Get Event Log LLC

INFORMATION SECURITY POLICY

CONFIDENTIAL

Version: 1.0
Approval Date:10 June 2025

Change Log

DATE	VERSION	SUMMARY OF CHANGES	AUTHOR
6/10/25	Draft	Initial draft	C Wireman
6/10/25	1.0	Approved document	C Wireman

Table of Contents

Contents

1.0 Purpose and Scope

This Information Security Policy defines the policies focused on protecting the security of Get Event Log LLC (or the "Company") including personnel, information systems, and information assets. This policy is intended to provide a holistic andcomprehensive approach to the Company's overall information security posture.

Information is an asset that the organization has a legal, regulatory, and contractualduty and responsibility to protect. Company senior management is responsible for promoting confidentiality, integrity, and availability of complete and accurate information as essential to the Company operating in an efficient manner and to providing its products and services to clients.

The Company's information security management system consists of the serviceofferings and applications developed by the Company and the dedicated environments supporting these offerings. In-scope services offerings and applications include the following:

- Get Event Log LLC API
- Get Event Log LLC Computing devices
- Get Event Log LLC Business devices
- Get Event Log LLC Software & Documentation

This Information Security Policy is based upon ISO 27001 and adheres to the ISO27002:20051 standard, which provides a framework for the key policy directivesof the Company in pursuit of Company Business Activities. This Information Security Policy is supported by additional detailed and specific standards and procedures that outline the execution of the Information Security Policy.

Company executive management is committed to supporting this Information Security Policy and requires that all members of the Company Workforce follow these requirements and related procedures with respect to Information Security.

This Information Security Policy update shall become effective upon publication.

1.1 Applicability

All members of the Company Workforce, including permanent full-time and temporary employees, and other members of the Workforce including agency andindependent contractors shall abide by this policy.

Suppliers and Vendors with access to or providing sensitive or protected information shall also be required to abide by information security requirementsas outlined in the relevant contracts.

1.2 Related Documents

This policy is intended to define Management's intent, which will drive the establishment of a Control Framework that establishes requirements and guidelines for the standard operating procedures in place within the organization.

2.0 Requirements

The Company's organizing principles responsible for the implementation, maintenance, and enforcement of this Information Security Policy are described inSection 6.0 Organization of Information Security.

Terms used throughout the document are defined in section 16.0 Definitions.

2.1 Exceptions and Approvals

The Information Security Risk Council shall review and approve this policy on anannual basis.

Any exceptions to, or variations from this Information Security Policy shall be submitted in writing to the Information Security Risk Council for review and approval prior to implementation. All exception requests must be submitted in writing and include reasoning for the request, an action plan to ensure compliance, and the name of the responsible party for plan execution. The plan must include proposed compensating controls to ensure that Information SecurityPolicy objectives are appropriately met.

The Information Security Risk Council shall review granted exceptions for approvalannually.

3.0 Policy Framework

3.1 Policy Document

This policy is based upon ISO 27001 and is structured to address the 13 clausesincluded in Annex A of the ISO 27001 framework.

Get Event Log LLC's approach to Information Security includes the maintenance of completeand accurate information through the preservation of:

- **Confidentiality**: ensuring information is accessible only to those authorizedto have access
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods
- **Availability**: ensuring authorized users have access to information and associated assets related to sensitive information ("Assets") when required

The Information Security Policy shall be communicated to all members of the Get Event Log LLC workforce through appropriate means including the Intranet, educational and training, and supervisor instructions. All members of the workforce shall provide acknowledgment of receipt of the Information SecurityPolicy annually, and the Human Resources department shall track said acknowledgements.

4.0 Risk Assessment and Treatment

The Company shall implement a risk management process to identify, categorize,classify, prioritize, treat, and document information security risk.

The Company shall implement an Information Security Risk Council to define andmanage the risk management process.

The Information Security Risk Council shall meet regularly to review and determinerisk treatment and priority. The process for risk evaluation and treatment shall be defined in a Risk Management process document.

5.0 Information Security Policy

This Information Security Policy shall document the policies and some procedures of the Company's Information System Management System. This Information Security Policy is established to provide a holistic and comprehensive approach to the Company's overall information security posture.The high-level objective of the Information Security Policy is to ensure the confidentiality, integrity, and availability of information.

The Information Security Policy and updates shall be communicated to all staff andemployees of the organization, and relevant third parties annually.

5.1 Management Direction for Information Security

Company executive management is committed to supporting this Information Security Policy and requires that all members of the Company workforce are informed aboutthe Information Security Policy and follow the defined requirements and related procedures with respect to Information Security.

IT Management shall review the Information Security Policy and related proceduresannually. IT Management shall recommend updates to the Information Security Policy and related procedures to ensure continued suitability, adequacy, and effectiveness of Company policies and procedures.

The Information Security Risk Council shall review and approve all updates tothe Information Security Policy annually for major updates, and as needed forinterim or minor updates.

The Senior Security Program Manager is the member of the executive management team that has the ultimate responsibility for the InformationSecurity Program.

6.0 Organization of Information Security

6.1 Internal Organization

6.1.1 Information Security Roles and Responsibilities

The Company CEO and CTO are responsible for the establishment of the Information Security Policy, and as such must annually review and approve the policyas a member of the Information Security Risk Council. The Senior Security Program Manager (SSPM) shall be designated and assigned responsibility for theorganization's cybersecurity program. The official shall be responsible for ensuring security processes are in place, taking into consideration organizational requirements, and communicating security processes to all stakeholders. The SSPM shall also be assigned responsibility for the effectiveness of the informationprotection program through program oversight. This includes but is not limited to, establishing and communicating the organization's priorities for organizational mission, objectives, training, and activities, reviewing and updating the security plan, ensuring compliance with the security plan by the workforce, and evaluating and accepting security risks on behalf of the organization.

Company executive management are responsible for overseeing the development,implementation, and support of this policy.

The Information Security Risk Council is made up of select members of the executive management who are responsible for making decisions on security issues by evaluating their risks to the company and approving the remediation priority required to address these issues. The Senior Security Program Manager isthe member of the executive management team and Information Security Risk Council who has the ultimate responsibility for the Information Security Program.

The Company designates the CTO as the Information Security Officer. The Office ofInformation Security shall include the CTO, the Director of Datacenter Operations,the SSPM, The Director of Architecture, and the VP of Development.

The SSPM is the custodian of the policy, responsible for the development of theinformation security policies and the ongoing review of their effectiveness.
Additionally, the SSPM will oversee the information protection program and reviewthe program when any significant changes occur, and at least annually.
Documentation related to the information protection program shall be madeavailable to relevant personnel internal and external to the organization.

Company managers are responsible for supporting and ensuring that respectiveemployees comply with the Company Information Security Policy.

All employees and contractors with access to sensitive systems are required to comply with the Information Security Policy to protect the company information assets. They must not access or use information without authorization and must immediately report suspected security breaches or vulnerabilities to the Office of Information Security. All employees and any contractor with Get Event Log LLC email address shall be responsible for completing the annual Company Information SecurityAwareness Training and post training assessment to demonstrate a minimum levelof understanding. (Contractors without access to sensitive Get Event Log LLC systems are excluded.) Each employee and contractor with a Get Event Log LLC email address must take the Information Security Assessment and pass with a score of 75% or higher. Those who do not pass will be remediated by the Information Security Program Owner to ensure those members have a thorough understanding of this policy andtraining material.

Detailed job descriptions shall be defined and documented for personnel responsible for the management of information systems and information assets.Job descriptions shall be utilized to define user roles and responsibilities and setexpectations for the duties associated with the role.

6.1.2 Segregation of Duties

Segregation of duties shall be implemented, where appropriate, to reduce the risk ofunauthorized or undetected changes within the Company's information system andreduce the risk of fraud and errors.

In the context of the Company's Information System, access to production and nonproduction environments shall be restricted using assigned information systemaccess authorizations based on user role, responsibility, and the principle of least privilege.

The principle of least privilege requires that access to information be granted themost restrictive set of privileges needed for the performance of authorized tasks.Under the principle of least privilege, users are granted the minimal level of access to information and information systems needed to perform their duties.
The manager of the requester and the Information Security Officer must approveescalated privilege.

HR and Company managers shall develop user role descriptions. IT shall translaterole description into system-based user roles with appropriate system authorizations. IT shall grant access to Company systems based on these definitions. The manager of the requestor and the Office of Information Security must approve system-based user roles and authorizations. The manager of the requester and the Information Security Officer must approve exceptions to standard roles and/or authorizations.

When segregation of duties is not possible, the Company shall implement peer review and approval processes to ensure systems and information are not created,modified, or deleted in an unauthorized manner.

6.1.3 Contact with Authorities

Procedures and appropriate personnel designated to contact authorities (e.g., law enforcement, regulatory bodies, etc.) based on the nature of the event (e.g., cyber security attacks, natural disasters, utility outages) shall be defined in the company'sIncident Response, Disaster Recovery and Business Continuity plans.

As part of the Disaster Recovery Plan, emergency procedures, manual fallback procedures, and resumption plans are the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services are the responsibility of the applicable service providers. When new requirements are identified, any existing emergency procedures are amendedas appropriate.

6.1.4 Contact with Special Interest Groups

Information Security leadership should maintain membership in special interestgroups including specialist security forums and professional organizations.
Memberships in such organizations are specified as part of the Information systememployee's job requirements. Only those employees who have specific job requirements shall have access to special interest groups.

6.1.5 Information Security in Project Management

The Company shall implement a risk management process to identify and evaluate information security risks. The Information Security Risk Council shall define and manage the risk management process. A formal risk assessment must be completedprior to initiation and implementation of all company projects. All risks must be documented and a response to each risk must be identified and integrated into the project plan.

Information Security objectives must be established prior to the initiation of Company projects. The objectives must align to Company policy, standards, and procedures with the intent to protect the confidentiality, integrity and availabilityof Company information and systems. Information Security objectives must be evaluated throughout the project lifecycle to ensure objectives are appropriately met.

The Company shall implement standards and procedures to ensure informationsecurity is managed throughout the lifecycle of every project. These standards and procedures will be incorporated into all aspects of the project including development, quality assurance, operations, and post-project evaluation.
Examples of the standards and procedures include secure build standards, securedevelopment standards, security testing procedures, etc.

6.2 Mobile Devices and Teleworking

6.2.1 Mobile Device Policy

Users of company issued or personal mobile devices that access or store companyinformation or connect to the company network must adhere to the following guideline below in conjunction with the Acceptable Use Policy.

6.2.1.1 Personal Mobile Devices

Users of personal mobile devices that access or store company information, or connect to the company network must adhere to the following:

- The mobile device must be password protected using the features of the device and a strong password is required to access the company network.
- Access to company information or connection to company network is subject to removal of access, remote disconnection, or lockout and/or

- remote wipe of the personal device if A) the device is lost or stolen, B) employment is terminated, C) there is detection of a data, network, or policy breach, malware, spyware, any unwanted potential applications, orsimilar threats to the security of the company's data or network.
- The mobile device must lock itself with a password or personalidentification number (PIN) after it is idled for 5 minutes.

6.2.1.2 Wireless Access Connection

Users of company issued or personal mobile devices that access or store companyinformation, or connect to the company network must adhere to the following:

- Users connecting to a public wireless connection should only connect to anaccess point that offers a secure connection using Wi-Fi Protected Access (WPA) with AES encryption.
- Users should never connect to a public wireless connection that is open orinsecure without using a Company VPN connection.
- For company issued devices, when connecting to a public wireless accesspoint or hotspot, if applicable users should connect to the Company VPN.

