consent. Any attempt to assign this Agreement, without prior written approval, shall result in the termination of this Agreement, at the sole discretion of the Port. All rights of action for any breach of this Agreement by the Vendor are reserved by the Port.

11.4. Subcontracting. The Vendor may enter into any subcontract(s) relation to the performance of this Agreement if mutually agreed upon in writing by both parties. The Vendor's use of subcontracts shall not in any way relieve the Vendor of its responsibility for the professional and technical accuracy, adequacy, and timeliness of the work to be performed under this Agreement. The Vendor shall be and remain liable for the performance of the work in accordance with this Agreement, as well as any damages to the Port caused by the negligent performance or non-performance of the Vendor's subcontractor(s).

11.5. Severability. To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any clause of this Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of this Agreement is held to be invalid or otherwise unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent permitted by applicable law, and the remaining provisions of this Agreement will continue in full force and effect.

11.6. No Waiver. Neither party will be deemed to have waived any of its rights under this Agreement by lapse of time or by any statement or representation other than by an authorized representative in an explicit written waiver. No waiver of a breach of this Agreement will

constitute a waiver of any other breach of this Agreement.

11.7. Choice of Law & Jurisdiction: This Agreement will be governed solely by the internal laws of the State of Washington. The parties consent to the personal and exclusive jurisdiction of the federal and state courts of Pierce County, Tacoma, Washington.

11.8. Time is of the Essence. Vendor agrees that time is of the essence in its performance under this Agreement.

11.9. Technology Export. The Port shall not: (a) permit any third party to access or use the System in violation of any U.S. law or regulation; or (b) export any software provided by Vendor or otherwise remove it from the United States except in compliance with all applicable U.S. laws and regulations. Without limiting the generality of the foregoing, The Port shall not permit any third party to access or use the System in, or export such software to, a country subject to a United States embargo (as of the Effective Date, Cuba, Iran, North Korea, Sudan, and Syria).

11.10. Public Records. The Port has to avail its records to a public inspection. Any and all records, i.e., proposals and pricing provided by the Vendor, this Agreement, client data, and other documentation are considered non-confidential and non-proprietary in nature and will be subject to public records requests, public disclosure, and audit.

11.11. Amendments. Any amendment or modification to this Agreement must be mutually agreed upon by both parties via a written amendment to be effective.

ATTACHMENT F

General SaaS Requirements Checklist: 070973

The following table describes requirements for SaaS services that the Port of Tacoma finds most important. Please fill in the table below and indicate, by placing an "x" in the appropriate column for each item to indicate which are Fully Met, Partially Met, or Not Met by the proposed solution. Specify in the Comments column any clarifying information. Information in the Comments column is required if selecting Partially Met.

	Requirement	Fully Met	Part-ially Met	Not Met	Comments (including Restrictions and Exceptions)
	The system shall be capable of supporting 24/7 365 availability				
	The system shall be protected by current virus and malware protection software				
	Vendor indemnifies the Port of Tacoma if vendor system infects the Port with virus/malware				
	The system shall be protected by firewalls that serve to prevent unauthorized access and attacks				
	The system shall be capable of providing an audit log of:				
	All users with general access				
	All users with superuser access				
	All users with system level access				
	All users with database level access				
	All users with server level access				
	The system shall be capable of providing an audit log of access for all users				
	The system shall be supported by data centers located in the continental United States				
	The system shall have redundancy protocols in place that support				
	Less than 15-minute downtime for users (RTO Recovery Time Objective)				
	Less than 30-minute loss of data for users(RPO Recovery Point Objective)				
	Do not require users or PoT staff to update configuration settings				
	The system shall have backup protocols in place that support				
	A restore/ image point for data taken once per hour				
	A restore/ image point for system and data taken once per day				
	A restore/ image point for system and data taken once per week				
	A restore/ image point for system and data taken once per month in an				

	Requirement	Fully Met	Part-ially Met	Not Met	Comments (including Restrictions and Exceptions)
	additional format [such as tapes] in the event of a total loss of the system				
	The system shall be physically protected by:				
	On premise security personnel				
	Controlled access				
	Continuous video surveillance				
	Seismically braced server racks				
	Fire suppression systems				
	Continuous monitoring of server operations				
	The system shall be supported by a disaster recovery plan				
	That is tested at minimum of 1x per year				
	Testing shall be of minimum impact to PoT users				
	The system shall be able to ensure that no data belonging to the PoT is shared with other customers, no commingling of data with other customers is permitted				
	The system shall be supported by a penetration testing plan				
	That is tested at minimum of 1x per year				
	Testing shall be of minimum impact to PoT users				
	Testing shall not require PoT staff to support				
	The system shall be able to ensure that no data belonging to the PoT leaves the continental United States				
	The system shall be composed of components in accordance/compliant with NIST Special Publication 800-53r4 including but not limited to:				
	The system integrates with Active Directory				
	The system shall be capable of supporting secure passwords by supporting one of the following				
	Integration with Active directory				
	Support the following requirements: Minimum password length – 12 Characters Password expiration of 90 days Complex password requirements – 3 of 4 (lower case, upper case, number or Special Character)				

	Requirement	Fully Met	Part-ially Met	Not Met	Comments (including Restrictions and Exceptions)
	The system shall be supported by a documented Security Plan				
	The vendor shall be able to provide an annual audit on request to support the following items:				
	Security Vulnerability				
	SSAE16				
	The system vendor will be able to meet the following notification obligations to the PoT:				
	Immediate notification in the event of a system failure				
	Immediate notification upon the discovery of a virus attack				
	Root cause analysis documentation within one day of the virus attack effects being reduced				
	Immediately in the event of a security breach				
	Immediately if an acceptable use breach is detected				
	2 hours in the event of a client data breach				
	Within five (5) business days any remediation items needed as a result of the Security Vulnerability Audit				
	Immediately by phone in the event of a Force Majeure resulting in a system outage				
	In writing subsequent to phone call with details of the outage				
	Notifications of upgrades/ patches etc. that may alter or change the user experience				
	Notifications of the system that materially change the SLA that was mutually agreed upon				
	Notifications of upgrades/ patches etc. that may alter or change the security infrastructure				
	The vendor will have application support hours:				
	07:00 to 18:00 PST/PDT Monday through Friday (excluding port holidays) The Port's Holidays are New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Veterans Day, Thanksgiving Day, the				

	Requirement	Fully Met	Part-ially Met	Not Met	Comments (including Restrictions and Exceptions)
	Day after Thanksgiving, Christmas Eve Day, and Christmas Day.				
	For Severity Levels 1 and 2 (as documented in Exhibit B, Service Level Agreement), the Vendor must be available during non-core support hours.				