PUGET SOUND ENERGY

INFORMATION SECURITY REQUIREMENTS ADDENDUM
TO MASTER SERVICES AGREEMENT NO. _____

(Supplier / Hosted)

THIS INFORMATION SECURITY REQUIREMENTS ADDENDUM ("Security Addendum") is by and between Puget Sound Energy, Inc. ("PSE") and the party identified in the signature block below ("Supplier") and supplements that certain **<*agreement type, #*>** between the Parties dated _____ ("MSA") and any statements of work, exhibits, orders, attachments, or ancillary agreements thereto (together with the MSA, the "Agreement") and is incorporated by reference therein. PSE and Supplier may also be referred to herein individually as a "Party" or collectively as the "Parties". Terms defined in the MSA and not otherwise defined herein shall have the meanings given those terms in the MSA.

This Security Addendum sets forth certain information security obligations and information security activities to be performed by Supplier, and supplements the confidentiality and security obligations of Supplier under the Agreement. In the event of any conflict between this Security Addendum and the Agreement, this Security Addendum shall control solely to the extent of such conflict.

1. System Security and Data Backup

1.1. Information Security

(a) As used in this Security Addendum "PSE Confidential Information" means "Confidential Information" and includes: (i) PSE Information as defined in the MSA; and (ii) non-public PSE operational, business, and financial data, and PSE project, design, roadmap, and architecture plans.

(b) PSE makes PSE Confidential Information available to Supplier exclusively for the necessary business purpose of fulfilling the Services. Supplier is prohibited from collecting, selling, retaining, using or disclosing such PSE Confidential Information for any purpose other than for those specific purposes stated in the Agreement. Supplier is responsible for protecting the confidentiality, integrity and availability of all PSE Confidential Information in its possession or control and for all Processing of PSE Confidential Information. For purposes of this Security Addendum, the term "Process", "Processed", or "Processing" means any operation or set of operations which is performed on PSE Confidential Information by or for Supplier, whether or not by automated means, such as the access, collection, use, storage, disclosure, dissemination, combination, recording, organization, structuring, adaption, alteration, copying, transfer, retrieval, consultation, disposal, restriction, erasure and/or destruction of PSE Confidential Information. Supplier shall:

(i) Process PSE Confidential Information solely in accordance with PSE's documented instructions, including those set forth in this Security Addendum, the MSA, and applicable Statement of Work; and

(ii) Process PSE Confidential Information in accordance with all applicable laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations (collectively, "Applicable Law").

(c) Supplier will implement and maintain physical and logical security controls to prevent unauthorized access, collection, storage, disclosure, misuse, reidentification, damage or destruction of PSE Confidential Information in its possession or control, including a documented information security program that complies with the requirements of this Security Addendum ("Information Security Program"). Supplier shall provide to PSE annually (beginning with the date of the Parties' execution of this Security Addendum) a current summarized description of its Information Security Program, including documentation verifying the authenticity and integrity of any software that will have access to PSE Confidential Information (e.g., patch management program, testing, fingerprints, or cipher hashes). The Information Security Program shall be available for review and audit by PSE upon request. The Information Security Program and the security controls that cover Supplier's networks, systems, applications, technical services, and premises (collectively, the "Supplier Systems") will be appropriate for the nature of the PSE Confidential Information that Supplier Processes and will meet or exceed prevailing industry standards. During the term of the Agreement, Supplier will comply with its Information Security Program and will perform all of the security controls that are required pursuant to this Section 1.1(c). Without limiting the foregoing, the Information Security Program and such security controls will include, without limitation:

(i) Physical Security - maintaining physical security of all premises where PSE Confidential Information will be Processed;

(ii) Background Checks - taking reasonable precautions with respect to the employment of personnel (including Subcontractor personnel, collectively the "Support") who have access to PSE Confidential Information, including background checks and other measures as may be required under the Agreement or Applicable Law. Background checks and security clearances required for specific access privileges should be renewed on a reasonable periodic basis or if any Support is suspected or recognized by Supplier or PSE as a security risk;

(iii) Training - training of Support on the proper use of data, computer systems, and the importance of information security via the provision of training materials on an annual basis;

(iv) Access - restricting access to records and files containing PSE Confidential Information to Support who need such information to perform their job duties; encrypting of all PSE Confidential Information on laptops and other portable devices; and encrypting of all records and files containing PSE Confidential Information that will (x) travel across public networks without secure connections or VPN; (y) will be transmitted wirelessly, or (z) will be transmitted outside of the secure Supplier Systems.

