Insperity Technology Security Statement

Revised January 2020

Insperity™
Inspiring Business Performance™

Insperity Technology Security Statement

Introduction

The purpose of this Insperity Technology Security Statement (Security Statement) is to provide the recipient with an understanding of the Information Security and Contingency Planning (InfoSec) infrastructure in place at Insperity. The information contained in this Security Statement for existing and prospective clients is for informational purposes only. This Security Statement does not and is not intended to create, add to or change any agreement between Insperity and its clients. Any binding terms, obligations, or warranties related to Insperity products and/or services shall be in the form of written agreements between Insperity and its clients. Insperity reserves the right to make changes to this Security Statement and the topics covered any time without notice to existing or prospective clients, unless otherwise stated in a written agreement.

Sub-Service Organizations

Insperity contracts with FIBERTOWN in Bryan, Texas and StreamData Centers in The Woodlands, Texas to provide hosting services. This Security Statement only addresses Insperity's InfoSec infrastructure and does not address or include descriptions of the sub-service organizations' information security and contingency planning infrastructure.

Confidentiality

All information provided in this Security Statement is to be kept confidential and may not be disclosed recipient to any third parties. However, accountants, consultants, and attorneys of the recipient may have access to this Security Statement provided that the recipient has informed such consultants of the confidential nature of this document and they are under a legal obligation to the recipient to maintain the confidentiality of this Security Statement.

Contact Information

To request copies, suggest changes, or submit corrections to this document, contact:

Insperity, Inc.
Attention: Dr. Tim Proffitt
Managing Director, Information Security
19001 Crescent Springs Drive
Kingwood, TX 77339

Managerial Controls

1.1 Information Security Staff

Insperity has a fully staffed information security team which includes security infrastructure, SOC, penetration testing, networking, Disaster Recovery, and audit. Information security staff responsibilities include prevention, monitoring, reporting, maintaining, testing, and remediation. The Senior Vice President of Innovative Technology Solutions is responsible for the InfoSec management and supervises the information security team.

1.2 Security Policies, Standards, and Maintenance

This Security Statement summarizes many of Insperity's security practices, but is not an exhaustive list of practices. Insperity has a formally documented set of security policies and guidelines. These policies have been approved and adopted by management and are published for all Insperity corporate employees to review. As part of their employment with Insperity, corporate employees must agree to comply with these policies. The security policies are reviewed on an annual basis for changes reflecting new technologies or business processes.

1.3 Security and Awareness

Insperity has several programs in place to support its policies and standards, including but not limited to, new employee orientation; regular "awareness" emails; and postings on *Inside Insperity,* the company intranet. Each employee undergoes security and awareness training at the time of hiring and annually thereafter. Annual training is a formal requirement.

1.4 Employee provisioning and termination

Insperity conducts background checks on all employees. Each position at Insperity has a specific job description and modifier that allows for the proper level of access (role-based access control -RBAC) to be granted to the employee. Formal termination procedures, which apply to all employees when their employment with Insperity ends, requires immediate disabling of the employee's access. All provisioning and de-provisioning is managed and logged in the Insperity Identity and Access Management system for quality checking and auditing processes.

Operational Controls

2.1 Physical Access Controls

Insperity uses a combination of video surveillance, electronic door badge access, keys, and security guards to secure access to its data centers and office buildings. Motion detection video is deployed in the data centers and other restricted areas, and all visitors are required to sign guest logs. It is Insperity's policy that Insperity employees and visitors wear identification badges while on the premises.

2.2 Environmental Protections

Insperity deploys several general practices for environmental controls. Dry pipe, fire extinguishers, fire alarms, smoke detectors, heat sensors, FM200 fire suppression agents, battery backup systems and diesel generators are used. Battery backup systems along with diesel generators provide uninterrupted power to the data center when power is disrupted from the normal utility service. The data centers have stored capacity of fuel on-site with contracts for emergency delivery when applicable.

2.3 Change Management

Insperity maintains a formal change control process where all changes are tested, scheduled and approved by the proper management chain. The change control system is in place to track requests, approvals, accountability and emergency break-fix. All changes to production require testing in preproduction environments or laboratories before submission into production.

2.4 Audit and log review

Insperity reviews system logs as needed. Daily, weekly and monthly reports are generated and reviewed. Logs are extracted from security, network and server systems to be retained in an enterprise security event manager (SEM). Logs shipped to the SEM are retained as long as commercially feasible with a minimum retainage of at least six months. Log entries will record individual or process ID, date, time, event description, source, destination and event data. The SEM supports after-the-fact investigations to answer forensic questions. The SEM provides alarms/alerts to Insperity of critical events and correlated actions as defined by the security team.

2.5 Risk Assessments

An Insperity enterprise risk assessment ("Review") is conducted by the Enterprise Risk Management Committee which is composed of key Insperity management. The Review analyzes and identifies Insperity's enterprise-wide risks. The Review is facilitated by the Director of Internal Audit on a regular basis and is presented to the Insperity Board of Directors. Risks are identified as well as any remediating factors that lessen risk. Key management personnel throughout the technology department are assigned to complete the Review.

2.6 Business Continuity

Insperity has multiple data centers housing computing resources. Each geographically dispersed data center running the production environment has a rating of tier 3 or tier 4 depending on the location. Redundant systems running at separate sites allow for a site impacted by fire, flood, or weather-related events to not impact services offered to customers. Redundancy is built into systems at various levels including hardware, networking infrastructure, application space, and location. Insperity maintains a comprehensive business continuity plan (BCP) that deals with critical systems, staff, priorities and recovery sites. Insperity does not use offsite tape storage. A mature backup process is in place that places data in multiple data centers for redundancy.

