Gen Information Security Standards

INFORMATION SECURITY POLICIES

Gen maintains an Information Security Policy (ISP) that is reviewed and approved at least annually at the executive level. All Gen Personnel have access and are required to comply with the ISP.

ORGANIZATION OF INFORMATION SECURITY

Gen adopts physical, technical, and organizational security measures in accordance with industry best practices and standards and follows all applicable legal and regulatory requirements as they apply to the Gen's services.

HUMAN RESOURCE SECURITY

Where relevant and legally permissible, Gen performs background verification checks in compliance with Gen policies for all Personnel who may have access to Restricted Data or Confidential Data and/or Information Assets.

Gen provides security awareness training based on industry best practices and standards to all Personnel at least annually. Additional training as may be implemented by Gen as required from time to time.

Gen implements effective user termination or transfer controls that include access removal or disablement within 48 hours upon termination or transfer of Personnel or when such Personnel no longer require handling of Gen Data as part of their job duties for Gen.

ASSET MANAGEMENT

Gen has an Acceptable Use Policy that requires systems and information to be classified, labelled, and handled in accordance with the Asset Management Standard and GenDigital's Data Classification Standard. Those standards define the value, legal requirements, sensitivity, and criticality of the system and information to the organization. Gen Records are also retained in accordance with GenDigital's Records Management Policy.

Gen oversees secure disposal of systems and media to render all Gen Data contained therein as undecipherable or unrecoverable prior to final disposal or release from Gen's possession. This is undertaken in accordance with U.S. National Institute of Standards and Technology (NIST) approved standards.

ACCESS CONTROL

GEN implements strong access control and restricts access to operating system configurations to authorized, privileged personnel for systems handling Restricted Data or Confidential Data. Gen requires that all Personnel who are able to access to Gen Data must use a Gen managed device.

Gen confirms that the system (network, hosting, and application) is designed in compliance with the least privilege principle.

Gen applies the use of strong passwords for all systems (network, hosting, and application). All vendor default passwords within software and hardware products must be changed before or during installation. For administrative accounts and for any accounts that allow remote access to systems, Gen uses multi-factor authentication or other positive controls such as increased password length, shorter password life or restrictive whitelists of users to restrict access to administrative accounts.

CRYPTOGRAPHY

Gen uses NIST or PCI approved encryption and hashing standards (e.g. SSH, SSL, TLS) for transmission and storage of Restricted Data and Confidential Data. Our standard requires that data at rest is encrypted using AES-256 and data in transit is encrypted using TLS 1.2 at a minimum.

Where necessary to be stored on a portable device, the device are protected by full disk encryption. Restricted Data or Confidential Data stored on archive or backup systems are subject to at least the same protection measures used in the live environment

PHYSICAL AND ENVIRONMENT SECURITY

The physical and environmental security of all areas containing Restricted Data or Confidential Data, including but not limited to, data centers and server room facilities are designed to protect information assets from unauthorized physical and logical access, manage, monitor, and log movement of Personnel into and out of such facilities and all other applicable areas, guard against environmental hazards such as heat, fire, and water damage.

OPERATIONS SECURITY

Gen implements operating system hardening for hosts and infrastructure handling Restricted Data or Confidential Data.

Gen employs and maintains comprehensive end point protection including anti-malware solutions configured to download signatures at least daily and a firewall solution (or other threat protection technologies) for end user computing devices and servers which connect to the Gen network or handle Restricted Data or Confidential Data.

Gen prohibits and disables the use of external devices for storing or carrying, or in use with machines handling Restricted Data or Confidential Data.

System audit or event logging and related monitoring procedures are implemented and maintained to proactively record user access and system activity for routine review. All log files are retained for two (2) years and access restricted to authorized personnel only.

Gen utilizes industry standard scanning tools to identify network, host, and application vulnerabilities. We perform at least monthly internal vulnerability scans of network(s), host(s), and application(s) and ad-hoc vulnerability scanning to identify network, host, and application vulnerabilities prior to release to production and after more than minor changes. Gen remediates all immediate, critical, high, and medium vulnerabilities prior to release to production and thereafter. Our standard requires that Immediate vulnerabilities are remediated within 7 days. In addition, Critical vulnerabilities are remediated within 30 days, High vulnerabilities are remediated within 60 days, and Medium vulnerabilities are remediated within 90 days.

Gen performs regular annual penetration test of network(s), host(s), and application(s and ad-hoc penetration tests. In addition products are required to be security reviewed and security tested prior to release to production and no less than thirty (30) days after significant changes and remediate all critical, high, and medium vulnerabilities discovered by the pen-tester, prior to release to production and thereafter within remediation time frames defined above.

COMMUNICATIONS SECURITY

Gen uses firewall(s) to protect networks that handle Restricted Data or Confidential Data. The firewall(s) are able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Gen has network-based security monitoring (i.e., syslog, security information and event management (SIEM) software or host-based intrusion detection systems) for the segment(s) which handles Restricted Data or Confidential Data.

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Gen delivers at least annual secure code training to all Personnel in-scope for delivering service. Developers are proficient in the OWASP Top 10 and the CWE/SANS Top 25 vulnerabilities and their appropriate remediation techniques. Gen maintains an annual review of a documented change management process and software development lifecycle (SDLC). Test data is prohibited in production environments and production data is prohibited in non-production environments. Test data is protected and controlled in pre-production environments and production data is protected and controlled in production environments. Partner data is never used as test data.

THIRD PARTY MANAGEMENT

Gen requires suppliers that either connect to any Gen network, handle Restricted Data or Confidential Data and/or develop or host internet assessable sites on behalf of Gen, maintain applicable security attestations (SOC2/ISO/PCI certifications) and/or complete a Gen security risk assessment (SRA) prior to onboarding and thereafter on an annual basis.

Gen requires the use of confidentiality or non-disclosure agreements for third parties that have access to Restricted Data or Confidential Data. As a condition of gaining access to confidential information, networks, systems, and data, third parties are subject to contractual requirements, including compliance, privacy, and security obligations, such as background checks, audit rights, and data protection agreements.

INFORMATION SECURITY INCIDENT MANAGEMENT

Gen maintains a cross-functional Security Incident Response Team and maintains formal incident response plans and procedures. These procedures specify the responsibilities and actions required in the event of unauthorized disclosure of sensitive data, such as personally identifiable information of consumers, so that personnel can respond to security vulnerabilities and security incidents. In the event of a security event impacting Partner data, Partners will be notified within 72 hours. Gen will cooperate with Partner and provide necessary status reports and updates related to action and remediation plans, including preventative measures deployed.

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Gen maintains a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for its essential in-scope business functions and ensures plans are tested at least annually and findings remediated. The BCP contains the information necessary to plan for the recovery of each essential business function. Gen’s standard RTO/RPO for in-scope services is two (2) hours. The DRP includes multiple fiber optic connections, emergency power, automated fire suppression systems, and redundant bandwidth and server requirements.

GEN COMPLIANCE AND AUDIT COMMITMENTS

The effectiveness of our security program and controls is evaluated annually by independent third-party auditors for SOC2 report and PCI AOC. Gen maintains executive summary penetration tests for in-scope services. Gen makes these attestations of security and penetration test summaries available with appropriate confidentiality agreement and upon request annually. Additionally, Gen follows and adheres to the Shared Assessment Standardized Information Gathering (SIG) security questionnaires. These security questionnaire and internal personnel are available for further questions or follow-up to satisfy Partner audit requirements.