In addition, Supplier will ensure that Support who have access to PSE Confidential Information comply with the terms and conditions of this Security Addendum;

(v) Monitoring - monitoring of Supplier Systems for unauthorized use of or access to PSE Confidential Information;

(vi) Testing - testing changes to Supplier Systems to ensure the security posture of the system(s) and environments are not compromised by the change;

(vii) Network Security - maintaining network and electronic security perimeter controls to protect PSE Confidential Information;

(viii) Incident Response - taking appropriate corrective action; documenting and training on how to respond to an Unplanned Event (as defined in Section 3.1 below), and testing the plan on at least an annual basis;

(ix) No Commingling of Data - maintaining all PSE Confidential Information so as to be compartmentalized or otherwise logically separate from, and in no way commingled with, other information of Supplier or its other customers;

(x) Updates and Security Patches - maintaining Supplier Systems connecting to the PSE network with current updates to remediate security vulnerabilities or weaknesses identified to Supplier by OEM(s) or others, and applying security patches in a timely manner;

(xi) Anti-virus/anti-malware - ensuring that Supplier Systems are protected by anti-virus/anti-malware software;

(xii) Records - maintaining complete and accurate user logs, access credential data, records, and other information applicable to PSE network connection access activities for at least 90 days; and

(xii) Data and Hardcopy Destruction - destroying (and certifying in writing such destruction) any and all PSE Confidential Information upon the earlier of: (A) any expiration or termination of the MSA; or (B) when no longer needed by Supplier to fulfill its performance obligations under the Agreement; or (C) as requested by PSE. Notwithstanding the immediately foregoing, certain PSE records have regulatory requirements governing their retention periods with which Supplier must comply. PSE will notify Supplier in writing of any applicable requirements for the records Supplier is Processing hereunder, as may be updated from time to time by PSE in writing. Supplier's Processing of PSE's (**fill in**) mandates Supplier's retention of these records for a period of (**fill in**) years.

(d) Supplier will notify PSE within 12 hours of when any Support should be restricted from remote or onsite access to PSE Confidential Information. This includes circumstances such as: (i) persons permitted access are no longer qualified to maintain access; or (ii) Supplier's employment of, or relationship with, any Support is terminated for any reason.

(e) Supplier will not transfer, or cause to be transferred, any PSE Confidential Information to any third party or from one jurisdiction inside the United States to another jurisdiction outside of the United States without the prior written consent of PSE in each instance.

1.2. Audit

(a) Supplier will procure from an independent third party on at least an annual basis a SOC 2 Type II audit or its then-current AICPA equivalent, as set forth in the AICPA Trust Services Criteria. The independent audit will cover Supplier Systems. Supplier shall provide the audit report to PSE prior to or upon execution of the MSA (or this Security Addendum if executed subsequent to the MSA), and annually within five (5) business days of completion of the audit. The report must include: (i) whether the

audit revealed any material vulnerability in the Supplier Systems; and (ii) if any material vulnerability is revealed, the nature of those vulnerabilities.

(b) From time to time PSE, at its own expense, may conduct or engage an independent third party to conduct (subject to such third party entering into a commercially reasonable, mutually agreed upon non-disclosure agreement with Supplier), an information security audit of the Supplier security controls described in Section 1.1(c).

(c) If any audit conducted under (a) or (b) above reveals one or more material vulnerabilities, Supplier will correct each such vulnerability at its sole cost and expense and will certify in writing to PSE that it has corrected all such vulnerabilities. Supplier will complete all vulnerability corrections within fifteen (15) business days of receipt of the audit findings, unless the vulnerabilities by their nature cannot be corrected within such time, in which case the corrections must be completed within a mutually agreed upon time not to exceed sixty (60) days.

