CenturyLink Non-Disclosure Agreement Information Security and Privacy Requirements

If these CenturyLink Non-Disclosure Agreement 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.

1. **Definitions.** CenturyLink's Confidential Information may include CenturyLink critical infrastructure information (CII), customer proprietary network information (CPNI) or customer or employee personally-identifiable information (PII). 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. 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. 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 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 CenturyLink identifies as Sensitive PII, whether the information pertains to consumer, business or employment activities. CenturyLink will identify CenturyLink 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 a Party uses to access, process and/or store the other Party's Confidential Information, in alignment with 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 CenturyLink designates from time to time:
   http://www.centurylink.com/Pages/AboutUs/CompanyInformation/DoingBusiness

2. To protect a Party's Confidential Information from unauthorized use, including disclosure, loss or alteration, the other Party will, at all times that it accesses, stores or processes Confidential Information: (i) meet the Security Standards; and (ii) inventory and review Security Standards before accepting Confidential Information. Each Party will maintain written safety and facility procedures, data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of Confidential Information, and such procedures will reflect best practices within that Party's industry and will include appropriate employee training, as well as the posting of a privacy policy on its website.

3. If Supplier stores, processes, or transmits payment card information on behalf of, CenturyLink it 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, 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.

4. Upon a Party's reasonable request, the other Party will provide information to enable the Party to determine compliance with these Requirements.

5. Each Party will promptly (but in no event later than 24 hours after discovery) inform the other Party in writing on becoming aware of any known or suspected compromises, unauthorized access, misappropriation, misuse or release of Confidential Information. In any such instance, the Party will give specific information on what Confidential Information was accessed and any remediation efforts undertaken, to the extent known and will thereafter provide regular and timely updates throughout the ongoing investigation and remediation. The Parties will work cooperatively to secure the return of any Confidential Information removed or copied. The other Party'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. 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.

6. Neither Party will store Confidential Information on servers or workstations beyond what is necessary to perform the Party's business functions. Neither Party will 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 Confidential Information absent a business need to perform under this Agreement. If so needed, Mobile Devices that contain Confidential Information will interact with or store Confidential Information only in an encrypted form using a strong cryptographic protocol with highly-regarded, secure protocols consistent with commercially-reasonable practices in the Party's business sector. Each Party will securely erase Confidential Information from all media, using current commercially-reasonable erasure means, before provided to any third party with media on which Confidential Information has been captured or stored.

7. In the event 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 CenturyLink'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 CenturyLink's prior written consent.

8. Background Screening. Both Parties will comply with the Drug Testing and Background Check Requirements available at the Supplier Portal.