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 to Assent.

Penetration Testing: An independent third party performs web and network penetration tests on the application annually. Tests are performed every six months by internal teams.

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

Single Sign-On: Assent supports the most frequently used, high-security authentication protocols — OAuth (JSON based) and SAML (XML based).

PHYSICAL SECURITY

AWS Security: Assent leverages Amazon Web Services (AWS) to host its services. AWS security is backed by numerous certifications, including SOC 2 and ISO 27001.

NETWORK SECURITY

Intrusion Detection and Prevention: Network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are in place at application ingress and egress points to detect, prevent and mitigate potential security events.

Data Loss Prevention: Assent uses a layered approach to data loss prevention on endpoint, network and cloud using next-gen security tools in combination with more traditional approaches.

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

Network Vulnerability Scanning: Assent performs regular, 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.

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 that covers all aspects of an incident, from detection to post-incident analysis.

Disaster Recovery: Assent has a disaster recovery plan designed to ensure minimal disruption in the event of a disaster. The production environment, including customer data, is replicated to a secondary site that is available if the primary site goes offline. The disaster recovery plan 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.

Central Management: All workstations are centrally managed for patching and configuration.

SECURITY COMPLIANCE

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

ADDITIONAL SECURITY PRACTICES

Dedicated Security Team: All members of Assent's Security team hold appropriate security certifications and clearances.

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

Training: All new personnel attend security awareness training before gaining network access and are required to complete security awareness training annually thereafter. Additionally, the Security team provides periodic awareness updates via email.

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

Confidentiality Agreements: All new personnel are required to sign confidentiality agreements.

ITAR Compliant Offering: Assent has an available ITAR-compliant Assent Compliance Platform environment hosted in the AWS GovCloud. Please ask your sales representative for more information.

SUMMARY

Assent's data and information security policies and procedures give companies peace of mind. They ensure all Assent personnel are diligent and rigorous in the protection of data assets, and employ 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.