6.2.1.3 Safekeeping and Travel

Users of company issued or personal mobile devices that access or store companyinformation, or connect to the company network must adhere to the following:

- If applicable, devices must have full-disk encryption
- Users are to immediately report lost or stolen devices
- Always ensure appropriate physical safekeeping of the device

6.2.1.4 Minimum Mobile Device Security Requirements Policy

Mobile computing devices should always be protected by appropriate controls toensure the security of data accessed and transmitted by the device. Managementshould identify appropriate control measures which may include access controls,usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, or equivalent functionality, secure configurations, and physical protections. If it is determined that encryption is not reasonable, Get Event Log LLC shall ensure that the business justification and acceptance of risk is documented and reviewed at least annually by senior management. To minimize the risk of data loss through loss or theft of personal mobile devices with access to Company information, a mobile device management (MDM) capability must be used to enforce Company security policies on any personal mobile device accessing Company information.

6.2.1.5 Minimum Security Requirements Procedure

The Chief Technology Officer is responsible for establishing a minimum-security baseline to be required as implemented on any smart phone or tablet PC accessingcompany data or services. The MDM must enable Information Security personnel toperform the following functions on user devices accessing Company information:

- Registration and logging of the user device
- Remote wipe of Company data contained on the device or remote wipe of theentire device
- Remote locking of the user device
- Enforcement of encryption of the Company data container or full discencryption of the user device
- Jailbreak/Root detection on the user device
- Enforcement of minimum password/passcode requirements on user devicesand be prevented from being able to modify password parameters
- Require that the user authenticate to system resources through use of aSingle Sign-On provider which requires username, password, and
- multi-factor authentication before permitting any access to companyresources.

6.2.2 Teleworking

All employees and contractors are encouraged to telework. The company hires employees for their skills and does not need to baby-sit the workers.

7.0 Human Resources Security

7.1 Prior to Employment

As part of the hiring process with the Company, a background verification checkmust be completed by the Legal department.

Candidates for employment with adverse criminal background history or DMVhistory (where applicable) may be disqualified for employment. The hiring manager and HR shall make decisions regarding disqualification.

All new employees and contractors (with access to Get Event Log LLC systems) must reviewand sign an acknowledgement indicating understanding, receipt and agreement of the employee handbook, and expense policy, which define the terms and conditionsof employment, and a code of conduct.

Employees with access to confidential or sensitive information are required toread and sign an acknowledgement indicating understanding, receipt, and agreement with the Company's Confidentiality policy.

All new employees and contractors (with access to sensitive Get Event Log LLC systems)are required to read and sign an acknowledgement indicating understanding, receipt, and agreement with the Company's Information Security policy.

7.2 During Employment

7.2.1 Management Responsibilities

Prior to granting employees and contractors access to Company information or Company information systems, management must properly brief users on their roleand responsibilities regarding information security and protecting the confidentiality of Company information.

Managers must ensure that all members of the Workforce reporting directly to suchManager have been trained and comply with this Security Policy and its related policies and procedures.

Managers must ensure that this Security Policy and its related policies and procedures are fully implemented in his or her functional area of responsibility.

Managers must enforce with the appropriate level of discipline for non-compliancewith or violation of this Information Security Policy.

7.2.2 Information Security Awareness, Education and Training

All employees and contractors (with access to Get Event Log LLC systems) are to complete Information Security Training and acknowledge understanding, receipt and agreement of the Company's Information Security policy prior to being granted access to the Company's information systems (within 60 days of hire). Topics included in training modules will include but not be limited to authentication / passwords, phishing attacks, removable media, and risks of remote working arrangements. Other topics may include:

- Risks, controls, and user responsibilities with respect to the use of mobile computing devices
- Risks, controls, and user responsibilities with respect to teleworking
- BYOD usage, including providing a list of approved applications, applicationstores, and application extensions and plug-ins
- Installation of unauthorized software / programs
- Information exchange of sensitive data (PHI, PII, CUI, etc.)

Additionally, role-specific training will be offered to members of the InformationSecurity team based on their roles and responsibilities.

Annually thereafter, all employees and contractors (with access to Get Event Log LLCsystems) must complete information security training and acknowledge

understanding, receipt and agreement of the Company's policies and procedures to include the Information Security policy and Employee Handbook. Training is conducted via slide presentation. The questionnaire is attached to the training slideand is recorded within a google sheet and is reviewed by the SSPM.

In addition to the agreements, each employee and contractor must take the Information Security Questionnaire and pass with a score of 75% or higher.Those who do not pass will be remediated by the Information Security Program Owner to ensure those members have a thorough understanding of the policies andtraining material.

7.2.3 Incident Response Training

The SSPM is responsible for overseeing incident response training. Personnel with incident response related job requirements are required to complete incident response training within 90 days of assuming an incident response role and at leastannually thereafter. The incident response training topics include the following:

- Procedures related to the identification of potential system incidents or breaches.
- Response procedures based on the nature of an incident.
- Communication channels and escalation procedures when an incident isidentified.
- Notification obligations in accordance with legal and contractualcommitments.
- Documenting lessons learned and implementing remediation activities toprevent a similar incident from occurring in the future.

7.3 Termination or Change of Employment

Human Resources shall be responsible for managing the employee termination process. HR will ensure terminated employees are reminded of their on-going legal responsibilities and, where appropriate, responsibilities contained within theCompany confidentiality agreement, the terms and conditions of employment, andthe information security policy.

Upon separation of employment or termination of contract, the former employee must surrender all assets to the Company and ensure all Company information hasbeen deleted and/or destroyed from all personal devices.

HR is responsible for notifying IT of all terminations. IT shall be responsible for asset reclamation, user account disablement and, when appropriate, destructionof Company information contained on former employee personal devices. This includes the potential utilization of remote wipe capabilities of the implementedmobile device management solution to remotely delete data from or completelywipe the former employee's mobile devices.

Supervisors and Managers must notify HR of all employee role changes. HR isthen responsible for notifying IT of employee role changes. IT should review all employee role changes and modify access privileges as appropriate to the employee's new role.

The IT processes for employee terminations and employee role changes shall bedocumented in a standard operating procedures manual.

8.0 Asset Management

8.1 Responsibility for Assets

8.1.1 Inventory of Assets

All critical Company assets shall be identified and maintained in an asset inventory listing. This includes company virtual machines, physical servers, software assets, etc. The asset inventory listing shall include an owner for each asset. The asset inventory shall be centrally managed and shall not duplicate otherinventories. As part of its asset management processes Get Event Log LLC will follow a documented process regarding the provisioning and deprovisioning of assets.

All assets shall follow the system development life cycle (SDLC) process, whichgoverns practices related to the secure use, transfer, exchange, and disposal ofcompany assets.

8.1.2 Ownership of Assets

The Director of Development Support is responsible for maintaining an inventoryof all assets and services. The asset inventory is updated whenever there is a change of ownership with respect to an asset, and at least monthly. The asset inventory will be centrally managed in Google Drive, to the extent possible to ensure that assets are accurately recorded and tracked, and to avoid duplication. Asset owners shall be identified for all critical Company assets and the responsibility for the maintenance of appropriate controls, including access and availability, shall be assigned to the identified owner.

The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of theasset.

8.1.3 Return of Assets

Upon separation of employment or termination of contract, the former employee and/or contractor must surrender all assets to the company or ensure all companyinformation has been deleted and/or destroyed from all personal devices.

8.2 Information Classification

8.2.1 Classification of Information

Data classification is the classification of data based on its level of sensitivity and theimpact to the company should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All company data should be classified into one of three sensitivity levels, or classifications:

1. **Restricted Data - PII:** Data should be classified as Restricted PII when theunauthorized disclosure, alteration or destruction of that data could causea critical to high level of risk to the company, its clients, or affiliates. Examples of Restricted PII data include data protected by state or federal privacy regulations, and data protected by confidentiality agreements, anddata that contains personally identifiable information or personal health information. All Restricted PII data must be encrypted at rest and in transit.

2. **Restricted Data:** Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could causea critical to high level of risk to the company, its clients, or affiliates. Examples of Restricted data include data protected by state or federal privacy regulations, and data protected by confidentiality agreements. All Restricted data must be encrypted at rest and in transit.

3. **Confidential Data:** Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could resultin a high to medium level of risk to the company, its clients, or affiliates. Bydefault, all company data that is not explicitly classified as Restricted or Public data should be treated as Confidential data. A reasonable level of security controls should be applied to Confidential data.

4. **Public Data:** Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in low or norisk to the company, its clients, or affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of

Public data, some level of control is required to prevent unauthorizedmodification or destruction of public data.

8.2.2 Labeling of Information

All Company information classified as Restricted or Confidential, as defined in thedata classification scheme established in 8.2.1, shall be appropriately labeled. Thelabeling procedures (including labeling omissions) shall be outlined in the Data Classification and Labeling procedure in the Company Standard Operating Procedures.

8.2.3 Handling of Assets

The following guidelines apply to handling of the different types of companyinformation assets.

8.2.3.1 Storage

Restricted Information

Restricted information must be removed from desks, computer screens, and common areas unless it is currently in use. Restricted information must be storedin a secured location when not currently in use. All restricted data must be encrypted in transit and at rest. Encryption requirements shall be defined in 10.0Cryptography.

Confidential Information

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information must be stored in a secured location when not currently in use. Confidential informationshould be encrypted when reasonable to do so.

Public Information

No special storage requirements exist for Public Data.

8.2.3.2 Data Destruction

The following guidelines apply to the destruction of the different types of companydata.

Restricted Information

Restricted data must be destroyed in a manner that makes recovery of theinformation impossible. The following guidelines apply:

- Paper/documents: shredding is required.
- Digital storage (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: data wiping must be used. Ifwiping is used, the Company must use a DOD level wiping application.

Confidential Information

Shredding is required for physical documents. Digital media should beappropriately sanitized/wiped or destroyed.

Public Information

There are no requirements for public information.

8.2.3.3 Use of Restricted Information

The following applies to how users must interact with Restricted information:

- Users are advised of any Restricted information to which they have beengranted access
- Users must only access Restricted information to perform their job function
- Users must not seek personal benefit, or assist others in seeking personalbenefit, from the use of Restricted or Confidential information
- Users must protect any Restricted information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their jobor the action is approved by their supervisor
- Users must report any suspected misuse or unauthorized disclosure ofRestricted information immediately to their supervisor
- If Restricted information is shared with third parties, such as contractors or vendors, a Confidentiality or Non-disclosure agreement must govern the third parties' use of Restricted information

8.2.3.4 Security Controls for Restricted Data

Restricted data requires additional security controls to ensure its integrity.The Company requires that the following guidelines be followed:

- **Strong Encryption:** Strong encryption must be used for Restrictedinformation transmitted external to the company.
- **Authentication:** Strong passwords are used for access to Restrictedinformation.
- **Physical Security:** Systems that contain Restricted information must besecured logically and physically.
- **Printing:** When printing Restricted information, the user should use best efforts to ensure that the information is not viewed by others or left in publicplaces.
- **Faxing:** When faxing Restricted information, users must use cover sheets that inform the recipient that the information is Restricted. Faxes should be set to print a confirmation page after a fax is sent; and the user should attachthis page to the Restricted information if it is to be stored. Fax machines that

- are regularly used for sending and/or receiving Restricted information mustbe in secured areas.
- **Emailing:** Restricted information must not be emailed outside the companywithout the use of strong encryption.
- **Mailing:** If Restricted information is sent outside the company, the user mustuse a service that requires a signature for receipt of that information.
- **Discussion:** When Restricted information is discussed it should be done innon-public places, and where the discussion cannot be overheard.
- Restricted data must be removed from documents unless its inclusion isnecessary.
- Restricted information must never be stored on non-company-providedsystems.

8.3 Media Handling

8.3.1 Management of Removable Media

The use of removable media (e.g. thumb drives, external hard drives, etc.) is notallowed unless the Office of Information Security provides prior written authorization.

Any information stored on removable media must be classified and labeled as defined in 8.2 Information Classification. The information must also be protectedas defined in the same section (e.g., encryption).

