CenturyLink Information Security and Privacy Requirements Appendix

This Information Security and Privacy Requirements Appendix ("Appendix") governs whenever a Supplier Processes or has physical or logical access to CenturyLink Confidential Information or facilities and has access to a CenturyLink Information System. If any terms in this Appendix conflict with the terms of any Contract Document between the parties, the provisions providing the greatest protections to Confidential Information will prevail. Capitalized terms used, but not defined in this Appendix will have the same meanings as in the Contract Document.

Definitions

Affiliate, if not defined in the Contract Document, with respect to either party, shall mean any entity that is directly or indirectly in control of, controlled by, or under common control with such party whether now existing, or subsequently created or acquired during the Term of the Contract Document.

Critical Infrastructure Information (CII), is defined as Confidential Information about CenturyLink's network architecture and key network assets, such as the location and capability of central offices, network points of presence and other critical network sites, and network elements and equipment within them, and includes any information which CenturyLink identifies as critical infrastructure information.

Confidential Information, includes CenturyLink Critical Infrastructure Information (CII), Customer Proprietary Network Information (CPNI), Personally Identifiable Information (PII), information defined as confidential in a CenturyLink-customer contract, *Sensitive Confidential Information,* and any other sensitive, proprietary or legally-protected data that is owned, controlled, or Processed by CenturyLink.

Contract Document, as used in this Appendix, means the relevant contract, agreement, statement of work, task order or purchase order governing the provision of services and/or deliverables by Supplier to CenturyLink.

CenturyLink, means the CenturyLink, Inc., its Affiliates and operating units.

CenturyLink Information System(s), means any networks, applications, computers, hardware and/or Mobile Devices managed by CenturyLink, which includes laptops and network devices.

Customer Proprietary Network Information (CPNI), is as defined at 47 USC § 222(h) and includes any Confidential Information which CenturyLink identifies as CPNI. Customer proprietary information, including CPNI, is protected by federal statute (47 USC § 222) and Federal Communications Commission Rules.

Highly Privileged Accounts, or HPAs, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

Mobile Devices, means tablets and smartphones running mobile operating systems (e.g., iOS, Blackberry OS, Android, or Windows Mobile operating systems).

Personally Identifiable Information (PII), is Confidential Information that may be used to identify an individual or entity, whether the information pertains to consumer, business or employment

activities, such as a first and last name, home or other physical address, phone number or other contact information, e-mail address and electronic transaction information; as such relation is defined under applicable law or regulation. PII also includes any information relating to an identified or identifiable natural person, and an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Process or Processing, means to perform any operation or set of operations upon data (including but not limited to CenturyLink Confidential Information), whether or not by automatic means, including, but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

Security Incident, is any actual or suspected event in which CenturyLink Confidential Information is or may have been lost, stolen, improperly altered, improperly destroyed, improperly disclosed, used for a purpose not permitted under the Contract Document or this Appendix, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Appendix.

Security Notices, are any written communications, notices, filings, press releases, or reports related to any Security Incident.

Security Standards, means commercially reasonable security features in all material hardware and software systems and platforms that Supplier uses to access, Process and/or store CenturyLink's Confidential Information, in alignment with ISO/IEC 27002:2005, as that standard or its successor standards may be amended.

Sensitive Confidential Information, means CenturyLink Confidential Information that involves racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health and financial matters, sexual preferences, Social Security Numbers, credit cards and any other account numbers, customer data, or other Confidential Information which CenturyLink identifies as Sensitive Confidential Information, whether the information pertains to consumer, business or employment activities.

Supplier, is the entity that is a party to the Contract Document and any Affiliate of such entity that Processes or has access to CenturyLink Confidential Information or has access to a CenturyLink Information System.

Supplier Information System(s), means any Supplier systems, applications, computers, network equipment, hardware and Mobile Devices used to Process CenturyLink Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

Supplier Personnel, means Supplier's employees, as well as its Affiliates, suppliers, subcontractors, and agents and their respective employees.

