SECURITY

INFORMATION SECURITY PROGRAM STATEMENT

EQUISOLVE

What to Expect

This document will walk you through Equisolve's Information Security Program

Information Security Program Statement Summary

Equisolve's enterprise security strategy revolves around people, processes, and technology. The program is designed to assist customers in managing their risks across the supply chain.

Equisolve implements a defense in depth strategy, which combines physical control measures with logical control measures, and uses a layered security model to provide end-to-end security of corporate and customer information.

Equisolve's policies and procedures are considered proprietary and not for external distribution. This statement provides an overview of the standard controls applied within Equisolve's environment.

Information Security Program Overview

The high-level objective of the information security program is to protect the confidentiality, integrity, and availability of all information assets within the corporate environment. This is accomplished by building a program around five foundational control areas:

- Program Oversight
- Change and Vulnerability Management
- Access Management
- Network Security
- Incident Management

Each of these areas is supported by several key controls identified below. These key controls provide Equisolve management with assurance that the confidentiality, integrity, and availability of systems are managed in a risk-appropriate manner.

A.
Program Oversight

The objective of program oversight controls is to ensure that the overall structure of the information security program is effective.

The security program is led jointly by the CTO and Director of Information Security who collectively spearhead the development, implementation, and maintenance of all security policies and procedures.

The security program has been designed leveraging multiple control frameworks to support the defense-in-depth security strategy, including NIST Cyber Security Framework (CSF), ISO 27001, and AICPA's SOC2 Trust Service Principles.

A-1 Information Security Policies and Procedures

Information security policies and procedures are created and updated regularly. Equisolve's security program is governed via documented policies and procedures adopted by executive leadership and made available to the entire organization. These policies and procedures provide the organization's requirements and minimum mandatory security practices. These documents are reviewed at least annually for updates to ensure they continue to address the organization's security requirements.

A-2 Security Awareness

Organizational security requirements are communicated as a part of security awareness. To ensure that all employees are aware of their responsibilities around information security, security awareness training is created and provided to employees. To remain current, training is reviewed for updates no less than annually. Awareness of information security policies and procedures helps ensure the Confidentiality, Integrity, and Availability (CIA) of Equisolve information and systems.

A-3 Assurance Testing

Penetration Testing: Penetration testing is performed on a periodic (not less than annual) basis. To assure the effectiveness of the defense in depth model for the organization, penetration testing is performed periodically by an independent third party, no less than annually. The scope of this testing includes externally available resources and a sampling of internally available systems within the Equisolve environment.

SOC2 Certification: For Equisolve to maintain a robust security program, the organization is held accountable by engaging with a third party to perform external audits of security controls related to AICPA's Trust Services Principles, specifically Security and Availability.

Issue Management: All findings related to assurance testing are reviewed by management, and remediation efforts are tracked to completion.

A-4 Information Security Risk Assessments

Information Security risk assessments are performed regularly. The performance of these risk assessments provides data on the sufficiency and effectiveness of information security controls. The results of these assessments provide management with the information needed to make changes or additions to the security control structure. Risk assessments are completed not less than annually. The results are communicated appropriately within the organization to support effective and timely remediation efforts.

A.
Program Oversight (cont'd)

A-5 Log and Event Management

Critical system logs are sent to a central location for aggregation and incident and event monitoring. A centrally located, protected, and searchable log management solution is in place to support the security controls around change and vulnerability management, access management, and incident management. The log management solution also provides advanced analytics and alerting on events as necessary. All logs are recorded and maintained in a separate environment than customer data and are retained for one (1) year.

A-6 Third-Party Risk Management

Equisolve's Third-Party Vendor Risk Management function is responsible for establishing and overseeing processes and practices that help ensure vendors have processes to protect against the potential for compromise or loss of sensitive data. These processes include initial due diligence and ongoing assessment of third-party security practices (for third parties that have the potential to access or obtain sensitive data and those that present a significant business continuity risk), ensuring the establishment of contractual provisions that define responsibilities for data protection and appropriate escalation and issue tracking for identified control weaknesses.

