

CUSTOMER PROPRIETARY NETWORK INFORMATION COMPLIANCE POLICY

- I. **CPNI Protections.** As a customer of SandyNet, you have the right, and we have a duty under federal law, to protect the confidentiality of certain types of telecommunications data, including:
 - A. Information about the quality, technical, configuration, type, destination, location and amount of your use of telecommunications service
 - B. Information contained on your telephone bill concerns the services that you receive

This information is known as “Customer Proprietary Network Information (CPNI). CPNI does not include your name, address, or telephone number.
- II. **Customer Authentication.** Federal privacy rules require SandyNet to authenticate the identity of its customer’s prior to accessing account information housing CPNI. SandyNet representatives will use three methods to conduct customer authentication:
 - A. Customer account number
 - B. Serial or FSAN number on their ONT device
 - C. CPNI PIN number
- III. **Notifications of Certain Account Changes.** SandyNet will notify the account holder by email address when changes are made to their account for security purposes.
- IV. **Disclosure of CPNI.** SandyNet may disclose CPNI in the following circumstances:
 - A. When disclosure is required by law or court order
 - B. To protect the rights and property of SandyNet or to protect Customer with troubles associated with their services
 - C. To bill the Customer for services
- V. Protected CPNI. Violation of the SandyNet CPNI Policy by any employee will result in disciplinary action against that employee as set-forth in SandyNet’s CPNI Policy Employee Manual.
- VI. **Breach of CPNI Privacy.** Federal rules require SandyNet to report such breaches to law enforcement. Specifically, SandyNet will notify law enforcement no later than seven business days after a reasonable determination that such a breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service and the FBI. A link to the reporting facility can be found at: <https://www.cpnireporting.gov>. SandyNet cannot inform its Customers of the CPNI breach until at least seven days after notification has been sent to law enforcement, unless the law enforcement agent tells the carrier to postpone disclosure pending investigation. Additionally, SandyNet is required to maintain records of any discovered breaches, the date that SandyNet discovered the breach, the date carriers notified law enforcement and copies of the notification to law enforcement, a detailed description of the CPNI breach, including the circumstances of the breach, and law enforcement’s response (if any) to the reported breach. SandyNet will retain those records for a period of no less than two years.
- VII. **Notification of Changes to this Policy.** The City of Sandy reserves the right to modify this SandyNet Customer Proprietary Network Information (CPNI) Compliance Policy at

any time. We will notify you of any material changes via written, electronic, or other means permitted by law, including by posting it on the City of Sandy website. Our desire is to keep you updated as to what information we collected, how we use it, and under what circumstances, if any, we disclose it. If you find the changes unacceptable, you have the right to cancel the Services. If you continue to use the Services after receiving notice of such changes to this CPNI Policy, you shall be deemed to have given your consent to the changes in the revised policy.