When removable media is no longer required, all information stored on said mediamust be removed and made unrecoverable. Proper disposal procedures must be followed.

All removable media must be securely stored to mitigate the risk of unauthorizedaccess to the stored information.

8.3.2 Disposal of Media

When removable media assets are decommissioned, the following guidelinesmust be followed:

- Any asset tags or stickers that identify the company must be removed before disposal
- Data wiping must be performed upon device removal by DOD level software
- When possible, media containing restricted information should be disposed of securely, by incineration or shredding

8.3.3 Physical Media Transfer

The Company discourages the transfer of information via removable media. Whenthe transfer of information via removable media is unavoidable, the following guidelines must be followed:

- Reliable transport or couriers must be used to transfer the media
- Procedures must be in place to verify the identification of couriers
- Packaging must be sufficient to protect the contents from any physicaldamage
- Logs must be kept identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodiansand receipt at the destination

9.0 Access Control

9.1 Business Requirements for Access Control

9.1.1 Access Control Policy

The Company shall establish and enforce access control procedures. The Companyshall develop role definitions for all employees with access to critical systems and Restricted information. IT shall map role definitions to system access controls andauthorizations. Authorizations shall be granted on a need-to-know basis and in accordance with the Information Classification specifications in 8.2 Information Classification.

The Company shall implement appropriate technical safeguards to prohibit allaccess to Company information, networks, and systems unless specifically authorized through a formal process that validates the business need and is appropriately approved.

The following must be applied when evaluating the business requirements andimplementing supporting access controls:

- Access to IT resources and information must be commensurate with thesecurity requirements of that resource and the classification of data it provides access to.
- Authentication methods used for accessing IT Resources and informationmust be consistent with the Security Controls articulated in the Information Classification standards defined in 8.2 Information Classification.
- Application and data development efforts must define appropriate accesscontrol business requirements as part of the software development process.

9.1.2 Access to Networks and Network Services

Company employees, contractors (with access to Get Event Log LLC systems), and guests (including third parties) shall only be provided access to Company networks and network services for which access has been approved and authorized by management. Access to Company networks and network services shall be granted inaccordance with 9.1 Access Control Policy and on a need-to-know basis.

9.1.3 Access Procedures

All executed privileged functions are captured in logs and sent to Get Event Log LLC's MobileDevice Management solution. Members of the Security team are responsible for monitoring the logs and any alerts received on at least a daily basis. If a potentially malicious event is detected, and incident ticket will be generated, and investigative activities will be performed by members of the Security team and the Incident Response team as appropriate.

9.2 User Access Management

9.2.1 User Registration and De-Registration

The Company shall implement a formal user registration and de-registration process as documented in the Employee Onboarding, Offboarding, and Changeprocedures as documented in the Company Standard Operating Procedures.

All individuals with access to Company information and information systems shall be assigned unique user IDs and passwords to access those information andinformation systems. The principle of least privilege shall be applied to account creation and user authorizations.

User accounts shall be created by IT upon receipt of an approved request frommanagement, as defined in the above procedure.

User accounts shall be de-registered immediately upon termination of the employee, contractor or guest, and/or when there is no longer a need for said useraccount.

9.2.2 User Access Provisioning

The Company shall implement a formal process for user access provisioning anddeprovisioning.

Access shall be granted based on role definitions and role mappings toauthorizations.

All access requests must be reviewed and approved by the requestor's manager. Therequestor's manager and the OIS must approve all exceptions.

9.2.3 Management of Privileged Access Rights

The Company shall assign privileged access rights based on need-to-know and theprinciple of least privilege.

The Company shall assign privileged access rights to a user ID different from theuser credentials used for non-administrative business activities.
Non-administrative tasks should not be completed using the privileged ID.

The use of generic administrative user IDs should be avoided. In instances wherethe use of a generic administrative ID cannot be avoided, the confidentiality of the credentials should be maintained in a secure manner (e.g., through use of an enterprise password vault) and extra care should be given to ensure that passwords are complex and rotated frequently when a privileged user leaves theorganizations or their role results in the user no longer being permitted access tothe generic administrative ID. Single Sign-On which requires username, password, and multi-factor authentication is required in order to gain access to privileged accounts.

9.2.3.1 Shared Account Policies

Guests, anonymous, shared, emergency, and temporary accounts are required to bespecifically authorized prior to use, and activities performed by such accounts arelogged and monitored. The use of shared or generic accounts and passwords shallbe restricted to the extent feasible.

All account types are identified (including individual, shared, system, application, guest, emergency, and temporary accounts), and conditions for group and role membership are established. If used, shared account credentials are modified whenany users are removed from the group.

9.2.3.2 Shared Account Procedure

Get Event Log LLC restricts the use of shared or otherwise anonymous accounts wherever feasible. In instances where shared accounts are required to be used, membership tosuch accounts is restricted to personnel that require such access to complete their job responsibilities. If any users are removed from a shared account, the credentials are modified and the new credentials are communicated to remaining members in the group. All activities performed by shared accounts are logged and logs are transferred and maintained within a centralized logging system.

A listing of all active and inactive accounts is maintained, and account types are documented within the listing. As such, all individual, shared, and service accountsare specifically identified.

9.2.4 Management of Secret Authentication Information of Users

All users shall be trained on the importance of keeping authentication informationconfidential. The Company shall require that users acknowledge understanding ofthis company policy as part of onboarding training and re-acknowledge annually as part of annual Security Awareness Training (see 7.2.2).

Prior to providing a user with new, replacement or temporary user authenticationinformation, the identity of the user should be verified by the support technician. The Company shall establish a process or self-service system to verify the identityof any user prior to providing new, replacement, or temporary credentials.

Temporary credentials should be shared in a secure manner. Sending credentialsin clear text is prohibited. The credentials should be unique and not guessable.
Users should acknowledge receipt of credentials shared with them and besystematically required to reset passwords upon first login.

The Company shall also require that all default credentials and passwords for all systems and software be reset upon installation. Users can reset password through "Forgot Password" self-service password reset. Password resets are performed via a self-service model. Users who have forgotten their password can request a password reset after their identity has been verified. A temporary password is sent to the user's predefined email address, and the user is forced to change the temporary password after its initial use. Temporary passwordsare created by leveraging a random password generator that meets Get Event Log LLC's predefined password parameters.

9.2.5 Review of User Access Rights

The Company shall conduct a review of user access rights for both administrativeand non-administrative users on a quarterly basis. Access reviews shall include review of both the Single Sign On environment (e.g., Active Directory, Radius Server) and systems and applications where user access rights are administered locally (e.g., some AWS Server Instances, Applications leveraging Database Authentication).

The results of quarterly access reviews and associated issues identified as part ofreview shall be documented within help desk tickets and tracked to remediation.

9.2.5.1 Logical Access Review Policy

System owners are responsible for maintaining a current listing of all workforce members (including individuals, contractors, vendors, and business partners) withaccess to information assets (including assets containing covered or otherwise sensitive information). Assigned user IDs are required to be unique to ensure thatredundant IDs are not issued, and activities can be traced to the responsible individual.

User access rights are reviewed after any organizational changes, and on at least a quarterly basis for accounts with general system access. Logical access reviews areconducted at least every 60 days for accounts that have been assigned privileged access rights. Access privileges are adjusted accordingly based on any changes thatoccur.

9.2.5.2 Logical Access Review Procedures

System owners are responsible for maintaining a list of all workforce members withaccess to information assets (including sensitive data). Such lists are updated whenever changes to access occur, and reviews are completed at least quarterly. Aspart of the listing, users are assigned unique IDs which are captured in audit logs totrace activities completed to the responsible individual(s).

User access rights are reviewed by system owners whenever organization changes occur to ensure that (a) access to new resources required in the normal course of business are provisioned, and (b) access to resources no longer required based on the user's new role are removed. Additionally, user access reviews are performed atleast quarterly for accounts with general system access and at least every 60 days for accounts with privileged access rights. Any changes to access rights made basedon the results of logical access reviews are recorded in tickets.

9.2.6 Removal or Adjustment of Access Rights

The access rights of all employees, contractors, vendors, and other external partieswith access to the Company's information systems shall be removed upon termination, upon notification by management of termination of employment, contract or service agreement. Depending on risk factors, access rights to information assets and facilities may be reduced or removed prior to the termination of an individual's employment or other workforce arrangement.
Additionally, automation is leveraged to automatically disable user accounts thathave been inactive for a period of 90 days.

Changes of employment titles, roles or responsibility should result in removal oradjustment of employee access rights to reflect his/her updated role.

9.3 User Responsibilities

9.3.1 Use of Secret Authentication Information

End User Authentication Information

The sharing of usernames and passwords is strictly forbidden. Users should avoidwriting down authentication information and leaving it in unsecured places (e.g., sticky notes with username and passwords left in the open on desks).

The Company shall implement Single Sign-On which requires username, password, and multi-factor authentication before permitting any access to company resources.

Passwords shall not be included in automated log-on processes.

9.3.1.1 Password Requirements

Construction

The best security against a password incident is simple: following a sound passwordconstruction strategy. The organization mandates that users adhere to the followingguidelines on password construction:

- Passwords must be at least 10 characters
- Passwords must be comprised of a mix of letters, numbers, and specialcharacters (punctuation marks and symbols)
- Passwords must be comprised of a mix of upper and lower-case characters
- Passwords should not be comprised of, or otherwise utilize, words that canbe found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e.,qwerty)
- Passwords should not include "guessable" data such as personal informationThe Senior Security Program Manager reviews a list of passwords that have been commonly used or previously compromised at least twice per year and updates the administrative policies accordingly.

Further, users are prohibited from saving passwords to be used for automated log-on.

Confidentiality

Passwords are considered Restricted data and must be treated with the samediscretion as any of the organization's proprietary information. The followingguidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (e.g., co-workers,supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured (e.g.,post-it on a computer monitor, under a keyboard, etc.)
- Users must not disclose or send passwords via email or any other electronicmeans (e.g., intranet, ticketing system, etc.)

9.4 System and Application Access Control

9.4.1 Information Access Restriction

Access restrictions shall be based on business requirements and defined withinroles as defined in accordance with the Access Control Policy (see 9.1.1).

All business applications developed or procured by the Company must adhere to theCompany's access control requirements.

Examples of access restrictions include:

- Support for logical access control which enforces Company policy requirements for securing secret authentication data, password complexityand encryption requirements.
- Support for controlling access to data based on predefined user role and therights associated with those roles (e.g., read, write, execute).
- Limiting the information contained in outputs from the application based onuser role and rights associated with those roles.
- Secure design to prevent unauthorized users from modifying the application configurations and functionality, unintended communications with other systems and applications, or unauthorized modification of other systems, applications, or data.

9.4.2 Secure Log-On Procedures

The Company shall only implement systems and applications to meet businessrequirements which provide for log-on procedures which adhere to the accesscontrol requirements as required by this policy, including:

- Provides for authenticating the identity of a user based on assigned usercredentials.
- Limits access and abilities of a user in accordance with their assigned userrole.
- Enforces password complexity requirements and properly manages usercredentials including secure management and transportation of secret authentication information in accordance with Company standards (e.g., hashing and encryption requirements).
- Include security mechanisms to prevent brute force log-on attempts, log successful and unsuccessful attempts, mask user passwords, and not presentthe user with any information that might aid in circumventing the security controls in place (e.g., error condition details related to failed log-in attempts).

Systems and applications implemented to meet business requirements should bedesigned to minimize the opportunity for unauthorized access and prevent the disclosure of information to unauthorized users.

9.4.3 Password Management System

A password management system shall be implemented by the Company which enforces the use of assigned user IDs and passwords to provide for identificationand authentication of users accessing information systems and assets.

