

Qwest Supplier Privacy Requirements

If these 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 Privacy Requirements will have the same meanings as in the Agreement.

1. **Required Safeguards and Procedures.** Supplier will develop, implement and maintain administrative, technical and physical safeguards at the network, system, server, database, work station and application level to protect the security, availability, confidentiality, and integrity of the Qwest's Confidential Information ("Required Safeguards"). Supplier will also establish and maintain written safety and facility procedures, data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of Qwest's Confidential Information ("Required Procedures"). Required Safeguards and Required 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. Upon Qwest's reasonable written request, Qwest may review Supplier's Required Procedures and Required Safeguards.
2. **Updates.** Supplier agrees to cooperate in good faith to modify its business practices to accommodate any future changes in the Parties hardware or software, or in legal or industry standards regarding the treatment of Confidential Information, that may affect the reasonableness of the protections under the Agreement or these Privacy Requirements.
3. **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 Qwest 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.
 - b. **CPNI Training.** If Supplier has access to Qwest CPNI, Qwest will provide Supplier with instruction and training material about CPNI rules and Qwest's practices and policies pertaining to CPNI. Supplier must provide training to all of its employees, contractors and agents who have access to this information to ensure compliance with the CPNI Rules and Qwest's practices and policies pertaining to CPNI. This training will be given annually and, for new hires, as soon as reasonably practicable after hire.
4. **Data Storage.** Supplier will not store Qwest Data on Supplier servers or workstations beyond what is necessary to perform the Supplier business functions.
5. **Security Testing.** Qwest reserves the right to perform security testing on any system that transmits, collects, processes, or stores (including caching), its Confidential Information. Qwest will cooperate to establish dates and times for testing, with a goal of avoiding any significant effect to Supplier's production systems or cycles.

6. **Mobile Devices.** 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 Qwest Confidential Information absent a business need to perform under the Agreement. If so needed, Mobile Devices that contain Qwest Confidential Information shall interact with or store Qwest 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.
7. **Audits of Required Safeguards and Procedures.** Qwest reserves the right to require that an annual audit be conducted with respect to the Required Safeguards and Required Procedures. Upon Qwest's request, the audit will include a data-flow chart or narrative. Supplier will provide Qwest with the results of any audit, upon Qwest's written request. Regardless of any Qwest request, however, Supplier will advise Qwest 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.
8. **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. If a dedicated network connection between Qwest and Supplier is used (i.e., a dedicated circuit or Virtual Private Network), Qwest will provide the technical specifications required for the transmission of such information. 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 to any persons who are not citizens of the United States or entities that are not incorporated or organized in the United States without Qwest's prior written consent.
9. **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.
 - d. In the event of the unauthorized disclosure or use of CPNI or PII, Supplier's indemnity obligation in the 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).
10. **Payment Card Information.** Suppliers that store and/or process Qwest customer payment card information must protect that information in accordance with the PCI Security Standards Council's Payment Card Industry Data Security Standard (PCI-DSS). Supplier will provide Qwest annually with a PCI-DSS compliance certificate, signed by an officer of Supplier with oversight responsibility.
11. **Financial Account Information.** Suppliers that store and/or process Qwest 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. Supplier will provide Qwest annually with a NACHA/ACH compliance certificate, signed by an officer of Supplier with oversight responsibility.

12. **Background Screening.** Supplier will utilize thorough screening and selection of its employees, including appropriate background screening. If Supplier has access to CII, CPNI or Sensitive PII, the screening procedure will include credit and felony checks for the last 3 years. Supplier will not utilize any Supplier Personnel who fail to satisfy the screening requirements. Supplier must maintain security/criminal investigation results for review by Qwest upon request. Details of actual results will remain confidential.
13. **Media.** Supplier will securely erase Qwest Confidential Information from all media, using current commercially-reasonable erasure means, before Supplier provides any third party with media on which Qwest Confidential Information has been captured or stored.