ASG Technologies Group, Inc.

Document title	**Secure Software Development Life Cycle of ASG Products**
Document status	Final
Document owner	Jeana Huynh, Director Information Security & Svcs Prashob Padmanabhan, Manager Customer Care Deepthi Gulla, Sr. Software Engineer
Document approver(s)	Pascal Vitoux, SVP Development & CTO Vernon Clemons, SVP Global Customer Care

Version	Version history	Version date
1.00	Final	2/25/2021
1.01	Updated verbiage in Secure Development Methodology section	2/26/2021
1.02	Updated verbiage for Vulnerability Management section	3/2/2021

Preface and document control

This document is intended to provide ASG Technologies Group, Inc.'s policy, procedure, standards and guidance on the subject matter contained herein. This document shall be reviewed at least annually to ensure validity.

ASG reserves the right to modify or change this policy at any time without prior notice (subject to compliance with applicable law).

Neither all nor part of this document shall be reproduced or released by a recipient without the explicit authorization of the stated document owner.

Secure Software Development Life Cycle of ASG Products

This document serves to inform our ASG customers of our application security for ASG products.

ASG's objective for our internal environment is to adhere to the Control Objectives for Information and Related Technologies (COBIT) and align to ISO 27001/27002 standard and controls.

This includes:

- Providing security awareness training for new hires and annually thereafter. The Security team provides additional advisories and training based on current security events. Providing development staff secure code training covering OWASP Top 10 security risks.
- Performing background checks on all new employees and contractors in accordance with applicable laws. All staff are required to sign Non-Disclosure and Confidentiality agreements or obligated to agree to confidentiality provisions within their contract with ASG.
- Requiring relevant third-party supplier(s) to comply with the same strict adherence to its Vendor Code of Conduct and information security obligations.
- Maintaining security policies and standards, updating as appropriate, and communicating that information to employees and contractors with access to ASG information.
- Centralizing user account management and ensuring appropriate segregation of duties by practicing the principle of least privilege.
- Requiring password authentication to all corporate resources and enforcing a strong password standard and enabling multi-factor authentication.
- Implementing network security, including on-access anti-malware scanning, encryption of sensitive data in flight and at rest, and monitoring and limiting traffic via firewalls.
- Logging security events and monitoring those logs.
- Testing and staging environments are logically separated from the production environment.
- Providing physical security at our sites using a combination of biometrics, cardkeys, and physical keys.

Secure Development Methodology for ASG Products

ASG aligns with generally accepted industry standards as well as secure software development practices designed to detect and protect its software products against any viruses, trojans, worms, spyware, malware, or other harmful code or interference with or harm to their operation. ASG uses the latest, up-to-date commercially available anti-malware software. When ASG makes available software products to its customers, these have been thoroughly tested.

ASG supports secure software build and design patterns following applicable privacy by design approaches to ensure that cryptographic algorithms apply to the software's processing of data-at-rest and data-in-motion.

Vulnerability Management

ASG employs third-party security tools (e.g., HP Fortify, IBM AppScan, VeraCode) to perform fully automated product scans during our CI/CD (continuous integration/continuous delivery) pipeline for every build to address OWASP Top 10 security risks. We maintain a dedicated product security team to test and work with development teams to remediate all discovered issues; products with security issues are not allowed to be released. The source code repositories are scanned for security issues at three layers; we not only scan source code but are doing more active security testing on live products (e.g., DAST) and validation/testing of all 3rd party libraries.

ASG also employs third-party security experts to perform detailed penetration tests on ASG's SaaS products. For ASG on-premise products, ASG does not directly contract with third parties to perform penetration tests; however, many of our customers have internal teams or external service providers (e.g. VeraCode and Fortify) that scan our products in situ.

Security Incident and Event Monitoring

We have security incident and event monitoring in place for ASG SaaS products and follow documented Information Security Incident Escalation Procedures to ensure all security incidents are assessed and addressed with relevant core team members.

Can Customers have a copy of ASG's latest security scan results?

For the protection of all ASG customers, ASG does not publicly release records of vulnerabilities found and corrected in the software.

Customers with additional questions are invited to email asgsupport@asg.com.