Equisolve Security Program

At Equisolve we take security and availability seriously and work hard to keep your site secure and operational 24/7.

SOC 2 Audited

Our control environment is audited to the AICPA SSAE 18 SOC 2 standard including security, availability, confidentiality, and processing integrity. In addition, our cloud provider Amazon AWS is SOC 2 audited and holds multiple other certifications.

Technical Controls

Firewalls

Firewalls are used for both our internal and external services and configured with the minimum access necessary to provide the services.

Monitoring and Intrusion Detection

Equisolve continuously monitors services for availability and runs intrusion detection systems (IDS) both on the host and network levels to detect any anomalies or unauthorized access attempts.

Physical Security

Equisolve relies on best-in-class cloud infrastructure provider Amazon Web Services (AWS) for our server and network infrastructure. AWS has one of the strongest security environments of any cloud provider, with SOC 2, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and other standards and audits. For more information see https://aws.amazon.com/compliance/programs/

Access Controls

Employee access is protected by a strong password policy, and 2-factor authentication wherever possible. Account access is limited to the minimum access level needed to perform the required duties. Single sign-on (SAML) is available to provide clients seamless account management.

Logging and Auditing

All-access to our systems is logged. Logs of changes to client data are retained for the duration of the client contract.

Account Security

Passwords are protected by multiple rounds of hashing with a salt according to industry standards.

Encryption

All data is encrypted in transit using industry-standard TLS, VPN, and SSH protocols. Data is encrypted at rest using industry-standard AES encryption with keys stored in hardware security modules.

Policies & Procedures

Software Development Lifecycle

Our secure software development lifecycle helps to ensure the security of the software that we develop. This includes developer security training, code reviews including security checklists, regular vulnerability scanning, and regular third-party penetration tests.

Change Management

Equisolve uses a formal change management process to track and approve changes to systems and software.

Incident Response

Equisolve has a security incident response policy covering response to any security incidents identified, including classification, response, recovery, and reporting.

Security Log Retention

Security logs are retained for 180 days, after which they are securely deleted.

Background Checks

All new hires must pass strict background checks including SSN trace, criminal search, sex offenders registry, and education and employment verification.

Security Training

All employees are provided initial security training and annual security training, as well as continuing alerts on emerging threats.

Business Continuity & Disaster Recovery

Equisolve has a formal Business Continuity and Disaster Recovery plan, which is regularly reviewed and updated. Our use of multiple regions within AWS and backups outside of AWS provides resilience in the face of large service provider outages.

Third-Party Security

Our security is only as good as the security of the vendors we rely upon, so all vendors are strictly vetted and monitored according to our vendor management policy.