Security Requirements

1. To protect CenturyLink's Confidential Information from unauthorized Processing including disclosure, loss or alteration, Supplier will, at all times that it accesses, stores or Processes CenturyLink's Confidential Information: (i) meet the Security Standards (ii) review this Appendix before accepting CenturyLink's Confidential Information; and (iii) meet and continue to meet the terms of the Security Requirements section, and Additional Security

Requirements Section, as applicable, of this Appendix. Supplier will maintain written safety and facility procedures, data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of CenturyLink's Confidential Information, and such procedures will reflect best practices for information security and will include appropriate employee initial and annual training, as well as the posting of a privacy policy on Supplier's website. Supplier agrees to cooperate in good faith to modify its business practices to accommodate any future changes in the parties' hardware, software, or services, or in legal or industry standards regarding the treatment of CenturyLink Confidential Information that may affect the reasonableness or effectiveness of the protections under this Agreement.

2. Prior to providing access to any CenturyLink Confidential Information Supplier must obligate Supplier Personnel to comply with the level of security required in the Contract Document and this Appendix and verify such compliance through an appropriate due diligence process. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel with this Appendix and shall remain responsible at all times for their compliance.

3. Supplier shall undertake reasonable measures to terminate Supplier Personnel access to CenturyLink Confidential Information, whether physical or logical, no later than the date of personnel separation or personnel transfer to a role no longer requiring access to CenturyLink Confidential Information; where Supplier Personnel have been assigned CenturyLink single sign-on (SSO) credentials, Supplier must notify CenturyLink of any such separation or transfer no later than the day of that event.

4. Supplier Personnel with access to CenturyLink Confidential Information must participate in appropriate information security awareness training provided by the Supplier prior to obtaining access to CenturyLink Confidential Information and thereafter on at least an annual basis while such personnel have access to CenturyLink Confidential Information.

5. Unless prohibited by applicable law or regulation, Supplier shall notify CenturyLink promptly and act only upon CenturyLink's instruction concerning any request by a third party, including without limitation law enforcement, governmental authority, or in connection with litigation or other court process for disclosure of CenturyLink Confidential Information or for information concerning the Processing of CenturyLink Confidential Information in connection with the Contract Document or this Appendix, as well as any request received from an individual concerning his/her PII.

6. CenturyLink Confidential Information shall not be Processed on personal accounts (e.g., individual email or cloud services accounts (e.g., Gmail, Yahoo, Dropbox, Google Drive)) or on personally-owned computers, devices or media.

7. Supplier will not Process CenturyLink Confidential Information on Supplier servers or workstations beyond what is necessary to perform the Supplier business functions.

8. Supplier will securely erase CenturyLink Confidential Information from all media, using then current commercially-reasonable erasure means, before Supplier provides any third party with media on which CenturyLink Confidential Information has been Processed.

9. Supplier must receive approval from CenturyLink prior to (a) moving CenturyLink Confidential Information from its CenturyLink-approved hosting jurisdiction to a different hosting jurisdiction; or (b) provisioning remote access to such CenturyLink Confidential

Information from any location other than the CenturyLink-approved hosting jurisdiction or other CenturyLink-approved jurisdiction or (c) moving CenturyLink Confidential Information from its CenturyLink-approved physical location or jurisdiction to a different physical location or jurisdiction.

10. Supplier will not Process any CenturyLink Confidential Information at any location outside the United States or through entities that are not incorporated or organized in the United States without CenturyLink's prior written consent.

11. Encryption must be implemented in any of the following instances: (a) any computers, devices or media (e.g., laptop computers, Mobile Devices, USB drives, back-up tapes) containing CenturyLink Confidential Information must be encrypted at rest; (b) transferring CenturyLink Confidential Information over public networks (such as the Internet) or over non-US soil; and (c) CenturyLink Highly Confidential information must be encrypted at rest and in transit. Where encryption is required, Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with highly-regarded level industry practices.

12. Supplier Information Systems must have security controls that can detect and prevent attacks and must be continuously monitored. For example, network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) between the Internet and DMZ, and between DMZ and internal servers containing CenturyLink Confidential Information. IDS/IPS high and critical priority alerts must be responded to as soon as reasonably practicable but in no case more than 72 hours.

13. Any Supplier Personnel remotely accessing Supplier Information Systems must be authenticated using at least a two-factor authentication method and such transmissions must be secured using industry standard encryption.

14. Supplier must use an auditable process (e.g., certification of destruction) to remove CenturyLink Confidential Information from Supplier Information Systems prior to disposal or re-use in a manner that ensures that the CenturyLink Confidential Information may not be accessed or readable.