The Third-Party Risk Management process is designed to manage and mitigate operational and reputational risk associated with third-party provider services. Key control elements include due diligence reviews, contract establishment, ongoing monitoring practices related to third-party relationships, and adequate risk assessment activities at all stages of the lifecycle. Critical third parties are reviewed annually for the duration of the relationship.

B.

Change and Vulnerability Management

Appropriate change and vulnerability management efforts are essential to the effective implementation of the information security program. The controls in this area are intended to ensure that changes to the infrastructure do not compromise the enterprise information security posture and that vulnerabilities are identified and remediated effectively.

B-1 Vulnerability Management

Equisolve has developed a vulnerability management methodology where systems are scanned for vulnerabilities and patched ongoing. System vulnerabilities are continuously detected and patched according to a risk-based methodology. Regular patch updates are applied to all desktops, workstations, and critical infrastructure per a 24-hour SLA. Additionally, processes are in place that allows out-of-band or emergency updates to systems as needed.

B-2 Endpoint Security

Equisolve issues corporate laptops to all employees and prohibits the use of personal devices to conduct business. Every corporate endpoint is assigned a certificate, and access to the IT environment can only be accomplished using these devices with assigned certificates. Equisolve maintains control over all endpoints through an Endpoint Mobility Management (EMM) service, which allows the enforcement of configurations, asset tracking, and overall monitoring. Equisolve also enforces encryption on all workstations and strong password parameters.

B-3 Malware Defenses

Malware defense controls are deployed on systems throughout the environment. Equisolve uses a “best of breed” endpoint security solution that continuously monitors all systems for malicious files, unauthorized software, and suspicious behavior. Where necessary, high-risk issues are actively addressed through quarantine and blocking. Only supported versions of the endpoint security agents are deployed, and signatures are updated regularly to ensure up-to-date coverage. The software is managed by a central console which provides details on system definition compliance. Malicious activity generates alerts that are sent to appropriate personnel for remediation.

B-4 Change Control

Changes to enterprise production systems go through the change control process. Change control is essential for creating a recoverable, auditable, and securable environment. As a result, Equisolve has a change control process requiring that all production systems changes go through the Change Control Board (CAB). All requests for changes (RFCs) are documented in a change repository and can be used for troubleshooting and historical tracking. The CAB meets bi-weekly to review all RFCs for approval. Emergency change requests may be implemented using the emergency change procedure outside of the normal CAB meeting schedule.

B-5 Application Security

Application security requirements are considered throughout the software development lifecycle (SDLC). As a company that creates internet-accessible web applications, creating secure applications is a priority. To accomplish this, all changes within the application development process are designed and tested rigorously in a non-production environment before moving into production. All key development milestones are documented, and strict segregation of duties is maintained across development, test, and production environments to mitigate unauthorized. Additionally, monitoring controls are in place that track changes moved into production and are periodically audited to confirm appropriateness.

C.

Access Management

The proper implementation of access management controls is essential for protecting corporate and customer information assets' confidentiality, integrity, and availability. The controls in this area are intended to ensure that only the appropriate users have access to create, read, update, or delete protected assets.

C-1 New Access

Equisolve has adopted the strategy of least privilege for all access granted within the organization. Each user is assigned an email account that serves as their identity for many systems where Single Sign-On (SSO) is enabled. Furthermore, role-based privileges are incorporated into the Amazon Web Services (AWS) environment to ensure appropriate access.

C-2 Role Changes, Terminations, Reviews

Managers are required to ensure that status changes and terminations of employees, contractors, and third-party users are immediately reported to mitigate the risk of unauthorized access.

User access reviews of all systems are conducted at least annually which are conducted at least annually across all systems to ensure access and permissions remain appropriate.

C-3 Authentication

Where possible and appropriate, Single Sign On (SSO) is leveraged as the primary authentication method used when accessing Equisolve managed information assets. In addition to the SSO capabilities, Multi-Factor Authentication (MFA) is enforced for all systems that contain sensitive data, including the AWS and client environments. MFA mechanisms require that a separate device in possession of the user be used to validate secondary authentication. It should also be noted that Equisolve leverages private keys to further protect customer instances within the cloud environment.

