POINTS NORTH

Information and Data Security Statement

The security and privacy of your data is a core part of our business and is our top priority. This document is intended to provide our clients with an overview of our information security efforts.

Physical Security

All client data is housed on dedicated servers hosted by OneNeck It Solutions (OneNeck) and are located in a SSAE-16 Type 2 secure data center located a significant geographic distance from Points North offices. Prior registration and retinal scan are required to enter the facility. Access to various sections of the facility and hardware require additional security, such as pin, biometrics, etc., and is only granted to individuals who require access to perform their job duties. Servers are contained in locked cabinets with reinforced data conduits. The server room is monitored 24/7 by both security and technical personnel.

Hardware Security

Points North servers are protected from outside intrusion by an industry-standard firewall that is kept updated. OneNeck technicians monitor firewall logs and internet traffic to provide early detection of intrusion attacks to deflect all unauthorized intrusions. Points North data and database servers are not exposed to the internet and are protected against any direct intrusion attempts.

Web Server Security

TLS Data Encryption

Points North uses Transport Layer Security (TLS) technology for authentication, data encryption, and data integrity of all client data. TLS is the industry standard security protocol to encrypt sensitive information.

Operating System

Web servers are updated regularly, as security updates become available.

Websites

Websites are created using industry-standard tools and are designed to withstand hacking attempts. Multi-tier data access is used to only provide information required by the websites. Websites require user name and password access. All passwords are stored hashed.