SpryPoint
SMART SOLUTIONS FOR SMART UTILITIES
CITY OF GRAND RAPIDS
IT'S IN MINNESOTA'S NATURE
GRAND RAPIDS PUBLIC UTILITIES
Service is Our Nature
GRAND RAPIDS
IT'S IN MINNESOTA'S NATURE

Exhibit E – Security Overview

Table of Contents

1. Overview

This security document ("Exhibit") details the security policy, procedures, and technologies used to protect client data. This document applies to SpryPoint's production software-as-a-service (SaaS) offering ("The Service"), client data stored in the service, and work performed by SpryPoint implementing, maintaining, and supporting the service. SpryPoint has established a comprehensive Written Information Security Program ("WISP") which includes defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards the firm has selected to protect the information it collects, creates, uses, and maintains.

This program uses both technologies and business policies to

- Ensure the confidentiality of client's data from any unauthorized parties;
- Protect the integrity of data; and
- Maintain availability of the service by using scalable hosting with fault tolerance.

SpryPoint's security program is based on the NIST SP 800-53 standard and the concepts of Zero Trust. The program may evolve over time as the standard is revised. These evolutions will never degrade the strength of the program.

2. Personnel

2.1. Personnel Overview

2.1.1. All SpryPoint employees are subject to background screening prior to being employed, and employment agreements cover confidentiality, non-disclosure, and other key protections.

2.1.2. SpryPoint has a dedicated information security officer who is responsible for managing and continuously improving SpryPoint's security posture. The information security officer can be reached at security@sprypoint.com.

2.2. Security Awareness & Training

2.2.1. Employees receive security awareness training during their onboarding, and SpryPoint employees are subject to mandatory ongoing cybersecurity and phish awareness training on a regular basis. All employees are encouraged to attend security conferences where practicable.

2.2.2. Employees must read and adhere to the Information Security Policies and must re-certify each year.

2.3. End User Devices

Employees agree to the Asset Management Policy with regards to acceptable use. All end user devices provisioned by SpryPoint are hardened and equipped with:

- Mobile Device Management (MDM) software.
- Full Disk Encryption.
- Anti-Malware Software.
- Strong Password policies.
- Secure Password Vault.

2.4. Access Control

2.4.1. To ensure only authenticated users access data they are authorized to access, SpryPoint maintains policies and procedures regarding the following areas:

- Access Control Policy
- Business Continuity and Disaster Recovery Plan
- Cryptography Policy
- Human Resources Security Policy
- Information Security Policy
- Operations Security Policy
- Risk Management Policy
- Third-Party Management Policy
- Asset Management Policy
- Code of Conduct
- Data Management Policy
- Incident Response Plan
- Information Security RACI
- Physical Security Policy
- Secure Development Policy

2.4.2. User accounts on SpryPoint's Services use role-based security to enable least privilege authorization. Passwords on the service are protected by industry best practices, using industry-standard encryption algorithms. Access to systems can be configured to use Single-Sign-On identity providers such as Azure Active Directory, Okta, or other identity providers.

2.4.3. Where possible, services are whitelisted to specific IP ranges rather than the open internet. SpryPoint staff use VPN services to connect to SpryPoint services where appropriate.

2.4.4. Policies cover data classification and protection of classified and restricted data.

2.5. Physical Security

The SpryPoint office is alarmed with unique codes per employee, and is protected via electronic key cards & fobs. The SpryPoint office does not provide physical access to production systems from inside the office.

2.6. Monitoring

2.6.1. SpryPoint collects application and infrastructure logs to validate service uptime and operational status, to assist with troubleshooting system issues, and to protect and secure our networks and Client Data. Events are maintained for a period of at least one year.

2.6.2. Logs may include login ID, timestamps, login authorization granted or denied, number of denied login attempts, system load data such as CPU% and free memory, data changes within the system, or other relevant information and activity.

2.7. Control Assessments

SpryPoint maintains a documented risk management program that includes an annual risk assessment.

3. Data Integrity & Privacy

3.1. Data

3.1.1. The Service is provided through secure data centers operated by an ISO 27017:2015 certified third party.

3.1.2. Data is encrypted at rest and in transit.

3.1.3. Data backups are performed daily, and tests to restore the data are run regularly

3.1.4. Questions regarding data privacy may be directed to privacy@sprypoint.com.

3.2. Personally Identifiable Information (PII)

Confidential PII is compartmentalized and encrypted with unique record-level keys and an additional level of encryption.

3.3. Secure Disposal

SpryPoint policies mandate secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or defined policies.

4. Secure Application & Infrastructure Development

4.1. Least Privilege

Only authorized Personnel with a specific business purpose are allowed access to production and development environments and/or resources.

4.2. Peer Code Reviews

All code changes require a code review before allowing a merge.

4.3. Vulnerability Management

4.3.1. SpryPoint uses automated tools to check for vulnerabilities in the software and any framework dependencies.

4.3.2. Vulnerabilities are triaged and remediation timelines are managed as per a Service Level Agreement.

4.4. Configuration Management

4.4.1. SpryPoint has embraced infrastructure as code to ensure repeatability, and to streamline the application of security patches and updates. Deployment is managed via a CI/CD pipeline.

4.4.2. Infrastructure changes are documented and scheduled and contain approval chains and rollback plans.

4.5. Incident Response Procedures

SpryPoint's incident response policy includes well-defined procedures to be followed in the event of a breach or threat of any application or system associated with the accessing, processing or storage of data.

4.6. Contingency Planning

SpryPoint has a program to test and improve disaster recovery run books and business continuity plans. The security and DevOps teams perform BC/DR testing, conduct simulations, and request feedback to improve the plan.