The password management system must enforce the security requirements of theorganization and include the following attributes at a minimum:

- Allow a user to establish their own password without the aid of another user.
- Securely store the password in an indecipherable and irreversible format toprotect the confidentiality of the password and meet the hashing complexityrequirements of the Company (see 10.1).
- Enforce the Company's password complexity requirements (see 9.3.1.1).
- Maintain a record of previously used passwords to enforce the Company'spassword re-use restriction policy.
- Prevent unauthorized access and theft of user password hashes, and storeand transmit passwords in a secure fashion.

As part of the onboarding process, users are provided an automated email when thenew account is established. Only users with the provided link within the email can establish the password. Users are forced to establish passwords upon initiallogin and the password must meet Get Event Log LLC's pre-defined password parameters.
Get Event Log LLC uses self-service password resets that establish identity prior to reset.

9.4.4 Use of Privileged Utility Programs

Use of privileged utility programs shall be restricted unless there is a justifiedbusiness need.

9.4.5 Access Control to Program Source Code

Application source code and source code libraries shall be centrally managed andcontrolled within a system that allows limiting authorized personnel to prevent unauthorized or unintended changes as well as maintain the confidentiality of intellectual property.

The source code management system should allow for logging all accesses of source code libraries. Modification and transfer of source code libraries should besubject to strict source code change control procedures (see 14.2.2).

10.0 Cryptography

10.1 Cryptographic Controls

10.1.1 Policy on the use of Cryptographic Controls

Encryption, also known as cryptography, can be used to secure data while it is stored at rest or being transmitted. All restricted information must be encryptedin transit and at rest.

10.1.1.1 Applicability of Encryption

Data while stored: This includes any data located on company-owned or company-provided systems, devices, media, etc. Examples of encryption optionsfor stored data include:

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications
- Database encryption

Data while transmitted: This includes any data sent across the company network, or any data sent to or from a company-owned or company-providedsystem. Types of transmitted data that can be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications/databases

10.1.1.2 Acceptable Encryption Algorithms

Information security industry standard and non-proprietary encryption algorithmsare permissible. However, all restricted data must use at least Advanced EncryptionStandard (AES) 128-bit strength encryption if applicable. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not beensubjected to public inspection and its security cannot be assured.

For business applications that require the storage of user passwords within the application or locally, passwords should be hashed leveraging a hashing algorithm

appropriate for securing passwords with a key length of at least 128-bits (see NISTpublication FIPS 800-107 and FIPS 800-4).

Where possible, password hashes should be salted to increase the difficulty ofcracking the hashes.

10.1.1.3 Legal Use of Encryption

Some governments have regulations applying to the use and import/export of encryption technology. The Company must conform to encryption regulations ofthe applicable government.

The company specifically forbids the use of encryption to hide illegal, immoral, orunethical acts.

10.1.2 Key Management

Key management is critical to the success of an implementation of encryption technology. The following policies apply to the company's encryption keys and keymanagement:

- Management of keys must ensure that data is available for decryption whenneeded
- Keys must be backed up
- Keys must be locked up
- Keys must never be transmitted in clear text
- Keys must be considered Restricted information
- Keys must not be shared
- Physical key generation materials must be destroyed within 5 business days
- Keys must be used and changed in accordance with the Company passwordpolicy
- When user encryption is employed, minimum key length is 15 characters

11.0 Physical and Environmental Security

Physical access control to the following Company facilities must be in place to detect, prevent, and minimize the effects of unauthorized or unintended access tothese areas. Authorization is based on the principle of least privilege according tojob responsibilities. If applicable, buildings and floors

- Networking closets and wiring closets
- Power and emergency backup equipment
- Operations and control areas
- Any other Company controlled facilities

Please note that this policy covers the physical security of the company's Information Technology infrastructure and does not cover the security of non-ITitems or the important topic of employee security.

Third-party data center providers shall manage physical security related to data centers. Requirements shall be outlined in contracts with the associated data centerproviders.

11.1 Secure Areas

The Company shall ensure critical or sensitive information processing facilities arehoused in secure areas, protected by defined security perimeters, with appropriatesecurity barriers and entry controls.

11.1.1 Physical Security Perimeter

The company shall maintain standard security controls including locks on exteriordoors and alarm systems to secure the company's assets. In addition to this the company provides security in layers by designating different security zones withinthe buildings. Security zones include:

Public Zones

- This includes areas of the building or office that are intended for public access.
- Access Restrictions: None
- Additional Security Controls: None
- Examples: Lobby, common areas of building

Company Zones

- This includes areas of the building or office that are used only by employees andother persons for official company business.
- Access Restrictions: Only company personnel and approved/escorted guests.
- Additional Security Controls: Additional access controls shall be used, such askeys, keypads, keycards, or similar devices, with access to these areas logged when possible.
- Examples: Hallways, private offices, work areas, conference rooms.

Private Zones

- This includes areas that are restricted to use by certain people within the company,such as executives, scientists, engineers, and IT personnel, for security or safety reasons.
- Access Restrictions: Only specifically approved personnel shall be allowedaccess to Private Zones.
- Additional Security Controls: Additional access controls must be used, suchas keys, keypads, keycards, or similar devices. Access to these areas must be logged.

- Examples: Executive offices, lab space, network rooms, computer rooms, HRrooms, financial offices, and secure storage areas.

11.1.2 Physical Entry Controls

Access controls are necessary to restrict entry to the company premises and security zones to only approved persons. The Company shall secure physical entrypoints with keys, keypads, keycards, or similar devices.

11.1.2.1 Keys & Keypads

The use of keys and keypads are acceptable. These security mechanisms are themost inexpensive and are the most familiar to users.

11.1.2.2 Keycards

The Company requires that keycards be used for all user access controls. The company uses this technology to enforce security zones and provide employees theleast amount of access required to do their jobs.

Schedules must be set to forbid off-hours access (unless required by job role), andforbid users from accessing a security zone where they are not authorized. If a keycard is lost or stolen it must be immediately reported and disabled. If an employee is terminated or resigns, that user's access must be disabled, and the keycard returned.

11.1.2.3 Alarm System

The company shall use a professionally monitored alarm system at all companylocations. The system shall be monitored 24x7, with Company personnel beingnotified if an alarm is tripped at any time.

11.1.3 Securing Offices, Rooms and Facilities

11.1.3.1 Entry Security

It is Company policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general but is particularly true for minimizing risk to Company systems and data. The guidelinesbelow are intended to be specific to the Company's information technology assets and should conform to the Company's overall security policy.

11.1.3.2 Use of Identification Badges

The Company has established the following guidelines for the use of ID badges.

- **Employees:** ID badges are required and must be always displayed whileon company premises.
- **Non-employees/Visitors:** Visitor badges are required.
  Users must a report lost or stolen badge immediately to their supervisor. A temporary badge may be utilized in such cases until a badge can be regenerated.

- Initial badge generation shall be completed only at the direction of Human Resources for new hires or users changing jobs. Users must show photoidentification for identity verification.

11.1.3.3 Sign-in Requirements

The Company must maintain a sign-in log (or similar device) in the lobby or entryarea. Visitors are required to sign in upon arrival. The log must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

11.1.3.4 Visitor Access

Visitors must be given only the level of access to Company premises that is appropriate to the reason for their visit. After checking in, visitors must be escortedunless they are considered "trusted" by the Company.

11.1.4 Protecting Against External and Environmental Threats

The Company shall ensure that equipment be located or protected to reduce therisks from environmental threats, hazards, and opportunities for unauthorized access.

11.1.5 Working in Secure Areas

Company personnel shall be made aware that the existence of, or activities within, asecure area on a need-to-know basis.

Unsupervised working in secure areas should be avoided both for safety reasonsand to prevent the opportunities for malicious activities.

Vacant secure areas must be physically locked and access to the secure areas mustbe periodically reviewed.

Photographic, video, audio, or other recording equipment such as cameras in mobiledevices should not be allowed unless authorized.

11.1.6 Delivery and Loading Areas

Access to delivery and loading areas from outside of the building must be restrictedto identified and authorized personnel.

All deliveries must be inspected and examined for explosives, chemicals, or otherhazardous materials before it is moved from a delivery and loading area.11.2 Equipment.

11.2.1 Equipment Siting and Protection

The Company outsources all their datacenter operations to a third-party. Third-party requirements for equipment sitting shall be defined in the contractsgoverning the relationship with the third-party datacenter.

Company equipment utilized to process sensitive information shall be positionedcarefully to reduce the risk of unauthorized users viewing the information. This includes systems in the Private Zones and any systems used for work-from-home.

11.2.2 Supporting Utilities

The Company shall implement supporting utilities to ensure power conditioning and backup power for systems in data and network closets. All power conditioningand backup power for datacenter facilities shall be the responsibility of the
third-party datacenter providers and shall be governed by the contract in place withsaid providers.

11.2.3 Cabling Security

The Company shall implement access controls to prevent the unauthorized accessdata and network closets and access points. All datacenter cabling requirements shall be the responsibility of the third-party datacenter providers and shall be governed by the contract in place with said providers.

11.2.4 Equipment Maintenance

Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications. Authorized maintenance personnel shall carryout repairs and service equipment and records shall be kept of all maintenance activities. This applies to end-user systems and systems contained within data andnetworking closets. All datacenter systems maintenance requirements shall be theresponsibility of the third-party datacenter providers and shall be governed by thecontract in place with said providers.

Removal of Assets

Appropriate handling Standards shall be developed for each type of data, based onclassification, including the data introduction, transfer, removal, and disposal.

11.2.5 Security of Equipment and Assets Off-Premises

The Company outsources all their datacenter operations to a third-party.
Third-party requirements for securing equipment shall be defined in the contractsgoverning the relationship with third-party datacenters.

Employee equipment taken off-site must be always secured as defined in the 6.2Mobile Devices and Teleworking, any theft or unauthorized access to employee equipment off-site must be reported to IT immediately.

11.2.6 Secure Disposal or Re-Use of Equipment

Hardware must have all data and application software irreversibly removed prior todisposal or re-use.

Procedures for the disposal and re-use of equipment shall be defined by IT andincluded in the Standard Operating Procedures manual.

All guidelines outlined in 8.2.3 Handling of Assets must be adhered to as appropriate to the classification of data stored on the hardware that is beingdisposed of or reused.

11.2.7 Unattended User Equipment

Company issued computer assets are assigned owners. Owners are responsible forthe safekeeping and reasonable care of company assets assigned to them, as such purposeful or negligent handling or use that constitutes to the defacing or destruction of equipment is considered vandalism and prohibited. Users must adhere to the following guidelines:

- Active sessions should be terminated when finished, unless they can be secured by an appropriate locking mechanism, such as a password protectedscreen saver.
- Users must log-off from applications or network services when no longerneeded or in use.
- Users must take care to secure computers or mobile devices from unauthorized use by a key lock or an equivalent control when not in use.
- Users must not leave computers unattended in public places.

11.2.8 Clear Desk and Clear Screen Policy

A clean desk and clear screen policy helps to safeguard against unattended target forprying eyes and unauthorized access. Therefore, Company workforce must adopt the clean desk and clear screen policy and adhere to the following guidelines to safeguard their computer systems:

- Users must lock their computers when their workstation is unattended.
- All restricted or confidential information must be locked in a drawer or filecabinet at the end of the day.
- Upon disposal, restricted or confidential documents must be shredded.
- Whiteboards containing restricted or confidential use information must beerased.
- IT personnel are responsible for configuring workstations and other company-issued devices to automatically time-out after 15 minutes ofinactivity.

A time-out mechanism has been implemented for all publicly positioned systems topause the session screen after two minutes of inactivity and close network sessionsafter 30 minutes of inactivity.

12.0 Operations Security

12.1 Operational Procedures and Responsibilities

The Company shall implement appropriate Standard Operating Procedures to manage and operate all information processing facilities in a secure manner and inaccordance with the Information Security Policy.

