AuditFindings Security

We take the security and operation of AuditFindings seriously. As such, controls have been implemented to minimize the risk to the confidentiality, integrity, and availability of the system. Controls generally fall into one of the following categories: physical, technical, or administrative. This document outlines aspects of our control environment to current and potential clients.

Facilities Management (Physical Controls)

A primary control is to ensure that our datacenters protect data from physical and environmental risks. AuditFindings uses only industry-leading Tier II, SSAE(1) 16 compliant datacenters. Some of the controls at datacenters include, but are not limited to, the following:

Physical Security

- Physical access control systems that operate on the principle of least privilege
- Video surveillance of onsite access
- 24/7/365 onsite server engineers who perform regular checks of critical datacenter facility systems

Environmental Controls

- Automated non-water-based fire suppression systems
- Redundant heating and cooling systems
- Strategically placed water sensors
- Raised flooring
- Redundant uninterruptable power supplies and transfer switches
- Backup electrical power generators
- Regular testing and preventative maintenance of environment control systems
- Global network operations center that monitors environmental systems for availability and performance

Network and System Security (Technical Controls)

Network and telecommunications are a key to maintaining a secure environment. Several aspects of our network and system security are outlined below.

Perimeter Firewall

The perimeter firewall restricts traffic to authorized protocols, providing the first line of defense for network security. In addition, the firewall can specifically block known locations from attempting attacks on our system.

Web-Application Firewall

A web-application firewall (WAF) has been deployed as an additional layer of security. Unlike the network perimeter firewall, the WAF is designed to help mitigated risks such as cross-site scripting, SQL injection, or other types of attacks targeted specifically to web-based applications.

Patch Management

A key aspect of security is to ensure that system software updates are deployed in a timely manner. System updates are reviewed and applied monthly at a minimum. Key security updates are applied immediately, or may be "virtually patched" via the web-application firewall, until a proper software update can be deployed.

Vulnerability Assessments / Penetration Testing

Although we attempt to minimize vulnerabilities through proper configuration and updating of systems, we conduct security testing through automated and manual processes. At a minimum, weekly vulnerability assessments are conducted on the system. Any identified vulnerabilities are addressed promptly, to include the root cause of the issue.

Encryption

The AuditFindings system uses industry-accepted encryption methods to protect customer data and communication during transition between a customer's system and the AuditFindings system.

Remote Access

Remote access to AuditFindings systems is strictly controlled. All remote access is provided through a Virtual Private Network or dedicated connections from known end points via Secure Shell sessions.

Administrative Controls

The following section outlines some of the administrative controls related to information security program.

Risk Assessment

A risk assessment is conducted at least annually to determine appropriate controls are in place. The assessment is updated if there are significant changes in the environment, business processes, or technology.

Policy Oversight

Policies have been established to guide the operation of AuditFindings. These policies are reviewed annually at a minimum. Policies are modified, or updated, in light of risk assessments or audit recommendations.

Change Management

All changes to the network design or security settings go through a change management process. This change management process is used to ensure that security is not compromised during system changes.

Access Level Reviews

Access levels granted to AuditFindings employees or contractors are reviewed at least annually. This review ensures that access levels for personnel are limited to only the access needed for these personnel to perform their duties. AuditFindings subscribers manage the access levels for their authorized users.

Termination Procedures

Formal termination procedures have been established. System access is removed or disabled for all personnel who are no longer need access to the system.

Subscriber Agreement

All AuditFindings subscribers are required to agree to the AuditFindings Subscriber Agreement. During the first login, this agreement is signed electronically. The agreement describes the end-user requirements for access to, and use of, AuditFindings.

Application Development

Software development is governed by our Application Development Process. This process includes a planning phase where all recommended changes are reviewed for applicability, considering security as well as business needs. Backups of all application files are made before and after changes to the production systems.

Disaster Recovery

AuditFindings has taken steps to ensure that client data is available when needed. Although we strive to maintain 100% uptime, there could be extreme cases where natural disaster or other event impacts the operational capability of our datacenter. As such, backups of all systems are performed daily to ensure adequate recovery of data. Our disaster recovery plan has the following recovery objectives: (a) Restoration of the Auditfindings system within 48 hours of declaration of a disaster (b) maximum of 24 hours of customer data loss.

Return / Deletion of Customer Data

At any point customer may obtain their data in downloadable file in comma separated value (.csv) format and attachments in their native format. After contract termination, customer data submitted to the AuditFindings is retained in inactive status within the system for up to 30 days, after which it is overwritten or deleted. As part of our recovery/backup plan, customer data may be stored for an additional 90 days beyond this period on backup media.

Client Control Considerations

Within their organizations, AuditFindings subscribers should consider whether controls related to the following areas are in place:

- Users should log out of the application when the system is unattended. The "session" key can remain until the browser cache has been cleared. Selecting the "logout" ensures that the session key is deleted.
- Users should maintain appropriate anti-malware controls on systems that access AuditFindings.
- Subscribers should notify AuditFindings if they think their account has been compromised in some manner.
- Users should control output of AuditFindings generated reports.
- Subscriber administrators should ensure that only authorized users have access to AuditFindings system.

(1) Statements on Standards for Attestation Engagements (SSAE)