Additional Security Requirements
In the event Supplier will or may Process CenturyLink Sensitive Confidential Information**,** Supplier shall implement and maintain, in addition to the above Security Requirements, the following additional measures and controls:

1. Supplier must perform vulnerability assessments on Supplier Information Systems at least annually. For Supplier Information Systems that are internet facing, Supplier must engage an independent external party to perform a vulnerability assessment and shall remediate as required in Audits.

2. Supplier must have or implement hardening and configuration requirements consistent with highest level industry practices, to include testing and implementing all applicable security-related fixes, command scripts, etc. provided by operating system vendors, user associations, and other trusted third parties in a time frame appropriate with the associated risk.

3. Supplier must ensure that Supplier Information Systems are free from malicious software (malware). Antivirus software must be installed and running on all Supplier Information

Systems capable of running antivirus software, and it must be configured to automatically detect and remove harmful or malicious code. The antivirus software must be configured to update automatically and continuously to ensure the antivirus definitions will never be more than 24 hours old.

4. Supplier must have or implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of CenturyLink Confidential Information from Supplier Information Systems.

5. Supplier must implement processes to support the secure creation, modification, and deletion HPAs. Supplier must review and update access rights at least quarterly for HPAs. HPA usage logs must be continually reviewed. All HPA access must be established using encrypted mechanisms (e.g., secure shell).

6. Physical access must be monitored, recorded and controlled with physical access rights reviewed at minimum annually. Physical access logs detailing access must be stored for a period of one (1) year unless prohibited by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least thirty (30) days.

Technical Controls on Supplier Information Systems

1. Unless otherwise expressly agreed in the Contract Document, development and testing environments must not contain CenturyLink Confidential Information and shall only go "live" upon CenturyLink Information Security's review and approval, as appropriate.

2. Any back-up media containing CenturyLink Confidential Information stored at Supplier's site must be kept in a secure location (e.g., locked office or locked file cabinet) and be encrypted to a standard consistent with industry practice. If off-site media storage is used, Supplier must have a media check-in/check-out process with locked storage for transportation. Back-up information must be given the same level of physical and environmental protection as the level of control applied at the main site.

3. Network layer security devices must allow only authorized connections and rule sets must be reviewed at minimum semi-annually.

4. Mobile Devices used to Process CenturyLink Confidential Information (including emails) must have strong mobile device security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

5. Supplier will not use portable computing and storage devices such as laptops, personal digital assistants, diskettes, cell phones, USB flash drives, CDs, and portable disk drives (collectively referred to as "Mobile Devices") to Process CenturyLink Confidential Information absent a business need to perform under this Agreement. If so needed, Mobile Devices that contain CenturyLink Confidential Information will interact with or store CenturyLink Confidential Information only in an encrypted form using a strong cryptographic protocol with highly-regarded, secure protocols consistent with commercially reasonable practices in Supplier's business sector. Mobile Devices used to Process CenturyLink Confidential Information (including emails) must have strong mobile device security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

6. Any encryption required hereunder must be FIPS 140-2 certified/compliant.

Physical security controls

1. Supplier shall comply with CenturyLink's Physical Security Administration Standards available at the Supplier Portal.

Compliance

1. Supplier represents and warrants that it shall comply with all applicable laws and regulations applicable to Supplier's activities concerning CenturyLink Confidential Information governed by this Appendix.

2. If Supplier Processes any CenturyLink Confidential Information that includes PII, it shall comply with all legal obligations concerning notice and consent, onward transfer to a third party, and international transfer, and shall act only on CenturyLink's written instruction concerning any such transfers.

3. If Supplier Processes payment card information on behalf of CenturyLink, Supplier will comply with Payment Card Industry Data Security Standards (PCI-DSS), as amended or updated from time to time. Supplier will validate compliance with Payment Card Industry Data Security Standards, as needed, to permit CenturyLink to meet its compliance obligations, and will provide CenturyLink annually with a PCI-DSS compliance certificate signed by an officer of Supplier with oversight responsibility. If Supplier Processes financial account information (e.g., bank or credit union accounts), it will protect that information in accordance with the National Automated Clearing House Association's NACHA/ACH Rules and Operating Guidelines. Supplier will provide CenturyLink annually with a NACHA/ACH compliance certificate, signed by an officer of Supplier with oversight responsibility.