12.1.1 Documented Operating Procedures

Operating procedures shall be documented in the Company Standard OperatingProcedure manual. This document shall serve as the central repository for all procedures related to developing, managing, and maintaining the information systems of the Company.

IT shall have the primary responsibility for the creation and maintenance of the Company Standard Operating Procedure manual. All relevant parts of the organization shall be responsible for documenting related procedures and providingthen to IT for inclusion in the Company Standard Operating Procedures manual.

12.1.2 Change Management

The Company shall manage changes to production systems through a Change Management process as defined in the Company Standard Operating Procedures manual. All changes to production systems shall be requested, evaluated, and approved by a Change Advisory Board. The specific requirements for changes shallinclude:

- Changes must be requested by the system owner
- Changes must be evaluated for operational and security risk, and these risksmust be documented in the change request
- Changes must be tested by QA or peer reviewed prior to approval and implementation
- Rollback procedures must be defined as part of the change request
- All changes must be approved by the CAB before implementation
- Emergency changes must be approved according to the approval processesdefined in the Change Management process
- IT shall maintain a change log of all changes to production systems

12.1.3 Capacity Management

The Company shall implement system planning and acceptance procedures, including testing, to minimize the risk of system failures due to lack of capacityplanning required for an acceptable level of system performance.

12.1.4 Separation of Development, Testing and Operational Environments

The company shall maintain separate environments for development, testing andproduction.

Development Environment

Access to the Development environment shall be restricted to developers of the applications. This includes web development, database development, data science development, API development, etc. The Development environment shall be used todevelop application functionality, database capabilities, data science products, etc. The use of production data is prohibited in the Development environment.

Testing Environment

Access to the Testing environment shall be restricted appropriately based on Company need. The Testing environment shall be used to test production changesprior to deployment to the production environment. The use of production data isprohibited in the Testing environment.

Production Environment

Access to the Production Environment shall be appropriately restricted to individuals who require access to manage and maintain the production systems. Developers shall not have direct access to the Production environment without priorwritten approval by the OIS. Changes to the Production environment shall be governed by the Change Management policy and procedures defined in 12.1.2 Change Management.

12.2 Endpoint Protection

12.2.1 Anti-Virus and Anti-Spyware Policy

Get Event Log LLC shall ensure that anti-virus and anti-spyware are installed, operating, and updated on all end-user devices to conduct periodic scans of the systems to identifyand remove unauthorized software. A network-based malware detection system shall be used for server environments in which host-based antivirus and anti-spyware solutions are not used.

12.2.2 Antivirus and Anti-Spyware Procedure

The CTO is responsible for ensuring that anti-virus and anti-spyware software is installed on all end-user devices as part of the provisioning process. The antivirus /anti-spyware software on endpoint devices will be monitored via the mobile devicemanagement (MDM) solution, and antivirus scans are required to be run in real-time of the computer and its activities along with periodic scanning of thecomputer. Virus definitions are required to be updated on at least a daily basis.

The Director of Development Support is responsible for ensuring that antivirus and anti-spyware software are installed on all production servers as part of the predefined configuration standards. Scans shall be run on the production servers daily and identified malware shall be investigated. Virus definitions are required to be updated on at least a daily basis. The MDM solution will notify the Director of Development Support on any machine that does not meet these requirements.

If the company does not own the equipment, the user must implement technologycontrols to protect against malware, viruses, and other malicious software prior togaining access within the Get Event Log LLC VPN.

12.2.3 Audit Scan Logs

Device audits of the antivirus policy compliance from the MDM solutions will notifythe Director of Development Support when out of compliance. Out of compliance means antivirus software is out of date or not working properly. Scan logs of antivirus software are not documented or retained by antivirus software.

The Senior Security Program Manager is responsible for ensuring these notificationsof policy audits are captured and retained for a period of at least one year. The logs will capture all negative checks performed for a given scan. Logs of the audit scans will be retained within the managed console solution for a period of 365 days.

12.2.4 Malicious Code Protection

Protection against malicious code shall be based on malicious code detection andrepair software, security awareness, and appropriate system access and change management controls.

Director of Development Support is responsible for ensuring that antivirus andanti-spyware software is installed on all employer-issued devices and on all
production servers. Additionally, on non-employer owned devices, all machines willbe compliant with protection prior to gaining access to Get Event Log LLC's network. The Director will be alerted of identified malware in real-time and will investigate the alerts as needed.

Senior Security Program Manager is responsible for ensuring that security awareness training is completed for all new hires as part of the onboarding process and on an annual basis thereafter. The security awareness training materials includeinformation on how to identify and report actual or suspected malware.

System owners are responsible for ensuring that role-based access is enforced inaccordance with the Access Control Policy.

System owners are responsible for ensuring that the change management processdefined in Change Management (12.1.2) is enforced. System owners are also responsible for ensuring that changes are documented, approved, and tested priorto migration into the production environment.

12.2.5 Browser Setting Policy and Procedure

Automated controls shall be in place to authorize and restrict the use of mobile code.

The Director of Development Support is responsible for ensuring the device isconfigured to restrict the use of mobile code (Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, flash animations, etc.) unless use of the code isformally documented and accepted by the Chief Technology Officer.

12.3 Backup

12.3.1 Information Backup

Get Event Log LLC maintains a formal definition of the level of backup required for each system. Documentation includes information detailing how each system will be restored, the scope of the data to be imaged, frequency of imaging, and duration ofretention based on applicable contractual, legal, regulatory, and business requirements.

Backup services provided by third parties are required to be dictated by servicelevel agreements (SLAs) that include detailed protections to control the confidentiality, integrity, and availability of backup information.

12.3.1.1 Identification of Critical Data

The Company shall identify the most critical data to its organization. Critical datashall be identified so that it can be given the highest priority during the backup process.

12.3.1.2 Data to be Backed Up

The backup policy must balance the importance of the data to be backed up with theburden such backups place on the users, network resources, and the backup administrator. Data to be backed up shall include:

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s), aswell as these servers operating systems and logs. It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers,source code repositories, etc.

- Logs and configuration of network devices such as switches, routers, etc.

12.3.1.3 Backup Frequency

The Company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burdenon the users, network, and backup administrator.

- Incremental Backups: every day
- Full Backups: every 7 days

12.3.1.4 Backup Storage

The Company uses online media as provided by Amazon Web Services, Microsoft Azure, and Google Cloud (depending on the appropriate deployment), to store system backups. Long-term storage of backups may utilize Amazon S3, or Glacier orsimilar storage services.

12.3.1.5 Backup Retention

The Company has determined that the following will meet all requirements (notethat the backup retention policy must confirm to the company's data retention policy and any industry regulations, if applicable):

- Incremental Backups must be saved for one week.
- Full Backups must be saved for 1 month

12.3.1.6 Restoration Procedures & Documentation

The data restoration procedures must be documented in the Company Standard Operating Procedure manual. Documentation must include who is responsible forthe restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration.

12.3.1.7 Restoration Testing

Backup restoration shall be tested for all systems at least quarterly.

12.4 Logging and Monitoring

The Company shall maintain logs and perform log reviews at a regular interval asdefined in Company Standard Operating Procedures. All applicable legal requirements related to monitoring authorized access and unauthorized access attempts must be met.

Automated systems deployed throughout the company's environment are used to monitor key events and anomalous activity, as well as analyze system logs. Identifiedirregularities or anomalies, that may be indicators of a system malfunction or compromise, trigger notifications to appropriate team members to investigate.

Monitoring activities include the following:

- privileged operations,
- authorized access or unauthorized access attempts, including attempts toaccess deactivated accounts,
- system alerts or failures

Auditing and monitoring systems employed by the company should support auditreduction and report generation.

Company monitoring should include inbound and outbound communications aswell as file integrity monitoring on critical system files.

The CTO will oversee the implementation of monitoring solutions related to the company's production systems in AWS, Microsoft Azure and GCP. Native services and external tools should be configured to monitor and alert the security and engineering teams to any suspicious or anomalous activity, based upon policy requirements. Where feasible, the CTO will leverage native reporting functionalityin monitoring tools to assist with audit burden reduction.

Critical system files, as defined by the CTO and IRC, must be monitored for changes.When feasible a file integrity monitoring (FIM) solution must be implemented. In the absence of a FIM solution, compensating controls must be implemented to mitigate the risk of someone altering critical system files without approval.

12.4.1 Event Logging

Operating Systems, Applications, Network Devices, and other critical systems anddevices shall log the following information when possible:

- User IDs
- System activities
- Dates, times, and details of key events - e.g., log on and log off
- Device identity or location if possible and system identifier
- Records of successful and rejected system access attempts
- Records of successful and rejected data and other resource access attempts
- Changes to system configuration
- Use of privileges
- Use of system utilities and applications
- Files accessed and the kind of access
- Network addresses and protocols
- Alarms raised by the access control system

- Activation and deactivation of protection systems such as anti-virus systems and intrusion detection systems
- Records of transactions executed by users in applications
- Faults and malfunctions

12.4.2 Protection of Log Information

Access controls shall be implemented to adequately protect log information fromunauthorized access and/or tampering.

12.4.3 Administrator and Operator Logs

System administrator and system operator activities shall be logged, and the logsmust be protected and regularly reviewed.

12.4.4 Clock Synchronization

System clocks for critical systems shall be synchronized via Network Time Protocol.

12.5 Control of Operational Software

12.5.1 Installation of Software on Operational Systems

All software installation on operational systems must follow the Company change control procedures as outlined in 12.1.2 Change Management.

IT shall maintain Standard Build procedures for all end-user systems. Software on end-user systems shall be installed based on user role. Installation of unapproved software is prohibited.

Architecture shall maintain Standard Build procedures for all production systems. Installation of additional libraries or software on production systems is prohibited unless approved by the CSO.

12.6 Technical Vulnerability Management

12.6.1 Management of Technical Vulnerabilities

The Office of Information Security ("OIS") shall conduct or oversee quarterly vulnerability scans of the internal and external networks. The results of these scans shall be reviewed and prioritized by the Information Security Risk Council (ISRC). Vulnerabilities must be remediated based on the determination of the ISRC.

12.6.2 Restrictions on Software Installation

Installation of unapproved or unlicensed software or libraries is expressly prohibited. All software installations must be approved by IT, Architecture, and/or the OIS. Only authorized equipment (Tablet or Laptop) may access enterprise or

production application networks or systems. The Office of Information Security is responsible for implementing appropriate access controls to prevent non-approved devices from accessing non-approved resources and applications. Solutions may include restrictions via VPN, certificate-based authentication, and Network Access Control (802.1X).

12.6.2.1 Vendor Supplied Software Procedure

Management shall review the use of vendor supplied software on at least an annual basis to ensure that current versions of the software are in use and any security updates available have been implemented on operational systems.

Vendor supplied defaults should always be reset to a value specific to the organization. This may include default administrative passwords, encryption settings, logging, filtering of ports and availability of services.

12.6.2.2 Blacklisted Software Policy and Procedure

The Company must employ a means of identifying unauthorized (blacklisted) software on the information system, including servers, workstations, and laptops, and employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system. The IRC shall review and update the organization's list of unauthorized (blacklisted) software periodically but no less than annually.

The organization shall prevent program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage.

The IRC is responsible for creating and maintaining the organization's list of unauthorized software; the IRC will review this list annually and document their review in the organization's ticketing system.

The Director of Development Support is responsible for implementing technical controls (software) to identify and prevent the use of blacklisted software on all information systems, to include servers, workstations, and laptops. As part of the control, any implemented solution will also include an allow-all, deny-by-exception policy to prohibit the execution of blacklisted software on the information system.

12.7 Information Systems Audit Considerations

12.7.1 Information Systems Audit Controls

The Company shall develop a program to perform technical audits and tests of information systems. The scope of technical audits should be agreed to with appropriate members of management and the scope of technical audit projects agreed to and controlled.

