Northland Communications
RELIABILITY AND SECURITY STATEMENTS
Revision 06.24.25

Overview
Northland maintains equipment and services that provide highly reliable and secure services to the public. This document provides a summary of the critical measures and systems in place.

Physical Central Office and Data Center Security

Northland's data centers and central offices are located in multi-tenant buildings in downtown Syracuse and Utica, NY. Physical security measures for each location is as follows:

Syracuse: Facility access is monitored 24/7. Access to the facility is by lock and key and the room is locked at all times. Keys are only distributed to engineering level personnel. Customers and service vendors require escorted access at all times. Afterhours, the entrance to the building is protected by electronic key card access. The distribution of these access cards is also strictly controlled. Multiple security cameras are also installed on each floor of the building.

Utica: Facility access is monitored 24/7. Access to the facility is further protected by lock and key and the room is locked at all times. Keys are only distributed to engineering level personnel. Customers and service vendors require escorted access at all times. Afterhours, the entrance to the building, data center, elevators and stairwells are locked. The distribution of keys is strictly controlled. Multiple security cameras are also installed on each floor of the building.

Voice Services – Redundant Hardware and PSTN Connections

Northland Communications provides protection for its Switching Network via geo redundant central office voice switches (Metaswitch). These switches are located throughout our serving area in Utica, Syracuse, and Holland Patent. These switches are fully redundant in design and are powered by separate electrical entrances into the buildings where they are housed.

All switches have approximately 6-8 hours of back-up battery supply. For extended outages, a truck mount generator can be brought onsite before the battery supplies are exhausted. The switches are networked together and to the PSTN via redundant facilities including fiber optics and copper. Northland uses multiple voice carriers to provide redundancy for local and long distance services. Northland's switches are monitored 24x7, 365 days a year by its switch technicians, working closely with the Network Operations Center to alert them to any customer or network outages.

Internet Services - Bandwidth Reliability

Northland connects with multiple upstream providers. Northland's Internet connections are multi- homed, balanced and redundant, with separate network facilities over different carrier networks to different Tier 1 providers. Northland's core routers are fully redundant with dual power supplies and multiple hot standby controller cards in each city. Northland also maintains an inventory of replacement parts for all core and distribution network systems. All network equipment is attached to Northland's CO battery systems.

Northland's bandwidth to the Internet is continuously monitored and calculated for the short/long term. Additional connections are made to the Internet before Northland needs them.

Internet Services - Network and Server Security Statement

Northland's computing services network is protected by multiple layers of security. Individual servers and groups of servers are protected by multiple software and hardware-based firewalls. Northland manages access down to the individual file level based on user accounts stored with "one way" encrypted passwords. The administration of Northland's systems is only permitted through certain monitored and protected key systems and only via encrypted connections.

All Northland's servers, with the exception of servers provided by customers or purchased as cloud-based servers, are automatically backed up every 24 hours to archival disk storage. Finally, Northland utilizes a variety of monitoring systems that provide intrusion detection, real-time/trend observation and statistical usage information that is used to monitor, track and block activity and to collect/recover evidence during and after an attempt to breach security.

For web hosting customers that wish to provide secure communications to the Internet, Northland can optionally provide SSL (Secure Socket Layer) services. As an Internet standard, SSL encryption technology enables companies to encrypt online transactions, secure corporate Intranet and authenticate their web sites.

Internet Services - Server Network Reliability

The Northland Communications DNS Server network consists of several high-end servers designed to provide continuous service. The most critical reliability features include RAID 5 disk arrays (locally attached or though SAN), dual gigabit/meshed switching environment, dual power supplies and equipment from top grade manufacturers. Northland's servers operate continuously, usually up to 300 days or more at a time with occasional brief maintenance procedures that are scheduled at off-peak hours. All Northland's servers are automatically backed up every 24 hours to a staged disk array (for rapid recovery) and then to an archival disk. Northland's "clustered" network design permits Northland to quickly rebuild or transfer the operation of any network server to a new or existing server. This provides the minimum downtime in the worst situations.

Security and Risk Assessments

Northland performs weekly vulnerability assessments of our network, servers, and computer systems to detect any vulnerabilities. If needed, we will make changes to improve security based on the assessment results. In addition, we perform a detailed security and risk assessment annually. Every 3 years, we utilize a 3rd party vendor to provide a more detailed external assessment. Finally, we perform 3rd party penetration testing of our public facing networks every year. Based on these results, we will update and make changes to improve our security

Cloud Services Security

Northland provides Virtual Private Servers and Storage to multiple customers that share the underlying network, storage and server resources. Northland employs VMWare ESXi to "partition" server resources between customers. By design, all VMWare virtual machines are isolated from one another. From a network standpoint, each server, or group of servers for a particular customer, has a dedicated VLAN and/or separate IP address that is not shared by different customers. The storage area network (SAN) that provides disk storage to virtual servers are firewall protected and are only accessible from the VMWare environment. To ensure that these controls are in place, Northland's NMS monitors the availability of network access. Should something change, such as a human error that would put 2 different customers on the same VLAN, the affected service would be unresponsive and Northland engineering would receive a notification to correct the problem.