System Security

White Paper

September, 2017

towerstream®

Towerstream Security

Towerstream safeguards against physical and logical security violations in multiple ways from our corporate backbone to our Points of Presence. We prevent all unauthorized access to our equipment as well as all Towerstream locations. Access is described below based on the type of premise that we house our equipment in.

Towerstream POP Physical Security Considerations

High Rise Buildings: Many facilities are located on prominent high-rise buildings. (e.g. Empire State Building, AON, Willis Tower, Prudential, Hancock, etc.). These facilities control access to the rooftop space and equipment with an authorized Towerstream access list as well as electronic key cards, security logins and sometimes security escorts. Equipment racks are located in a locked room or other secured space. Equipment cabinet doors are securely locked when not being worked on by a Towerstream representative.

Tower Facilities: Several Towerstream sites are located at remote tower sites. These sites are secured by gated access roads and locked fences surrounding the tower and shelter. In many cases, we have our own dedicated secured room with locked cabinets inside the shelter building. Several sites have had security cameras installed. Many shelters have electronic key card access controlled by the site owner. Only authorized Towerstream employees have security clearance to access our gear.

- Several buildings and towers require union labor or a specific vendor, and all tower and antenna work is handled by the authorized vendor. This limits and controls who can access the radios and antennas. Cabinet mounted gear is in secured spaces with locked cabinets.

- It is Towerstream policy that Customer names and IP addresses are not displayed on equipment that can be viewed by Non-Towerstream employees.

Testimonials

“Last year, we moved to a new location and were not pleased with the options available to us. Our Hosted Services Provider, referred us to Towerstream. You provide a great service at a reasonable price. The bandwidth is more than adequate, the service is reliable and the price is competitive. I can’t recall having a single service interruption within the past year. In fact, I wish you provided internet service to residential homes in Miami Dade County!

~ *Josh Morris*, IT Manager, **TerraLex**

Network Security

Towerstream's routers and switches are protected by ACLs that restrict management access to just Towerstream's headquarters and Towerstream's server farm. We utilize intrusion detection monitoring that will identify any security violations to our routers and switches. In the event that a suspected security violation is detected, the traffic is analyzed to see if it is legitimate data or an attack. If there is a true security violation, we have a team of engineers to mitigate any attack. All customers are configured in their own broadcast domain isolating their traffic at layer 2 from all other customers. We keep all our devices up to date with the latest manufacturers software patches. Towerstream's corporate IT assets are cloud based. From utilizing Microsoft 365 and Azure services to our telephony, CRM, and ERP systems.

Towerstream performs routine port scans. In addition we have two 3rd party companies performing IT audits. The last mile radios are protected utilizing the manufacturers encryption techniques. AES 128 bit is the minimum supported.

The list of manufacturers and their encryption types are below:

Redline:

Over the Air Encryption:

AES-128 and AES-256 FIPS 140-2 Level 2 compliant

Radwin:

Over the Air Encryption:

AES-128
FIPS 197 certified

Siklu:

Over the Air Encryption:

AES-128 and AES-256

DragonWave:

Over the Air Encryption:

AES-256
FIPS 197 compliant

Ceragon:

Over the Air Encryption

X-509 Certificate