Audit tests and access granted to information systems and production data should be limited to read only access. Else, auditors should only be allowed access to isolated copies of system files, which should be properly secured and controlled.

Technical audit tests (e.g., penetration testing) with the potential to impact systemavailability should be performed outside of normal business hours.

13.0 Communications Security

13.1 Network Security Management

Get Event Log LLC's secure gateways (firewalls) (i) enforce security policies; (ii) are configured to filter traffic between domains; (iii) block unauthorized access; (iv) areused to maintain segregation between internal wired, internal wireless, and externalnetwork segments, including DMZs, and (v) enforce access control policies for each of the domains. Unless the risk is identified by the system owner, sensitive systems are logically isolated from non-sensitive systems.

For any public-facing applications that are not web-based, Get Event Log LLC has implemented a network-based firewall specific to the application. If the traffic to thepublic-facing application is encrypted, the device either sits behind the encryption or can decrypt the traffic prior to analysis.

The ability of users to connect to the internal network is restricted using a deny-by-default and allow-by-exception policy at managed interfaces according tothe access control policy and the requirements of its business applications.

Routing controls are implemented through security gateways used between internaland external networks.

A network diagram is maintained and is updated whenever network changes occur,and at least annually.

The Director of Development Support is responsible for maintaining the firewall rulesets. The firewall rule sets are reviewed at least twice per year, and updates are made to the rule sets on an as-needed basis. Get Event Log LLC utilizes access control lists (ACLs) to restrict access to system resources in accordance with the principle of least privilege. Only authorized connections are permitted, and all other connectionsare explicitly restricted. ACLs are also utilized to perform segmentation of the network. Systems containing sensitive information (PII, PHI, etc.) are logically segregated from non-sensitive systems.

Get Event Log LLC uses a next-generation firewall, which can utilize SSLdecryption to properly analyze and manage network traffic.

The Senior Security Program Manager is responsible for maintaining the network diagram and for reviewing the network diagram at least twice per year. Updates tothe diagram are made whenever a relevant change to the system occurs.

13.1.1 Network Controls

The company shall implement controls and procedures to manage and control networks and safeguard the confidentiality and integrity of data passing over thenetwork and residing on systems connected to the network.

Responsibility for management of networking equipment shall be established. Operational responsibility for networks should be segregated from end users of the Information Systems. Roles with responsibility for the management of networking equipment and the Information System shall be clearly defined by management (see6.1.1).

Systems connected to the network should be authenticated and the connection ofsystems to the network should be restricted and controlled.

Logging and monitoring of networking equipment should be implemented to enablerecording and detection of events relevant to information security.

13.1.2 Security of Network Services

Security requirements, service levels and management requirements should bedefined for all network services within Service Level Agreements (SLA) for bothoutsourced solutions and in-house provided services. The right to audit service providers should be agreed to with service providers and included within SLAs.

The ability of the Network Service provider to provide services in accordance withService Level Agreements and in adherence with the Company's security requirements should be assessed at least annually. Assessments may include inspection of third-party audit reports or through implementation of an in-house audit.

13.1.3 Segregation in Networks

The Company shall segregate Information System resources into separate networksor domains based on trust levels and function. The perimeter of each of these domains must be well defined with access between different network domains restricted using a gateway (e.g., firewall, router).

Access through gateways shall be defined based on the business and security requirements of each domain and adhere to the requirements defined within theaccess control policy (see 9.1.1).

All wireless networks must be considered highly sensitive, external connections with access segregated from internal networks until access passes through a gateway, in accordance with access control and network controls policies (see 9.1.1 and 13.1.1).

13.1.4 Web Application Firewall Policies and Procedures

For any public-facing web applications, application-level firewalls shall be implemented to control traffic.

The Director of Development Support is responsible for installing web application firewalls (WAFs) for any public-facing web applications. The WAFs are configured to filter, monitor, and block HTTP traffic to and from public-facing web applications.

13.2 Information Transfer

13.2.1 Information Transfer Policies and Procedures

The transfer of customer/client data, proprietary information, or Personally Identifiable Information (PII) over unencrypted methods is strictly prohibited and is classified as Restricted (see 8.2.1).

All transfer of customer/client data, proprietary information, or Personally Identifiable Information (PII) must only take place over pre-established, secure channels (e.g., SFTP, VPN, SSL/TLS) which have been approved by an appropriatemember of management.

Information transfer services must comply with any legal requirements.

13.2.2 Agreements on Information Transfer

Customer agreements and contracts should address the secure transfer of information classified as Restricted, which includes customer/client data and Personally Identifiable Information (PII).

These secure transfer agreements should incorporate the following:

- management responsibilities for controlling and notifying transmission, dispatch and receipt of classified information.
- procedures to ensure traceability and non-repudiation.
- minimum technical standards for packaging and transmission.
- escrow agreements.
- courier identification standards.

- responsibilities and liabilities in the event of information security incidents, such as loss of data.
- use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of
- the label is immediately understood, and that the information is appropriatelyprotected (see 8.2.1);
- technical standards for recording and reading information and software.
- any special controls that are required to protect sensitive items, such as cryptography.
- maintaining a chain of custody for information while in transit.
- acceptable levels of access control.

The Legal team maintains and periodically updates contracts/agreements that contain Get Event Log LLC's terms and conditions related to use of the system(s). The contracts define security and privacy related controls that are required to be implemented prior to organization-controlled information being transmitted toexternal information systems. System owners are responsible for ensuring that applicable third parties execute Get Event Log LLC's relevant contracts prior to sensitivedata being accessed or transmitted.

Contracts/Agreements maintained with customers/third parties are required to address the following topics, at a minimum:

- Rights and obligations of Get Event Log LLC and external parties
- Acceptance of responsibilities and liabilities for all parties executing the agreement
- A description of security and privacy-related requirements and obligations (including requirements to address information security risks identified as part of the due diligence process)
- Indemnification clause

Service level agreements are required to be maintained between Get Event Log LLC andthird parties where an agreed service arrangement exists. The service level agreements must address the following topics, at a minimum:

- Liability of all parties involved in the agreement
- Pre-defined service level definitions, identifying the level of service to be provided, including agreed-upon metrics
- Security and privacy-related control obligations

The public shall have access to information about Get Event Log LLC's security and privacyactivities. Additionally, the public shall have a means to communicate with Get Event Log LLC's Chief Technology Officer and Data Protection Officer (DPO).

Get Event Log LLC's public-facing Privacy Policy is reviewed annually and maintained by theDPO.

13.2.3 Electronic Messaging

Electronic messaging refers to both the one to one and many to one communication of information and may include email, fax, SMS, instant messaging, social media, andonline forums.

The transfer of information classified as Restricted via electronic messaging is prohibited unless expressly authorized by senior management. All information classified as Restricted must be transmitted via secured methods which provide the following:

- protection of the information from unauthorized access, modification or denial of service (i.e., confidentiality, integrity and availability);
- assurance of correct addressing and transportation of the message.
- adherence with contractual and legal obligations applicable to the organization.

All transfer of information classified as Confidential must only take place over the following approved electronic messaging systems/protocols:

- corporate email service,
- corporate instant messaging services.

13.2.4 Confidentiality or Non-Disclosure Agreements

Confidentiality or non-disclosure agreements between the Company, its customers, employees, and other external parties must protect confidential information using legally enforceable terms.

Agreements shall take into consideration the nature of the relationship the Company has with the other party and define its permissible access to confidential information.

Confidentiality and non-disclosure agreements shall address the following elements at a minimum:

- A definition and identification of what is considered confidential within the agreement.
- The duration of the agreement.

- Required actions when an agreement is terminated (e.g., steps for disposing ofor returning the confidential information);
- A statement of ownership of the confidential data, which may include PII, trade secrets, or intellectual property, and how this relates to the protection ofconfidential information.
- The permitted use of the confidential information and a statement of the rights of the signatory to use the confidential information.
- A process for reporting the unauthorized disclosure of confidential information.
- The expected actions to be taken in the event of a breach of the confidentiality or non-disclosure agreement.

All confidentiality and non-disclosure agreements must comply with all applicable laws and regulations.

Confidentiality and non-disclosure agreements should be reviewed at least annually to identify expired agreements, detect potential instances of non-compliance, or when changes occur which may affect the requirements of this policy.

14.0 System Acquisition, Development and Maintenance

14.1 Security Requirements of Information Systems

14.1.1 Information Security Requirements Analysis and Specifications

A formal testing and acquisition process should be developed so that a security assessment may be completed prior to the acquisition of new information systems of as part of the functional requirements development phase for information system enhancements, to ensure that these systems adhere to the requirements of the Information Security policy.

Information security requirements for new information systems or enhancements to be developed for existing information systems should consider at a minimum:

- Identification and authentication requirements of users.
- Logical access control and segregation of duties requirements.
- Technical requirements to properly secure and managing data interacting with the information system, based on the Data Classification policy.
- Transaction logging and monitoring requirements.

Contracts with suppliers should address the identified security requirements. If a proposed product fails to meet the Company's specified requirements,

the risk introduced and mitigating controls should be reconsidered prior to the acquisition of the product.

14.1.2 Securing Application Services on Public Networks

Company and customer information involved in the Company's application services being transmitted over the published internet shall be protected from unauthorized disclosure and ensure the integrity of the data. The data must also be managed in accordance with the requirements of the Data Classification policy (see 8.2.1).

Technical controls related to company and customer data being transmitted over the public internet must address the following at a minimum:

- The identity of the recipient must be authenticated (preferably using public key cryptography and digital signatures);
- Terms of use must be established with partners and third parties receiving company and customer data.
- Confidentiality of data must be ensured leveraging a data encryption protocol which adheres to the minimum data encryption requirements as established in the Information Security policy (see section 10).
- Integrity of data must be ensured through implementation of a protocol that allows for data integrity checks (such as TLS) or by using other data integrity checking mechanisms such as a checksum.

Access rights between Get Event Log LLC's applications and third-party applications are restricted using Single Sign-on (SSO). For further information regardingthe SSO, please refer to section 9.3.1 of this policy.

14.1.3 Protecting Applications Services Transactions

Application service transactions both internal or external of the Company's network should be protected from incomplete transmissions, misrouting, unauthorized disclosure, unauthorized duplication or replay and unauthorized alteration.

All technologies and protocols implemented by the Company shall adhere to the requirements of the Information Security policy, including but not limited to the following:

- Data Classification Policy (see 8.2)
- Logical Access (see 9.0)
- Data Encryption (see 10.0)
- Network Security (see 13.1 and 13.2)
- Data Integrity and Confidentiality (see 13.1)

14.2 Security in Development and Support Processes

14.2.1 System Integrity Policies and Procedures

System and information integrity requirements shall be developed, documented, made available to personnel, reviewed, and updated at least annually.

The system shall check for the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. For software developed in-house, Get Event Log LLC utilizes explicit error checking for all input, including for size, data type, and acceptance ranges or formats.

Product owners are responsible for maintaining system and information integrity requirements for all systems. The requirements are reviewed at least annually, and updates are made as appropriate. For any new projects, integrity requirements must be defined within the specification documentation.

Applications utilized by Get Event Log LLC must leverage input checks as appropriate (e.g., value limit controls, completeness controls, data validation checks, etc.) to ensure that data is accurate, complete, valid, and authentic. Additionally, as part of system processing potential errors are automatically flagged and communicated to relevantpersonnel via exception reports. Identified issues must be accepted or resolved for processing to be completed.

14.2.2 Secure Development Policy

Establishing secure software development processes are essential to building a service, application, and environment.