4. If Supplier Processes any CenturyLink Confidential Information that includes PHI, it shall comply with HIPAA and the Business Associate Agreement located at http://www.centurylink.com/aboutus/docs/Business_Associate_Agreement.pdf.

5. If Supplier Processes any CenturyLink Confidential Information that includes banking or financial information, it shall comply with the U.S. Sarbanes-Oxley Act, the U.S. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), and the Federal Financial Institutions Examination Council (FFIEC) guidance).

6. In the event there are additional legal or industry standards applicable to Supplier's Processing of CenturyLink Confidential Information, Supplier agrees to cooperate with CenturyLink to comply with such requirements. Such cooperation may include, without limitation: (a) execution of additional agreements required by applicable law or compliance standard, including, but not limited to, the EU Standard Contractual Clauses; (b) implementation of additional or revised security controls required by applicable law or compliance standard; (c) completion of regulatory filings or compliance certifications applicable to Supplier; and (d) completion of required regulatory or compliance audits.

Data Collection

1. Unless and except to the extent expressly provided in the Contract Document, Supplier must, in each case, seek and obtain CenturyLink's prior written approval regarding the scope of any PII to be collected directly by Supplier, as well as any notices to be provided and any consent language to be used when collecting such information from an individual. In the case of PII collected directly from individuals by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.

Security Incident

1. Supplier must develop and maintain an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and perform any required recovery actions to remedy the impact.

2. Security Incidents on Suppliers Information Systems must be logged, reviewed on a periodic basis (minimum quarterly), secured, and maintained for a minimum of twelve (12) months.

3. Supplier will promptly (but in no event later than 24 hours after discovery) inform CenturyLink in writing on becoming aware of any known or suspected compromises, unauthorized access, misappropriation, improperly altered or destroyed used for a purpose not permitted under the Contract Document or this Appendix or release of CenturyLink's Confidential Information.

   Supplier shall report any Security Incidents to CenturyLink's UNIcall at 1-866-864-2255 or at such contact information communicated to Supplier from time to time. In any such instance, Supplier will give specific information on what Confidential Information was accessed and any other information CenturyLink reasonably may request concerning the details of the Security Incident, as soon as such information can be collected or otherwise becomes available and any remediation efforts undertaken, to the extent known and will thereafter provide regular and timely updates throughout the ongoing investigation and remediation. (CenturyLink's Law Department will be consulted regarding the framework of any investigation, including aspects that should be covered by the attorney-client privilege.) The parties will work cooperatively to secure the return of any Confidential Information removed or copied. Unless otherwise agreed in writing by the parties at the time of the incident, the party experiencing the incident will, at its own expense, conduct an investigation of the incident and provide periodic reports to the other party on the status of the investigation. When Supplier experiences the incident, upon reasonable request of the CenturyLink, Supplier may be required to hire an independent, third party forensic or security firm to assist with this investigation or remediation effort. At the appropriate time, the party experiencing the incident will advise the other party of the final results of the investigation. Each party will work cooperatively with the other party on remediation and law enforcement activities, as appropriate.

4. Notwithstanding and excluded from any limitations in the Contract Document, Supplier shall pay for or reimburse CenturyLink or the applicable CenturyLink Affiliate for all costs associated with a Security Incident, including repeated and related losses and expenses relating to any Security Incident experienced by Supplier, including without limitation, costs of forensic assessments, Security Notices, credit monitoring or other fraud alert services, and all other remedies either required by applicable law and regulation or which are required to remediate the Security Incident and prevent similar Security Incidents in the future.

5. If requested by CenturyLink, and at CenturyLink's direction, Supplier shall send Security Notices regarding a Security Incident. Unless prohibited by applicable law or regulation, Supplier shall provide CenturyLink with reasonable notice of, and the opportunity to comment on and approve, the content of such Security Notices prior to any publication or communication thereof to any third party, except CenturyLink shall not have the right to reject any content in a Security Notice that is specifically required to comply with applicable law or regulation. Should CenturyLink elect to send a Security Notice

regarding a Security Incident, Supplier shall provide all reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.

6. Other than approved Security Notices, or to law enforcement or as otherwise required by law or regulation, Supplier may not make or permit any public statements concerning CenturyLink's involvement with any such Security Incident to any third-party without the explicit written authorization of CenturyLink's Legal Department.

