ASSENT COMPLIANCE PLATFORM

DATA & INFORMATION SECURITY

Data is the key component of every supply chain due diligence program. Companies want their data protected on multiple fronts, from network security to operational standards. As your data partner, we are committed to protecting your information, deploying sophisticated control standards to maintain the integrity of our database.

In holding to these standards, we rely on industry best practices, robust security infrastructure and comprehensive policies to protect our data, along with that of our clients and partners. Listed below are some of the ways Assent protects information and data.

APPLICATION SECURITY

ENCRYPTION:

Data in Transit: Internet communications are encrypted via Secure Hypertext Transfer Protocol (HTTPS), Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS).

Data at Rest: Customer data is secured using Advanced Encryption Standard (AES).

Separate Environments (QA, DEV, UAT, PROD): Development, testing and staging environments are separated from the production environment, both physically and logically.

Data Segregation: All customer data is segregated by state-of-the-art security controls that can only be accessed by designated individuals who have been assigned unique credentials and privileges. Additionally, separate SFTP directories are created for each customer to enable data transfer.

Penetration Test: An independent third party performs a manual web penetration test on the application annually.

Vulnerability Scanning: An automated vulnerability scan is run on every code release before it is pushed to user acceptance testing (UAT). If the penetration test fails, the release and relevant information are sent back to development.

Configurable Password Policy: The default password settings require a minimum of eight characters from three of the four groups (uppercase, lowercase, numeric, symbols). Passwords have a maximum age of 60 days and users cannot reuse the last three. This setting can be configured on a client-by-client basis.

PHYSICAL SECURITY

Data Center Security: Assent uses a third-party, Tier III data center with its own SOC 2 Type II certification (reviewed annually) to host its service. The facility employs a two-stage biometric authentication process, video-monitoring and individually-locked cages.

NETWORK SECURITY

Intrusion Detection and Prevention: Industry-leading Intrusion Detection System (IDS) and Intrusion Prevention Software (IPS) applications and appliances are used to detect, prevent and mitigate any potential security events.

Architecture: Assent's network architecture follows high availability and topology practices to ensure customer data is isolated from edge network traffic.

Vulnerability Scanning: Assent performs both real-time and scheduled weekly in-depth vulnerability scans to monitor network and endpoint security.

Security Incident Event Management (SIEM): Assent uses an industry recognized SIEM solution to monitor, detect and respond to security incidents.

Redundancy: Multiple data paths are configured through the entire stack to ensure network availability.

Network Access: Access to the Assent network is restricted to authorized users and devices.

OPERATIONAL SECURITY

Security Incident Response: Assent has a documented incident response plan.

Disaster Recovery: Assent has a disaster recovery plan that is tested annually.

Change Management: Production changes are subject to documented approval, testing and validation.

Two-Factor Authentication: Two-factor authentication is used for administration of the production environment.

Backups: Full backups are performed weekly, while log and differential backups are performed hourly (offset by 30 minutes).

SERVER PROTECTION:

Patching and Maintenance: System security patches are applied monthly.

Anti-Malware: All servers are protected using industry-recognized endpoint protection software.

USER WORKSTATION PROTECTION:

Full Disk Encryption: All Assent-owned mobile devices, including phones or laptops, are encrypted.
Anti-Malware: All workstations are protected using industry-recognized endpoint protection software.

SECURITY COMPLIANCE

SOC 2: Assent has a SOC 2 Type I report, available upon request and under non-disclosure agreement (NDA).

ADDITIONAL SECURITY PRACTICES

Policies: Assent has a comprehensive set of security policies. These policies are made available to all employees and contractors with access to Assent information assets.

Training: Assent has mandatory annual security awareness training for all employees.

Background Checks: Assent performs background and criminal reference checks on all new employees in accordance with local law.

Confidentiality Agreements: All new hires are screened through the hiring process and required to sign confidentiality agreements.

SUMMARY

Assent's data and information security policies and procedures give companies peace of mind. They ensure all Assent staff are diligent and rigorous in the protection of data assets, and employs state-of-the-art control standards to keep data safe from both physical and network security threats.

If you have any questions or would like to know more about our data and information security policies and procedures, please contact us at info@assentcompliance.com.