CenturyLink Information Security and Privacy Requirements

If these CenturyLink Information Security and Privacy Requirements ("Requirements") conflict with the terms of any Agreement between the parties, the provisions providing the greatest protections to Confidential Information will prevail. Capitalized terms used, but not defined in these Requirements will have the same meanings as in the Agreement. If the Agreement does not include definitions of CII, CPNI, PII, Sensitive PII, Security, or Supplier Portal Standards, the following applies:

1. **Definitions.** Company's Confidential Information may include Company critical infrastructure information (CII), customer proprietary network information (CPNI) or customer or employee personally-identifiable information (PII). CII is defined as Confidential Information about Company'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 Company identifies as critical infrastructure information. CPNI is as defined at 47 USC § 222(h) and includes any Confidential Information which Company identifies as CPNI. Customer proprietary information, including CPNI, is protected by federal statute (47 USC § 222) and Federal Communications Commission Rules. PII is Confidential Information that may be used to identify an individual or entity, 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. "Sensitive PII" means Company 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, or other Confidential Information which Company identifies as Sensitive PII, whether the information pertains to consumer, business or employment activities. Company will identify Company CII, CPNI, PII, or Sensitive PII if reasonably requested by Supplier in writing.

   "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 Company's Confidential Information, including ISO/IEC 27002:2005, as that standard or its successor standards may be amended.

   "Supplier Portal" means the following URL or such other URL as Company designates from time to time: http://www.centurylink.com/Pages/AboutUs/CompanyInformation/DoingBusiness

2. To protect Company's Confidential Information from unauthorized use, including disclosure, loss or alteration, Supplier will, at all times that it accesses, stores or processes Company's Confidential Information: (i) meet the Security Standards; and (ii) inventory and review Security Standards before accepting Company's Confidential Information. Supplier will maintain written safety and facility procedures, data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of Company's Confidential Information, and such procedures will reflect best practices within Supplier's industry and will include appropriate employee 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 Company Confidential Information that may affect the reasonableness of the protections under this Agreement.

3. If Supplier stores, processes, or transmits payment card information on behalf of Company, Supplier will comply with Payment Card Industry Data Security Standards, including PCI-DSS version 2.0 standards, as amended or updated from time to time. Supplier will validate compliance with Payment Card Industry Data Security Standards, as needed, to permit Company to meet its compliance obligations, and will provide Company annually with a PCI-DSS compliance certificate signed by an officer of Supplier with oversight responsibility. If Supplier stores or processes Customer 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 Company annually with a NACHA/ACH compliance certificate, signed by an officer of Supplier with oversight responsibility.
4. Upon Company's reasonable request, Supplier will provide information to Company to enable Company to determine compliance with these Requirements. As part of Company's assessment of Supplier's internal control structure, Company may require Supplier to, without limitation, answer security questionnaires or conduct scans of servers, databases and other network hardware. If Supplier accesses, stores or processes Company Confidential Information, Company reserves the right to require that an annual audit be conducted with respect to Supplier's compliance. Upon Company's request, the audit will include a data-flow chart or narrative. Supplier will provide Company with the results of any audit, upon Company's written request. Regardless of any Company request, however, Supplier will advise Company of any material negative finding

or conclusion of the audit and the corrective or remediation steps being taken to address such negative finding or conclusion.

5. Supplier will promptly (but in no event later than 24 hours after discovery) inform Company in writing on becoming aware of any known or suspected compromises, unauthorized access, misappropriation, misuse or release of Company's Confidential Information. In any such instance, Supplier will give specific information on what Confidential Information was accessed and any remediation efforts undertaken. The parties will work cooperatively to secure the return of any Confidential Information removed or copied. Company's Law Department must be consulted regarding the framework of any investigation, including aspects that should be covered by the attorney-client privilege. 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. 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. In the event of the unauthorized disclosure or use of CPNI or PII, Supplier's indemnity obligation in this Agreement will include repeated or related expenses arising from each disclosure and use, including, but not limited to, advertising, notifications, and services (such as the cost of credit monitoring).

6. On a periodic basis, but in no event more than twice in any 12-month period, Company may, upon 10 days' notice, perform a security assessment (on any system that transmits, collects, processes, or stores (including caching) its Confidential Information) to determine Supplier's compliance with the Security Standards. If Company has a reasonable basis to believe that Supplier has breached or is likely to breach the Security Standards, Company may, upon 5 days' notice, perform a vulnerability assessment, which assessment will be in addition to any assessment in the ordinary course.

7. At Company's reasonable request, Supplier will promptly cooperate with Company to develop a plan to protect Company's Confidential Information from failures or attacks on the Security Standards, which plan will include prioritization of recovery efforts, identification of and implementation plans for alternative data centers or other storage sites and backup capabilities.

8. Supplier will not store Company Data on Supplier servers or workstations beyond what is necessary to perform the Supplier business functions. 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") with respect to Company Confidential Information absent a business need to perform under this Agreement. If so needed, Mobile Devices that contain Company Confidential Information will interact with or store Company 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. Supplier will securely erase Company Confidential Information from all media, using current commercially-reasonable erasure means, before Supplier provides any third party with media on which Company Confidential Information has been captured or stored.

9. In the event Company Confidential Information will be transmitted (i) over non-US soil, or (ii) over the public Internet, the Confidential Information must be encrypted using highly-regarded, secure transport encryption protocols, consistent with commercially reasonable practices in the delivery of services within Supplier's business sector. Supplier will not access from, transfer or disclose to or use any of Company's CPNI, PII, or CII at any location outside the United States or entities that are not incorporated or organized in the United States without Company's prior written consent.

10. Background Screening. Supplier will comply with Company's Drug Testing and Background Check Requirements available at the Supplier Portal.