C-5 Password Management

The Equisolve Security team requires that an approved password management system be used for all corporate accounts that enforce the enterprise password policy, inclusive of complex construction requirements and the prevention of password reuse.

D.
Network Security

D-1 Network Segmentation

Equisolve leverages network segmentation extensively throughout its operating environment. Development and test environments have been designed to be completely segregated and inaccessible from the production infrastructure. A robust confirmation management

Firewalls and other network segmenting technologies are utilized to control access to systems and environments containing sensitive information. These technologies are located between key operating segments with differing trust levels and are configured with a default deny posture to ensure that only required connections are allowed.

Equisolve customer websites (and subsequent data) are hosted in a shared infrastructure but are logically separated from other customer instances.

D-2 Configuration Management

Equisolve maintains robust configuration management procedures within its operating environment to ensure that the entire production environment is hardened and aligns with industry best practices. This includes measures such as disabling open ports, removing vendor accounts, disabling root accounts, etc. Additionally, baseline configuration images are applied to production servers to maintain a consistently strong security posture.

D-3 Restricted Access

Equisolve provides public facing-facing website services that are accessible globally. All system admins are restricted to specific devices and must connect via VPN to the internal operating environment to ensure that the systems that support these services remain secure. Additionally, all system calls are monitored and recorded to ensure integrity and prevent unauthorized connections to known malicious and likely bad sites.

D-4 DoS/DDoS Mitigation

Equisolve maintains various mitigation technologies and processes required to quickly detect and mitigate Dos/DDoS attacks and migrate an affected website to different resources.

D.
Network Security (cont'd)

D-5 Encryption

Equisolve maintains stringent encryption standards to protect sensitive data while in transit and at rest:

- All data transmissions between Equisolve's service and associated clients utilize strong encryption. The latest recommended encryption methods are used to protect all web traffic to hosted websites, including TLS 1.2 protocols and AES 256 encryption.
- All production data stored in Equisolve's environment is encrypted using FIPS 140-2 compliant encryption standards. These encryption methods are incorporated throughout Equisolve's environment (e.g., databases, production backups, key management system). Equisolve leverages AWS Key Management System (KMS) solution to store encryption keys in a secure environment that is segregated from other resources.

D-6 Physical Security

Equisolve leverages the power of AWS, and all services are hosted in their secure cloud data centers with advanced protections around physical hardware and infrastructure.

D-7 Data Retention and Disposal

Equisolve protects customer data throughout its entire lifecycle and has mechanisms in place to remove customer data promptly upon expiration guidelines set forth by customers or when a contract has ended. Additionally, data is deleted periodically from production systems as backups are maintained. As Equisolve leverages AWS servers, removing data from decommissioned disks is the responsibility of the vendor, who follows strict guidelines based on NIST standards.

E.

Incident Management

While preventing an incident is always preferred, incidents will invariably occur. As a result, a well-formed plan around incident management is essential. The controls in this area are intended to ensure that Equisolve is positioned to respond to and remediate incidents efficiently, effectively, and promptly.

E-1 Security Incident Management

Equisolve's Incident Response Plan addresses the following components:

- Incident Reporting
- Incident Detection and Response
- Incident Handling Procedures
- Incident Team Responsibilities including reporting (internal/external)
- Incident Forensic Processes

Additionally, Equisolve maintains a communication process that alerts relevant parties (e.g., customers, service providers) in the event of an incident that may impact their environment. Finally, Equisolve's security team tests the Incident Response plan at least annually and records the results to continuously improve the process.

E-2 Business Continuity

Equisolve's technology operations are completely cloud-hosted, which provides a distributed operational production environment across multiple logical computing instances and physical locations. This architecture allows Equisolve the ability to distribute technology processes globally to maintain redundancy throughout the production environment. Subsequently, Equisolve inherently has protections against loss of connectivity, power outages, destruction of a physical location, etc. This allows for the easy replication of customer environments to avoid downtime. Additionally, Equisolve maintains full backup copies of production systems, which are updated daily. Finally, Equisolve conducts periodic tabletop exercises to test the Disaster Recovery plan and backup recovery capabilities.