Information and Data Security Statement, version 1.1.1

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Points North Management
Last Review Date: May 2022

Information and Data Security Statement

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Points North Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- **Confidentiality** – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "**need to know**" principle.
- **Integrity** – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- **Availability** – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Points North has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Points North by its stakeholders, partners, customers and other third parties.

The Points North Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

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.

Contents

Physical Security

Hardware Security

Data Management

Web Server Security

Policy

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.

Data Management

- Points North stores and disposes of sensitive data, in a manner that; reasonably safeguards the confidentiality of the data; protects against the unauthorized use or disclosure of the data; and renders the data secure or appropriately destroyed. Data entered into Points North applications must be validated where possible to ensure quality of information processed and to mitigate the impacts of web-based attacks on the systems.

Data Retention and Disposal

- The time periods for which Points North must retain customer data depends on the purpose for which it is used. Points North retains customer data as long as an account is active, as needed to provide services to the customer, or in accordance with the agreement(s) between Points North and the customer. An exemption to this policy would include if Points North is required by law to dispose of data earlier or keep data longer. Points North may retain and use customer data to comply with its legal obligations, resolve disputes, and enforce agreements.
- Except as otherwise set forth in the Points North policies, Points North also disposes of customer data when requested by customers.
- Points North maintains a sanitization process that is designed to prevent sensitive data from being exposed to unauthorized individuals. Points North hosting and service providers are responsible for ensuring the removal of data from disks allocated to Points North use before they are repurposed or destroyed.

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.

Definitions

See Appendix A: Definitions

References

- Points North Change Control Policy
- Points North Vulnerability Management Policy
- Points North Asset Management Policy
- Points North Identity and Access Management Policy
- Points North Encryption Standards and Policy

Accommodations

Temporary accommodations from certain policy provisions may be sought following the Points North Accommodation Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0.0	November 2016		Points North	Document Origination
1.0.0		July 2017	Points North	Approved and adopted
1.1.0	September 2021		Points North	Change of Server Location Reliacloud -> Azure
1.1.0		October 2021	Points North	Approved and adopted
1.1.1	May 2022	May 2022	Points North	Annual Review/Update Added Data Management Added an Introduction Section