2. Security Breach

2.1. Notice. Supplier shall notify PSE within **12 hours** of any recognized, suspected, or attempted physical or logical breach of the security of the Supplier Systems (each a "Security Breach"), further subject to the following:

(a) Recognized Security Breach involving PSE Confidential Information: **2 hours**; and

(b) Suspected Security Breach involving PSE Confidential Information: **4 hours.**

2.2. Security Logs and Mitigating Controls. In the case of a suspected or recognized Security Breach involving PSE Confidential Information, Supplier shall, upon PSE's request:

(a) Promptly provide PSE with relevant security logs for PSE's own investigative purposes and cooperate to the extent possible with PSE's investigation; and

(b) Promptly provide PSE with any known or suspected mitigating controls or patches that PSE might implement to limit related cyber security risk.

2.3. Remediation. Supplier will take reasonable and appropriate steps to promptly stop and remediate any Security Breach, and will cooperate with PSE's reasonable requests regarding the breach.

2.4. Data Retention Practices. Upon recognizing a Security Breach, Supplier shall also, upon PSE's request, modify its data retention practices as specified by PSE until ninety (90) days after the breach is resolved.

2.5. PSE Contact Information. Supplier shall notify PSE's IT Support Center (ITSC) at (425) 398-6020; subsequent contact shall be as mutually agreed.

2.6. PSE Security Breach. In the case of any recognized, suspected, or attempted physical or logical breach involving the security of PSE systems that PSE reasonably suspects to be related to Supplier Systems or the usage thereof, Supplier shall cooperate with PSE's investigation of such breach and provide PSE any mitigating controls or patches to limit related cybersecurity risk.

3. Technology Recovery

3.1. Definitions. For the purposes of this Security Addendum, the following definitions shall apply:

"Business Continuity" means Supplier's ability to continue critical business operations without stoppage, irrespective of the adverse circumstances of an Unplanned Event.

"Business Continuity Plan" means the logistical plan created and documented by Supplier specifying the policies, processes, and procedures Supplier will apply to recover after an Unplanned Event to partially or completely restore interrupted critical business operations within a predetermined period of time.

"Disaster Recovery" means Supplier's ability to recover or continue critical technology infrastructure and computing systems after an Unplanned Event.

"Disaster Recovery Plan" means the logistical plan created and documented by Supplier specifying the processes, policies, and procedures Supplier will apply to recover after an Unplanned Event to partially or completely restore interrupted critical technology infrastructure and computing systems within a predetermined period of time.

"Recovery Point Capability" or "RPC" means the actual tested and proven amount of data loss measured backward in time from the start of an Unplanned Event to the point of the last recoverable backup.

"Recovery Point Objective" or "RPO" means the maximum acceptable amount of data loss measured backward in time from the start of an Unplanned Event to the point of the last recoverable backup, as solely defined by PSE. The RPO for purposes of this Security Addendum shall be ____ hours ***(12 hours if left blank)***.

"Recovery Time Capability" or "RTC" means the actual tested and proven duration of time within which the Services, supporting technology infrastructure, and Supplier's critical business operations are restored after an Unplanned Event. The RTC is measured forward in time, from the initial occurrence of an Unplanned Event to the restoration of the Services.

"Recovery Time Objective" or "RTO" means the duration of time within which the Services, supporting technology infrastructure, and Supplier's critical business operations must be restored after an Unplanned Event in order to avoid unacceptable consequences associated with an interruption in Supplier's business processes. The RTO is measured forward in time, from the initial occurrence of an Unplanned Event to the restoration of the Services, as solely defined by PSE. The RTO for purposes of this Security Addendum shall be ___ hours ***(4 hours if left blank)***.

"Service Provider" means an approved subcontractor third-party entity that Supplier contracts with to provide technology services and/or systems access in support of the Services specified in this Security Addendum.

"Unplanned Event" means a logical or physical incident or event causing an unexpected disruption in the Supplier's ability to provide the Services to PSE, including without limitation: malware; compromised information systems; natural, technical, or man-made disasters; acts of crime or terrorism; other business or technical disruptions.