The Company shall establish a formal Software Development Lifecycle which incorporates the following requirements related to secure software development practices at a minimum:

- Secure development environments shall be established.
- Secure coding guidelines shall be followed based on industry best practices for each programming language used and based on the level of risk associated with the application. (e.g., OWASP Framework Security Project forthe secure development of web applications).
- Source code repositories must be managed in a secure environment to prevent the theft, corruption or loss or source code.
- Segregation of duties must be applied within source code repositories, to prevent unauthorized versions of source code from being promoted into the production environment. (See 6.1.2)

- Access to the administrative functionality of source code management applications and the ability to promote source code into production environments must be restricted to a select group of administrators and strictly enforced.

14.2.3 System Change Control Procedures

All changes to systems shall be controlled using the Company's formal change control procedures. These procedures are established to ensure the integrity of systems and applications from the early design stages through to ongoing maintenance stages of a systems life cycle.

These guidelines apply to both the acquisition of new systems and changes to existing systems.

- All change requests must be formally documented within the change management application.
- A risk assessment should be completed to determine the impact the change will have to the existing control environment.
- Additional security controls that might be required due to the change should be identified where applicable (e.g., a new application does not federate withthe enterprise Active Directory environment and will require special consideration for logical access).
- Roll back plans should be established and documented where applicable.
- Changes must be submitted to an authorized member of management of a Change Advisory Board for review.
- Formal approval of the detailed proposal of work should be obtained prior to the work commencing.
- The change request must document timing and identify dependencies affected by the change. Consideration to timing of the change and deployment should be based on this information to minimize disturbances to operations.
- All system documentation should be updated as needed prior to completion of the change.
- Postmortem details and results of the change should be documented before marking the change request as completed.
- Changes should be archived, maintaining an audit trail of all change requests.

14.2.4 Technical Review of Applications After Operating Platform Changes

All changes to operating platforms, which include operating systems, databases, andmiddleware platforms, shall be tested within a UAT/Staging environment prior to their implementation into the production environment to allow for appropriate

tests and review to take place and reduce the risk of the changes having an adverse impact on organizational operations and security.

Exceptions may be made for emergency changes (e.g., high priority securitypatches).

All changes, including emergency changes, should be documented in accordance with the system change control procedures (see 14.2.2).

14.2.5 Restrictions on Changes to Software Packages

Vendor-supplied software packages should not be modified unless expressly authorized by appropriate members of management.

Authorized modifications should be formally documented, and the followingconsiderations documented within the change request documentation:

- How will the changes impact the future maintenance of the software?
- Will the changes affect the ability to apply future security patches provided by the vendor?
- Will the changes introduce compatibility issues with other systems or applications?
- Will the changes affect the processing integrity of the application?
- Is consent from the vendor required to make modifications to the software?

14.2.6 Secure System Engineering Principles

Secure engineering principles refers to the application of security while developing Information Technology projects. Principles of secure systems engineering should be developed to assure the protection of Company and customer information during processing, in transit and at rest, at all architectural levels, as follows:

- Business Layer: e.g., Implementing controls in adherence with requirementsfor Segregation of Duties (see 6.1.2), Access Control, user authentication requirements, secure session control, and limited access to only authorized users, based on the least privilege required to perform their duties (see 9.0).
- Data Layer: e.g., Enforcement of strong authentication methods (see 9.4) and properly securing, ensuring the availability and integrity of data (see 10, 12.2, 12.3). Data validation and sanitation considerations.
- Applications: e.g., Implementing processes to ensure the processing integrityof applications. Ensuring the availability of services (see 12) and security of ingress and egress communications (see 13).
- Technology: e.g., Verification of technology before its procurement and properly documenting and managing the process of procuring, implementing

and maintaining technology (see 14 and 15) to ensure the integrity, confidentiality and availability of services, and customer and Company data.

Detailed standard operating procedures should be developed to build on the requirements set forth of this policy at all architectural layers of the Company's information systems.

14.2.7 Secure Development Environment

The risks associated with system and application development efforts should be assessed and proper security controls should be established to mitigate those risks.

The Company shall consider the following risks associated with system and implement appropriate security controls in accordance with the requirements of the Information Security policy and other applicable policies and procedures:

- The sensitivity of data to be processed, stored or transmitted by the system.
- Consideration of applicable internal policies, regulatory requirements or contractual requirements for the management of different classifications of data (e.g., Payment card data, personally identifiable information, personal health information);
- Consideration of pre-existing security controls already in place that may be utilized.
- Trustworthiness of personnel granted access to potentially sensitive Company or customer data (see 7.1);
- Consideration of third party/vendor access to sensitive Company or customer data.
- Separation of duties requirements (see 6.1.2) and control of access to different development environments.
- Monitoring and logging of changes to the development environment and the source code therein.
- Backup policy and management of backups of the development environment.
- Control over movement of data to and from the development environment.

Once security controls are identified for a specific environment, the secure development procedures for the given environment should be documented and provided to applicable members of management and users interacting with the environment.

14.2.8 Outsourced Development

Where system and application development are outsourced, the following points should be considered and included within customer contracts and service level agreements:

- Licensing arrangements, code ownership and intellectual property rights shall be expressly defined.
- The Company's requirements for secure design, coding and testing practices should be clearly stated (see 14.2.1).
- A requirement that formal quality acceptance and user acceptance testing must be completed prior to the Company accepting the deliverables should be stated.
- Evidence that the third party has established a control environment which conforms to the security and privacy requirements set forth within the Information Security policy must be obtained.
- A right to audit the development process and controls of the third party should be stated.
- Code escrow arrangements shall be established if the source code becomes unavailable from the third party.
- The third party remains responsible for compliance with all applicable laws and verifying the operating effectiveness of its control environment.

14.2.9 System Security Testing

Periodic system security testing should be completed throughout all stages of the development lifecycle (see 14.1).

Management shall implement the following security testing measures at a minimum:

- The completion of internally implemented vulnerability scans of internal networks and external facing interfaces in accordance with the Technical Vulnerability policy (see 12.6.1).
- The completion of user access reviews in accordance with the Access Review policy (see 9.2.5).
- The completion of annual external assessments including external IT and Cyber Risk assessments and penetration/security posture tests (see 12.7.1).
- Ongoing internal malware and virus scanning (see 12.2.1).
- Ongoing monitoring and review of security related audit logs and events (see 12.4).
- Completion of source code static application scans and remediation of issues for all releases, prior to completion of UAT.

14.2.10 System Acceptance Testing

In addition to the requirements defined in the Information Security Requirements Analysis and Specifications and Securing Application Services on Public Networks sections (see 14.1.1 and 14.1.2), as well as the requirements set forth in the Secure

Development policy (see 14.2.1), new systems implementing within the Company's network should be assessed using vulnerability scanners to identify potential configuration issues prior to deployment into production.

For example, prior to implementing a new router into production, a vulnerability scan might identify outdated firmware, enabled services, open ports or other potential issues not identified during setup.

14.3 Test Data

14.3.1 Protection of Test Data

The use of sensitive data in test and development environments should be avoided. Data classified as Confidential or Restricted (see 8.2.1) should be obfuscated when in use in test and development environments where possible.

In instances where sensitive data is used in test and development environments, the same control considerations must be applied to test and development as they are to production environments including policies surround monitoring and logging, data encryption, securing data in transit and access control procedures.

14.4 System Development Life Cycle (SDLC)

14.4.1 SDLC Policies

As part of the software acquisition process, Get Event Log LLC shall identify security requirements that must be implemented relative to a given product. Where the security functionality in a proposed product does not satisfy the specified requirements, the risk introduced, and associated controls (manual or automated) shall be reconsidered prior to acquisition of the product. Further, where additionalfunctionality is supplied and causes a security risk, the functionality shall be disabled or mitigated through the application of additional controls.

Get Event Log LLC developers (or outsourced developers performing services on behalf of Get Event Log LLC) shall identify and document the functions, ports, protocols, and servicesintended for use for a proposed product. Such information shall be documented as early in the life cycle as feasible.

All software approved for use within Get Event Log LLC's environments shall meetpre-defined system and information integrity requirements.

14.4.2 SDLC Procedures

The Senior Security Program Manager is responsible for maintaining Get Event Log LLC's SDLC procedures to ensure that a secure software acquisition process is followed forany purchased or internally developed software. As part of the process, security requirements are required to be developed and documented as part of the

requirement specifications. Once all specifications have been defined, the system owner requesting new software will present his or her proposal to the IRC. Members of the IRC are responsible for reviewing the proposals and determining if the proposal presents any additional risks to Get Event Log LLC.

If the security functionality of a proposed product does not satisfy thespecified requirements, the IRC and the applicable system owner will determine if manual or automated controls can be implemented to mitigate the identified risks. Ifthe risks cannot be mitigated by a control activity, the risk must be accepted by the IRC for the software to be approved, or the software request will be denied. For any products installed, additional functionality that is not required to satisfy a business purpose must be disabled, consistent with Get Event Log LLC's hardening standards.

For any software that is developed internally by Get Event Log LLC personnel or by outsourced developers, the functions, ports, protocols, and services intended for use are required to be documented as part of the product specifications. Such information will be reviewed by the IRC consistent with the process, before software is implemented within Get Event Log LLC's environments. Additionally, the specifications are required to include system and information integrity requirements that must be met, along with control activities (automated or manual) that must be implemented to preserve the integrity of the associated data.

15.0 Supplier Relationships

15.1 Information Security in Supplier Relationships

15.1.1 Information Security Policy for Supplier Relationships

Suppliers are defined by the Company as vendors or partners with whom the Company maintains some business relationship related to:

- Hardware and software support and maintenance.
- Consulting or contracting.
- IT or business process outsourcing; • Data acquisition, sharing, or processing.

Criteria for selecting suppliers shall be defined and documented, and consider:

- The supplier's reputation and business history.
- Quality of services provided to other customers.
- Quality and quantity of staff and managers.
- Financial stability of the supplier.
- Information security assurances (e.g., SOC 2 reports, ISO certifications, etc.).

The business owner of the supplier relationship shall be responsible for engaging the OIS to conduct a risk assessment prior to formalizing a relationship and

conducting business with a supplier. The risk assessment must be approved by the ISRC based on the rules established in the Company Risk Management Process.

All supplier relationships must be conducted under the governance of a formal contract between the parties. If restricted information is to be exchanged, a binding confidentiality agreement must be in place. All information exchanged between the parties must be appropriately classified, labeled, and protected.

All contracts shall be submitted to Legal for review of content, language, andpresentation.

15.1.2 Addressing Security Within Supplier Agreements

Various additional information security controls should be embedded or referenced within the contracts between the Company and the suppliers, such as:

- Information security policies, procedures, standards, and guidelines.
- Background checks on employees or third parties working on the contract.
- Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc.
- Information security incident management procedures including mandatory incident reporting requirements.
- Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity.
- Copyright, patents, and similar protection for any intellectual property sharedwith the outsourcer or developed in the course of the contract.
- Specification, design, development, testing, implementation, configuration, management, maintenance, support, and use of security controls within or associated with IT systems, plus source code escrow.
- Anti-malware, anti-spam and similar controls.
- IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks.

15.1.3 Information and Communication Technology Supply Chain

Information security controls concerning product supply chain should be embedded or referenced within the supplier agreements between the Company and the suppliers, such as:

- Requiring that the supplier propagate the Company's information security requirements and practices throughout the supply chain including its subcontractors.

- Monitoring the supplier for compliance with the Company's information security requirements.
- Requiring that suppliers of mission critical services and infrastructure demonstrate an ability to deliver the product or service at a level that meets the Company's business requirements (e.g., availability requirements and BCP/DR requirements);
- Defining rules for controlling and sharing information in accordance with the Company's data classification policy.

15.2 Supplier Service Delivery Management

15.2.1 Monitoring and Review of Supplier Services

The Company shall actively monitor suppliers for compliance with service level agreements and contractual requirements.

The Company shall periodically audit Suppliers for compliance with information security requirements as specified in contractual agreements. The periodicity and level of audit shall be defined in each contract.