2.7 Incident Response Team

Insperity has assigned specific individuals to have a responsibility for the Incident response team. This formal incident response team follows a detailed process and has documented procedures for dealing with various events. The response plan addresses intruders, detection, communications, legal issues, containment strategies, and lessons learned activities. Employees are trained to report incidents to the IRT when encountered.

2.8 Compliance Efforts

Insperity must comply with several federal laws as well as industry-specific compliance efforts. These efforts require annual information security audits from outside auditing firms. Outstanding issues identified during an audit are prioritized for remediation and addressed.

Technical Controls

3.1 Network Infrastructure:

The network infrastructure for Insperity systems is an enterprise-class deployment of redundant routers, switches, firewalls and access points that are diagrammed and restricted by administrators. The overall network is designed to use isolated sub-networks between the internal, external and public-facing segments. Network Access Control (NAC) technology has been deployed to control unauthorized devices being placed on the production network. Insperity provides a secured wireless network for corporate-approved devices. Foreign devices are able to use a segmented guest network for internet-only access.

3.2 Internet and Remote Access

Insperity has multiple internet carriers to support redundancy and capacity. Ingress/egress to the internet is protected by enterprise-class, next-generation firewalls. The least access principle is utilized to design any change in the rule base maintained by the security team. The firewall infrastructure provides egress URL filtering, file blocking and antivirus for IP conversations crossing its interfaces.

VPN connections are managed by an enterprise-class VPN solution. Each VPN connection undergoes profiling and security checks before allowing a connection to its approved destination. Contractors use a separate VPN connection and are segmented from corporate users. VPN connections for contractors are firewalled to allow only explicitly defined destinations. Dial-up is not deployed in the environment and is forbidden. All VPN conversations are encrypted, regulated and closely monitored.

3.3 Information Security

The Insperity Security Strategy is generally modeled after the CIS Top 20 critical controls framework. Security infrastructure, processes and procedures are implemented and maintained to meet each objective of the framework. The security controls are frequently evaluated for gaps or advances in technology that could be addressed.

- **Inventory of Authorized and Unauthorized Devices**. Insperity uses asset discovery tools, corporate-approved images, network access controls, vulnerability assessment and auditing in order to control devices.
- **Inventory of Authorized and Unauthorized Software**. Insperity uses an enterprise software delivery mechanism, census tools, and a formal software licensing process to control software installations.
- **Secure Configurations for Hardware and Software on Workstations and Servers.** Endpoints are configured with an approved image. Each technology is secured by a crafted hardening guide. The Microsoft® GPO feature is used to both deploy and maintain security configurations on workstations and servers in the Insperity environment. Auditing activities ensure hardening settings are maintained.
- **Secure Configurations for Network Devices**. Network devices are configured according to industry-based hardening guides. 802.1x authentication is used for all networking devices and vulnerability assessment procedures highlight any misconfigurations when equipment is deployed. Insecure protocols are not used.
- **Boundary Defense**. Insperity uses enterprise-class firewalls in its boundary defenses. The enterprise firewall uses several technologies such as application-based rules, antivirus, IPS, file blocking and data leak prevention.
- **Maintenance and Monitoring of Audit Logs**. Insperity uses log collaboration and correlation for events from production systems. Security equipment, networking gear, servers, and workstations log to a central repository that allows for reporting and alerting.
- **Application Software Security**. Insperity performs periodic web application penetration testing and automated vulnerability assessments against externally facing applications.
- **Controlled Use of Administrative Privileges**. Insperity tightly controls the use of administrative privileges. Corporate assets are not deployed with users having extraordinary rights. Quarterly audit reporting is used to control any rights that were granted and not later revoked. Administrative accounts are secured in an electronic password vault.
- **Controlled Access Based On Need to Know**. Insperity uses Roles Based Access Controls (RBAC) to provision access based on the job title. A formal provisioning team is established for administering rights.
- **Vulnerability Assessment and Remediation**. Insperity uses a formal vulnerability assessment program in addition to a formal patch management program. The criticality of the findings from the assessment program are assigned by the security team and passed to the patching teams.
- **User Account Monitoring and Control**. The provisioning team uses written procedures for managing users. This process is continually audited.
- **Malware Defenses**. Several malware defenses are deployed: firewalls, IPS, IDS, on the wire and at the endpoint. Malware logs are generated and centrally collected for actions if applicable.
- **Limitation and Control of Network Ports, Protocols and Services**. Insperity uses host-based firewalls and hardening guides to limit and control network ports and services.
- **Wireless Device Control**. WPA2 enabled wireless network is required for corporate assets when utilizing wireless. Foreign devices will have “guest only” internet access available. NAC technology monitors and negates the installation of rogue access points.

- **Data Loss Prevention**. Full disk encryption is used on Insperity endpoints. In addition to encryption, Insperity used de-identification technologies for data in testing environments.
- **Incident Response Capability**. A formalized Insperity incident response team is in place to properly react to reported or discovered incidents. The team consists of core management from throughout the company.
- **Data Recovery Capability**. A formal backup program is in place. Data is replicated in a near real-time fashion to an alternate data center. This ensures that redundant copies are available in the event of a disaster. Insperity tests its disaster recovery plans between the redundant sites and that staff is properly trained to handle potential disasters.
- **Security Skills Assessment and Training**. Each employee, at the time of hiring and every following year, is required to complete security and awareness training.