CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) POLICY

CPNI PROTECTIONS

In compliance with section 222 of the amended Communications Act of 1934 (Act), XAirNet Corp. is committed to protecting Customer Proprietary Network Information (CPNI) entrusted to us. We recognize that CPNI is personal and sensitive information that our customers provide us when using our services, and we take our responsibility to protect it very seriously.

To ensure that we meet our legal obligations and adequately protect our customers' CPNI, we have implemented the following procedures:

Access Control: We have restricted access to CPNI only to those employees who require access to perform their job functions. Access is granted based on an employee's job function and need to know. This means that only authorized personnel can access CPNI, and they can only access it to perform their job functions. By restricting access to CPNI we are reducing the likelihood of unauthorized access, disclosure, or misuse of this confidential information.

Employee Training: All our employees who have access to CPNI receive regular training on our CPNI protection policies and procedures. This training includes education on how to protect CPNI, detect potential threats, and report any violations of our security policies. Regular training is essential to ensure that our employees are aware of the latest security practices and are equipped to handle any possible security threats to our customers' CPNI.

Security Measures: We have implemented a variety of physical, technical, and administrative security measures to protect CPNI. Physical security measures include access controls to our facilities, such as ID card access, security cameras, and locks. Technical security measures include firewalls, intrusion detection systems, and encryption technologies. Administrative security measures include policies and procedures governing how CPNI is managed, accessed, and shared. All these security measures are designed to protect CPNI against unauthorized access, disclosure, or misuse.

We authenticate the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact or in-office visit. We shall disclose CPNI to a customer in person at our office location only when the customer presents a valid photo ID, and such ID matches the name on the account. If the request is made by a customer-initiated telephone call, our company representative will only release the requested CPNI after the customer provides the biographical data or account data on file.

Third-Party Authorization: Whenever we share CPNI with third parties, we obtain express authorization from our customer and only share the information necessary to fulfill the services requested. We also ensure that any third party with whom we share CPNI has data protection policies and procedures like ours.

Documentation and Reporting: We document all complaints received about unauthorized disclosure of CPNI and take steps to remedy any issues. Additionally, we submit an annual certification to the Commission documenting our compliance with CPNI rules, as well as any actions taken against data brokers.

Breach of CPNI Privacy: In the event XAirNet Corp. experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require us to report such breaches to law enforcement and/or regulatory authorities. We will notify law enforcement no later than seven (7) business days after a reasonable determination that such breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. A link to the reporting facility can be found at: https://www.cpnireporting.gov. We cannot inform its customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, unless the law enforcement agent tells the carrier to postpone disclosure pending investigation. We maintain for at least two years a record of any discovered breaches, the date of discovery, the date carriers notified law enforcement and copies of the notifications 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.

Customer Approval: As a customer of XAirNet Corp., you have the right to approve or restrict our use of your CPNI to let you know about communications-related services other than those to which you currently subscribe and that we believe may be of interest to you. **IF YOU APPROVE, YOU DO NOT HAVE TO TAKE ANY ACTION.** However, YOU MAY DENY OR WITHDRAW OUR RIGHT TO USE YOUR CPNI FOR MARKETING PURPOSES AT ANY TIME BY SENDING AN EMAIL TO info@xsn.net or by mail at 525 Ave. Jose A. Cedeño Arecibo PR, 00612. Denying or restricting approval for us to use your CPNI for marketing purposes (also known as "opting out") will not affect any of our services to which you subscribe. Any denial or restriction of your approval remains valid until your services are discontinued or you affirmatively revoke or limit such approval or denial.

Notification of Changes to this Policy: It is our policy to post any changes we make to our privacy policy on our website. If we make material changes to how we treat CPNI, we will notify you by email to the primary email address specified in your account and/or through a notice on the Website home page. You are responsible for ensuring that we have an active and deliverable email address from you. Periodically visiting our website and our privacy policy to check for any changes.

By implementing these procedures, we are ensuring that we meet our legal obligations and adequately protect our customers' CPNI. We take the protection of our customers' confidential personal information very seriously and will continue to improve our security policies and procedures to maintain the highest standards of CPNI protection.

To ask questions or comment about this privacy policy and our privacy practices, contact us at: *info@xsn.net.*