Qwest Non-Disclosure Agreement Information Security and Privacy Requirements

If these Qwest Non-Disclosure Agreement Information Security and Privacy 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. **Required Safeguards and Procedures.** The Parties will maintain administrative, technical and physical safeguards at the network, system, server, database, workstation and application level to protect the security, availability, confidentiality, and integrity of Confidential Information ("Required Safeguards"), and will maintain written safety and facility procedures, data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of Confidential Information ("Required Procedures"). Required Safeguards and Required Procedures will reflect best practices within each Party's industry and will include appropriate employee training, as well as the posting of a Privacy Policy on the Party's website.

2. **Critical Infrastructure, Customer Proprietary Network Information (CPNI) and Personally-Identifiable Information.**

    a. **Definitions.** Qwest's Confidential Information may include Qwest critical infrastructure information (CII), customer proprietary network information (CPNI) or customer or employee personally-identifiable information (PII). CII is defined as Confidential Information about Qwest'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 Qwest identifies as critical infrastructure information. CPNI is as defined at 47 USC § 222(h) and includes any Confidential Information which Qwest 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 Qwest identifies as Sensitive PII, whether the information pertains to consumer, business or employment activities. Qwest will identify Qwest CII, CPNI, PII, or Sensitive PII if reasonably requested by Supplier in writing.

3. **Data Storage.** The Parties will not store Confidential Information on servers or workstations beyond what is necessary to perform the obligations or as otherwise permitted under the Agreement.

4. **Mobile Devices.** 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 the Agreement. If so needed, laptops that contain Confidential Information shall interact with or store it 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.

5. **International Access.** In the event Qwest 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 Qwest's CPNI, Sensitive PII, or CII at any location outside the United States or entities that are not incorporated or organized in the United States without Qwest's prior written consent.

6. **Security Incidents.**

a. The Receiving Party will notify the Disclosing Party of any breach of this Agreement or unauthorized disclosure of the Confidential Information ("Security Incident") as soon as reasonably possible, but no later than 24 hours from the date of discovery. This notice will include specific information on what Confidential Information was accessed and any remediation efforts undertaken. Qwest must be notified at its UNIcall service number 1- 866-864-2255, and following the prompts to Qwest employee and cyber events.

b. If a Security Incident is confirmed, the Parties will work cooperatively to secure the return of any Confidential Information removed or copied. Qwest's Risk Management and Law Department must be consulted regarding the framework of any investigation, including aspects that should be covered by the attorney-client privilege.

c. Unless otherwise agreed in writing by the parties at the time of the Security Incident, the Party experiencing the Security 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 Security 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.

7. **Payment Card Information.** If either Party stores and/or processes customer payment card information, it must protect that information in accordance with the PCI Security Standards Council's Payment Card Industry Data Security Standard (PCI-DSS).

8. **Financial Account Information.** If either Party stores and/or processes customer financial account information (i.e., bank or credit union accounts) must protect that information in accordance with the National Automated Clearing House Association's NACHA/ACH Rules and Operating Guidelines.

9. **Background Screening.** Both parties will utilize thorough screening and selection of all Personnel assigned to perform services utilizing confidential information, including appropriate background screening. The screening procedure will include:

a. An inquiry of official government record repositories for any federal, state, and local felony or misdemeanor adjudication (e.g., conviction, deferred judgment, nolo contendere or finding of criminal liability by a court of competent jurisdiction) and/or pending dispositions for all areas of residence/employment over the last seven (7) years.

b. Both parties will consider all of the information provided from a background check when determining if the Personnel will handle or have access to confidential information. Either party will not utilize any Personnel whose background screening indicates that the person has a material history of adverse credit, criminal adjudication as described above, or if the party has any information which suggests that such person is unqualified, dishonest, untrustworthy, unreliable, or has any history of violence.

c. If Personnel are based outside of the U.S. and such or criminal checks are not available or applicable within the party's country of operation, either party will notify the other party of this fact and make every effort to utilize Personnel who could reasonably meet these standards. These efforts should include alternative screening to include verification of previous employment and education.

10. **Media**. Each Party will securely erase Confidential Information subject to this Agreement from all media, using current commercially-reasonable erasure means, before Supplier provides any third party with media on which such Confidential Information has been captured or stored.