POINTS NORTH THE POWER OF INTEGRATION SOLUTIONS

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 in Azure hosted by Microsoft and are compliant with ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2 industry standards, located a significant geographic distance from Points North offices. Microsoft follows a layered approach to physical security, including access approval at the facilities perimeter, inside the building, and on the datacenter floor. These different layers include request and approval on a need-to-access basis, well-defined access points with 24/7 security monitoring, professional security officers who have undergone rigorous training and background checks, two-factor authentication with biometrics to enter the datacenter and a full body metal detection screening before allowed onto the floor where the servers are located.

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 username and password access. All passwords are stored hashed.