15.2.2 Managing Changes to Supplier Services

The Company shall implement processes to monitor and manage changes to supplier provided services including supplier enhancements, implementation of new technologies, tools or environments, subcontracting changes, or changes to the supplier's facility locations.

Company controls and processes should be tracked and updated as necessary based on the actions of suppliers.

16.0 Information Security Incident Management

16.1 Management of Information Security Incidents and Improvements

16.1.1 Responsibilities and Procedures

For the purposes of this Policy, all privacy and security events / incidents shall follow the same incident response plan.

The Office of Information Security shall manage all incident response per this Incident Response Plan.

IT and management shall be responsible for initial evaluation of reported or suspected security incidents, in accordance with the Incident Assessment Checklist (see Appendix II).

Upon identification of a potential incident, IT shall notify the OIS and initiate the incident response procedures (see Appendix I and II).

16.1.2 Reporting Information Security Events

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify their supervisor or the OIS.

Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.)
- Suspected virus/malware/Trojan infection
- Loss or theft of any device that contains company information
- Loss or theft of ID badge or keycard
- Any attempt by any person to obtain a user's password over the telephone or by email (e.g., phishing attack)
- Ineffective security controls
- Breach of information integrity, confidentiality, or availability expectations
- Human errors
- Non-compliances with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Malfunctions of software or hardware
- Any other suspicious event that may impact the company's information security

Users must treat a suspected security incident as Restricted information and report the incident only to his or her supervisor or the OIS. Users must not withhold information relating to a security incident or interfere with any investigation to include state and federal investigations.

16.1.3 Reporting Information Security Weaknesses

If a security weakness is discovered or suspected, the user must immediately notify their supervisor or the OIS and follow any applicable guidelines as detailed in the Company Incident Response Plan.

16.1.4 Assessment of and Decision on Information Security Events

As stated above, IT shall be responsible for initial evaluation of reported or suspected security incidents. Upon confirmation of an incident, IT shall notify the OIS and initiate the incident response procedures.

16.1.5 Response to Information Security Incidents

The OIS shall be responsible for managing the response to verified security incidents. The response should adhere to the Incident Management and Response

Workflow, Incident Assessment Checklist, and Incident Containment Checklists (see Appendixes I, II, and III).

16.1.6 Learning from Information Security Incidents

The OIS shall manage Information Security improvement activities to ensure the activities meet Company business objectives including the objective of reasonable improvement of Information Security. The Company shall implement a "lessons learned" process as a follow-up to all security incidents. This process shall be defined in the Company Incident Response plan.

16.1.7 Collection of Evidence

If an incident occurs which may result in a legal investigation takingplace, Management shall identify a qualified digital forensic professional to assist in properly documenting, preserving evidence and maintaining proper chain of custody.

The Digital Evidence Preservation Checklist should be consulted for additional guidance (see Appendix IV).

17.0 Information Security Aspects of Business Continuity Management

17.1 Information Security Continuity

The Company utilizes "cloud" services to host all production applications. High disaster recovery and business continuity planning for datacenter operations are, therefore, the responsibility of the third-party "cloud" provider. The scope of this section is limited to the business continuity of the production software running on the "cloud" infrastructure.

Information security aspects of business continuity are: (i) based on identifying events that can cause interruptions to Get Event Log LLC's critical business processes; (ii) followed by a risk assessment to determine the probability and impact of such interruptions; (iii) based on the results of the risk assessment, a business continuitystrategy is developed to identify the overall approach to business continuity; and
(iv) once this strategy has been created, endorsement is provided by management, and a plan is created and endorsed to implement this strategy. Company personnel are required to validate that business operations can be recovered and restored within the time frame required by the business objectives and without a deterioration of the security measures.

As part of the Business Continuity Plan, the required capacity, critical missions and functions, recovery objectives and priorities, and roles and responsibilities of applicable personnel shall be documented.

Copies of the Business Continuity Plan shall be distributed to all personnel who have business continuity related roles and responsibilities.

17.1.1 Planning Information Security Continuity

The Company shall determine requirements for information security and the continuity of information security management in adverse conditions. These requirements shall be documented in the Company Business Continuity Plan.

17.1.2 Implementing Information Security Continuity

The Company shall implement and maintain processes, procedures and controls as defined in the Company Business Continuity Plan to ensure the required level of continuity for information security during an adverse situation.

17.1.3 Verify, Review and Evaluate Information Security Continuity

The Company shall verify the established and implemented information security continuity controls at regular intervals to ensure that they are valid andeffective during adverse situations

17.2 Redundancies

17.2.1 Availability of Information Processing Facilities

The Company shall adopt an architecture that is highly available and highly redundant. The Company shall leverage resources available from the “cloud” provider to ensure the availability of production systems and data.

18.0 Compliance

18.1 Compliance with Legal and Contractual Requirements

18.1.1 Identification of Applicable Legislation and Contractual Requirements

All legislation applicable to the Company, both in the USA and external jurisdictions where the Company operates, should be identified to ensure legal and regulatory compliance.

The Information Risk Council is responsible for the identification of relevant legal and regulatory requirements and communicating these requirements to applicable business unit leadership.

18.1.2 Intellectual Property Rights

To ensure that the Company remains compliant with all legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software, the following guidelines must be considered to protect any material that may be considered intellectual property:

- Establish a policy of only acquiring software through approved vendors of a reputable source, to ensure copyrights are not violated.
- Communicate the expectations that all users protect intellectual property rights and give notice of intent to take disciplinary action against personnel breaching IP rights.
- Maintain an asset register which documents rights to use of all assets used within the organization and maintain evidence of licenses and ownership of all assets.
- Carry out periodic reviews to ensure that only authorized software is installed on Company owned systems.

18.1.3 Protection of Records

All records should be classified, labeled, managed, and secured in accordance withthe Company's data classification policy (see 8.2). Records should be maintained and retained in accordance with all legislative, regulatory, and contractual requirements.

The confidentiality and integrity of data may be assured using encryption in accordance with the requirements of the cryptographic policy. All cryptographic keys leveraged to secure company data and records should be managed in accordance with the Company's cryptographic policies (see 10.0).

The type of media selected for storage of records should be designed to last for the duration of the retention requirements of the records being stored on the media. This is to safeguard against loss due to future technology change or natural degradation of some media formats (e.g., The life expectancy of optical discs variesbased on many factors.)

18.1.4 Privacy and Protection of Personally Identifiable Information

A privacy policy should be established which defines how the Company will provide for the privacy and protection of personally identifiable information and reflect all legislative, regulatory, and contractual requirements.

The Information Risk Council is responsible for the identification of relevant legal and regulatory requirements and communicating these requirements to applicable business unit leadership.

18.1.5 Regulation of Cryptographic Controls

Legal advice should be sought by the Company prior moving encrypted data and controls across jurisdictional borders, to ensure that legislative and regulatory requirements are met in all jurisdictions where the Company is operating.

18.2 Information Security Reviews

18.2.1 Independent Review of Information Security

The Company shall initiate periodic independent review of the state of information security control within the Company's information systems. Independent review may be carried out through an internal audit function (independent of the area under review), an external audit function (e.g., AICPA attestation engagements) andexternal security posture assessments.

Management should make a best effort to determine that the individuals carrying out these reviews have appropriate skill, experience, and credentials. The results ofindependent review should be reported to management and identify areas where the organization is meeting or failing to meet the requirements of the Information Security policies.

18.2.2 Compliance with Security Policies and Standards

Compliance reviews over Get Event Log LLC's information security program must be completed on an annual basis, and the results and recommendations must bedocumented and reported to management for their review and approval.
Management (IRC or senior leadership) will review the results of the annual review and take necessary action to approve and/or document necessary follow-up items.

Annual compliance reviews must include the following:

- Annual Review of Security Policies, Procedures & Standards
- Annual Review of Implemented Security Controls
- Annual Risk Assessment
- Annual Penetration Test
- Vulnerability Scanning (minimum quarterly)

Processes (both manual or systematic) should be identified to demonstrate ongoing compliance with security policies and standards.

Manual processes may include periodic compliance reviews performed by internal audit or security analysts.

Systematic utilities may include infrastructure and network monitoring utilities (i.e., Network Management tools, IDS, NextGen Firewalls), log monitoring (i.e., SIEM) and configuration management/enforcement utilities (e.g., Puppet, AD GPO, Centrify).

18.2.3 Compliance Review Procedure

The following annual compliance review procedures are specified by management:

- Annual Review of Security Policies & Standards: management will review all policies and standards and update the 'reviewed date' and 'version' (if necessary) and report completion of the review to the Information Risk Council (IRC) no later than (NLT) Q4 of each calendar year. Any necessary and proposed changes to existing company documentation will be reviewed by the IRC for comment and approval.
- Annual Review of Implemented Security Controls: management will review the suite of implemented security controls (e.g., SOC 2 and HITRUST CSF) on an annual basis to validate the relevance, implementation status, and make recommendations based upon current needs of the business (e.g., adjust control language; implement additional controls). Recommendations will be presented to the IRC for review, comment, and approval of NLT Q4 of each calendar year.
- Annual Risk Assessment: An annual risk assessment will be conducted in accordance with the Risk Management Policy and results of the risk assessment will be presented to the IRC for review, comment, and risk treatment. Newly identified risks will be added to the risk register, and the risk register will be updated to reflect the current risk profile and environment of the business.
- Annual Penetration Test: The organization will engage with a third-party security firm to conduct minimum annual penetration testing of its systems and applications. Results will be presented to the IRC for review and for remediation plans to be created. The IRC will monitor remediation of identified gaps and security issues and ensure that security issues are prioritized and addressed in a timely manner.
- Vulnerability Scanning (minimum quarterly): The organization will conduct minimum quarterly vulnerability scans of its environment and will prioritize and remediate identified issues based upon the risk of the vulnerability. If an automated/continuous vulnerability scanning service or managed service is used to meet vulnerability scanning requirements, management will ensure that meetings are conducted quarterly (minimum) between the organization's DevOps/Security teams and the third-party vendor to validate findings, trends, issues, and ensure that timely reporting, tracking, and remediation of issues are being conducted. Management will report the results of vulnerability scans and any associated meetings to the IRC on a quarterly basis.

Technical compliance with the Company's Information Security policies should be reviewed with the assistance of systematic tools (see 18.2.2) with the output of ongoing monitoring utilities being analyzed by a qualified system or security engineer.

All penetration tests and vulnerability assessments should be undertaken with caution due to such activities potentially causing downtime or compromises of the security of systems.

All technical compliance reviews should be carried out by qualified individuals. Management shall make a best effort to only engage individuals with appropriate skill, experience, and credentials.

18.2.4 Sanctions Process Policy

The organization shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. Designated personnel shall be notified within a defined time frame when a formal sanction process is initiated.

Get Event Log LLC takes disciplinary action against workforce members that fail tocooperate with federal and state investigations.

18.2.4.1 Sanctions Process Procedure

As part of the Acceptable Use Policy, personnel are required to inform a supervisor or the Human Resources department within 24 hours when a deviation from information security policies and procedures is identified.

The Human Resources department is responsible for maintenance of the Employee Handbook, which defines sanctions or disciplinary procedures that may be applied to personnel who violate Get Event Log LLC's information security policies or who fail to cooperate with federal and state investigations. Disciplinary procedures are appliedon a case-by-case basis based on the severity of a situation but may include procedures up to and including termination.

Incident tickets are maintained for each identified incident that contain a description of (i) personnel involved with the incident, (ii) steps taken to identify and respond to the incident, along with a timeline of the steps taken, (iii) steps taken to notify personnel that were alerted of the incident, (iv) rationale for disciplinary procedures applied, if applicable, and (v) the outcome of each incident along with lessons learned. Human Resources personnel also maintain a separate listing of personnel involved in incidents, which is updated each time an incident is discovered and responded to.