Audits

1. Supplier shall monitor the effectiveness of its security program by conducting, or engaging a third party to conduct, audits and risk assessments of Supplier Information Systems against the requirements of written policies and procedures maintained as required by this Appendix no less frequently than every twelve (12) months. Supplier shall be responsible for ensuring consistency of its security operations, including proactive monitoring and mitigation of all vulnerabilities across any Supplier Information Systems used to access or Process CenturyLink Confidential Information or CenturyLink Information Systems.

2. Upon CenturyLink's request, Supplier will provide information to CenturyLink to enable CenturyLink to determine compliance with the applicable Security Requirements. As part of CenturyLink's assessment of Supplier's internal control structure, CenturyLink may require Supplier to, without limitation, answer security questionnaires or conduct scans of servers, databases and other network hardware, and submit an attestation by an officer of Supplier with knowledge of Supplier's compliance.

3. Upon request, Supplier must provide to CenturyLink reports of any audits and assessments conducted on Supplier Information Systems, which reports shall include, at a minimum, the scope of the audit and/or assessment and any vulnerabilities, issues, findings, concerns, and/or recommendations in so far as they impact CenturyLink Confidential Information. Such reports provided by Supplier to CenturyLink shall be treated as confidential.

4. Supplier must remediate within thirty (30) days, or as soon as reasonably practicable thereafter, any items rated as high or critical (or similar rating indicating similar risk) in any audits or assessments of Supplier Information Systems. CenturyLink reserves the right to request remediation to be completed in less than 30 days, implementation of a compensating control, or suspension of further activity where necessary to adequately protect CenturyLink Confidential Information.

5. Upon request, with reasonable advance notice and conducted in such a manner not to unduly interfere with Supplier's operations, CenturyLink reserves the right to conduct, or to engage third parties to conduct, an audit of Supplier's compliance with the requirements in this Appendix relating to CenturyLink Confidential Information including but not limited to: (a) a review of Supplier's applicable policies, processes, and procedures, (b) a review of the results of Supplier's most recent vulnerability assessment (e.g., application vulnerability scanning, penetration testing, and similar testing results) and accompanying remediation plans, and (c) on-site assessments of Supplier's physical security arrangements and Supplier Information Systems during Supplier's regular working hours pursuant to a mutually agreeable audit plan. CenturyLink reserves the right to conduct an onsite audit of Supplier on thirty (30) days prior written notice during regular business hours. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes CenturyLink Confidential Information provided under the Contract Document. Supplier agrees to cooperate fully with CenturyLink or its designee during such audits and shall provide access to facilities, appropriate resources provide applicable supporting documentation to CenturyLink, and complete security assessment questionnaires that may be requested.

6. If CenturyLink has a reasonable basis to believe that Supplier has breached or is likely to breach the terms of this Appendix, CenturyLink may, upon 5 days' notice, perform a vulnerability assessment, which assessment will be in addition to any assessment in the ordinary course. At CenturyLink's reasonable request, Supplier will promptly cooperate with CenturyLink to develop a plan to protect CenturyLink's Confidential Information from any applicable failures or attacks, which plan will include prioritization of recovery efforts, identification of and implementation plans for alternative data centers or other storage sites and backup capabilities.

Material Breach

1. Notwithstanding anything to the contrary herein or in the Contract Document, Supplier's (including Supplier Personnel) failure to comply with the obligations set forth in this Appendix also constitutes a material breach of the Contract Document, with such rights and remedies set forth therein or under applicable law and regulation.

2. CenturyLink or the applicable CenturyLink Affiliate owning any of the CenturyLink Confidential Information being accessed pursuant to the Contract Document may enforce the terms of this Appendix as permitted or required by applicable law and regulation.

Miscellaneous

1. Supplier understands and agrees that CenturyLink or its Affiliates may require Supplier to provide certain personal information such as the name, address, telephone number, and e-mail address of Supplier's representatives in transactions to facilitate the performance of the Contract Document, and that CenturyLink, its Affiliates, and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. CenturyLink or the applicable CenturyLink Affiliate will be the controller of this data for legal purposes and agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws. Supplier

may obtain a copy of the Supplier personal information by written request or submit updates and corrections by written notice to CenturyLink.

Background Screening

1. Supplier will comply with CenturyLink's Drug Testing and Background Check Requirements available at the supplier portal.