3.2. Unplanned Events. Should an Unplanned Event occur, Supplier shall:

(a) Promptly initiate the Disaster Recovery Plan and/or Business Continuity Plan, as applicable;

(b) Notify PSE as soon as possible (in no event longer than the time periods specified in Section 2.1), with initial contact to be made to PSE's IT Support Center ("ITSC") at (425) 398-6020 and subsequent contact shall be as mutually agreed;

(c) Provide PSE updates hourly, or sooner should major status changes occur;

(d) Restore all Services and business operations that support the Services in a timeframe that meets or exceeds both the RTO and RPO; and

(e) Notify PSE upon the restoration of normal operations of the Services.

3.3. Disaster Recovery and Business Continuity Planning. Throughout the term of the Agreement, Supplier shall perform, at a minimum, the following activities to ensure Supplier's ability to provide uninterrupted Services after an Unplanned Event, or to recover within agreed-upon times:

(a) Build and maintain a Disaster Recovery and Business Continuity Plan which shall be updated:

(i) At least once a year;

(ii) In the event of major Supplier organizational changes;

(iii) If professional or other services that support Supplier's ability to provide the Services are outsourced to a Service Provider;

(iv) If any outsourced Services are outsourced to an alternate Service Provider; and

(v) If any outsourced Services are insourced to be within Supplier's purview.

(b) Maintain a recovery facility or subscribe to recovery facility services that allow Supplier to restore Services per the requirements set forth herein;

(c) Perform comprehensive exercises of its Disaster Recovery and Business Continuity capabilities at least once a year, and also when major changes are made to production systems that affect the Services;

(d) Allow PSE to observe during scheduled recovery exercises, and allow PSE access to all Supplier Systems to ensure all functionality and data have been restored;

(e) Allow PSE site visits unrelated to scheduled exercises; and

(f) Comply with PSE's requests for documentation to satisfy recovery questions.

3.4. Documentation. Supplier will provide the following documentation to PSE on at least an annual basis:

(a) Evidence of an owned and operational recovery facility or current subscription to recovery facility services;

(b) Evidence that the Disaster Recovery Plan and Business Continuity Plan are both updated as specified herein;

(c) Evidence that Disaster Recovery and Business Continuity exercises are both performed at least annually; and

(d) Results from the Disaster Recovery and Business Continuity exercises demonstrating:

(i) Supplier's execution of the respective plans; and

(ii) Exercise results detailing: (A) successes; (B) failures; (C) remediation plan for failures and issues encountered during testing; and (D) RTC and RPC capabilities.

4. Data Transfers (in the event that Supplier transfers or receives PSE Confidential Information)

4.1. Shared Information. During the term of the MSA, PSE may request that: (a) Supplier transfers certain PSE Confidential Information to one or more third parties designated by PSE (each, a "Designated Recipient"); or (b) Supplier receives certain PSE Confidential Information from one or more third parties designated by PSE (each, a "Designated Representative"). In the event that PSE makes such a request, PSE will provide written notice and express permission to Supplier that: (i) identifies the applicable Designated Recipient or Designated Representative; (ii) identifies the PSE Confidential Information that Supplier must either transfer to such Designated Recipient or receive from such Designated Representative (in each case, the "Shared Information"); and (iii) sets forth additional terms and conditions including the data transfer mechanism, adequate permissions and grants of authority, if any, that apply to the transfer or receipt of the Shared Information by Supplier pursuant to this Section 4.1. The Shared Information shall remain the sole and exclusive property of PSE.

4.2. Secure Transfer. When Supplier transfers Shared Information at the written request of PSE pursuant to this Section 4, Supplier shall:

(a) Transfer solely the Shared Information to the Designated Recipient identified by PSE pursuant to and in accordance with the written notice provided by PSE pursuant to Section 4.1; and

(b) Securely transfer the Shared Information in accordance with Applicable Law and via a data transfer mechanism approved by PSE.

4.3. Secure Receipt. When Supplier receives Shared Information pursuant to this Section 4, Supplier shall:

(a) Use commercially reasonable efforts to securely receive the Shared Information from the Designated Representative identified by PSE pursuant to and in accordance with the written notice provided by PSE pursuant to Section 4.1;

(b) Securely store the Shared Information in accordance with Applicable Law and as approved by the Parties;

(c) Treat the Shared Information received from the Designated Representative as: (i) information, data and materials provided to Supplier directly from PSE under the Agreement; and (ii) PSE Confidential Information under this Security Addendum; and

(d) Use the PSE Confidential Information solely as authorized by PSE in writing, including in this Security Addendum, the MSA, and in all applicable Statements of Work, and solely for purposes of performing its obligations under these agreements.

4.4. Cessation. PSE may direct Supplier to cease transferring or receiving Shared Information pursuant to this Section 4, at any time and in its sole discretion, by providing written notice to Supplier. Upon Supplier's receipt of such written notice, Supplier shall immediately cease transferring or receiving Shared Information pursuant to this Section 4, as

applicable, and destroy such information pursuant to Section 1.1(c)(xii) above unless otherwise directed by PSE.

5. Cost

There shall be no additional cost to PSE for Supplier's performance of its obligations under this Security Addendum.

6. Miscellaneous

6.1. Subcontracting. Supplier will not subcontract or delegate the Processing of PSE Confidential Information or the performance of its obligations under this Security Addendum without the prior written consent of PSE. For purposes of clarity, PSE may authorize Supplier's subcontracting of Services under the MSA or a Statement of Work, however the subcontracting of any of the obligations specified under this Security Addendum requires additional specific written authorization by PSE. Supplier will remain fully responsible for fulfillment of its obligations under this Security Addendum and will remain the primary point of contact regarding any Processing of PSE Confidential Information or the performance of any of its obligations under this Security Addendum that have been subcontracted or delegated.

6.2. Representation and Warranties. Supplier represents and warrants the following:

(a) it has the full power and authority to enter into this Security Addendum and to perform its obligations under this Security Addendum;

(b) Supplier is not aware of any previous Security Breaches or, if a Security Breach has occurred, Supplier has disclosed in writing each such Security Breach to PSE and remedied all related security vulnerabilities and taken appropriate measures to prevent similar Security Breaches from occurring again;

(c) Supplier is not, and has not been, a party to any current, pending, threatened or resolved enforcement action of any government agency, or any consent decree or settlement with any governmental agency or private person or entity, regarding any Security Breach or otherwise regarding privacy or information security, or if it has been a party to any such enforcement actions, consent decrees or settlements, it has disclosed in writing all such enforcement actions, consent decrees or settlements to PSE and taken appropriate measures to comply with any requirements imposed in connection therewith;

(d) Supplier's Information Security Program complies with Applicable Law; and

(e) Supplier is and will remain in compliance with all Applicable Law and will not, by an act or omission, place PSE in breach of such laws.

6.3. Indemnification. Supplier will indemnify, defend and hold harmless PSE and its parent, subsidiaries, affiliates, agents and suppliers, and their respective officers, directors, shareholders and personnel, from and against any claims, suits, hearings, actions, damages, liabilities, fines, penalties, costs, losses, judgments or expenses (including reasonable attorneys' fees) arising out of or relating to its failure to comply with this Security Addendum.

6.4. Breach of Obligations. If Supplier can no longer meet its obligations under this Security Addendum, it will immediately notify PSE in writing. Supplier will take reasonable and appropriate steps to stop and remediate, and will cooperate with PSE's reasonable requests regarding, any unauthorized Processing of PSE Confidential Information by

Supplier or Service Provider. A breach of any provision of this Security Addendum may result in irreparable harm to PSE, for which monetary damages may not provide a sufficient remedy, and therefore, PSE may seek both monetary damages and equitable relief. Monetary damages for breach of the obligations in this Security Addendum are not subject to any limitation of liability provision in the MSA. In the event Supplier breaches any of its obligations under this Security Addendum, PSE will have the right to terminate the Agreement or suspend Supplier's continued Processing of any PSE Confidential Information, without penalty, immediately upon written notice to Supplier.

Intending to be legally bound, PSE and Supplier have caused their duly authorized representatives to execute this Security Addendum in the space provided below.

PSE:	**Supplier**:
Puget Sound Energy, Inc.	_____
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____