Organization Information Security Policy

Purpose and Scope

This Information Security Policy addresses the information security policy topics and requirements which maintain the security, confidentiality, integrity, and availability of Organization applications, systems, infrastructure, and data. The topics and requirements called out in this policy should be continuously improved upon to maintain a secure information security posture. From time to time, Organization may update this policy and implement different levels of security controls for different information assets based on risk and other considerations. This policy is guided by security requirements specific to Organization including compliance with applicable laws and regulations.

This policy applies to all Organization assets utilized by personnel acting on behalf of Organization or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all Organization policies and plans upon starting and at least annually.

Information Security Communication

Please contact Employee name if you have any questions about the Organization information security program.

People Security

Background Check

All Organization personnel are required to complete a background check. An authorized member of Organization must review each background check in accordance with local laws.

Confidentiality

Prior to accessing sensitive information, personnel are required to sign an industry-standard confidentiality agreement protecting Organization 's confidential information.

Security Awareness Training

Organization has a security awareness training program in place to promote the understanding of security policies and procedures. All personnel are required to undergo training following initial employment and annually thereafter. Completion of the training program is logged by Organization .

Secure Coding

Organization promotes the understanding of secure coding to its engineers in order to improve the security and robustness of Organization products.

Physical Security

Clear Desk

Organization personnel are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area when it is unattended. This requirement extends to both remote and in-office work.

Organization personnel must remove hard copies of sensitive information from desks and lock the information in a drawer when desks are unoccupied and at the end of the workday. Keys used to access sensitive information must not be left at an unattended desk.

Clear Screen

Organization employees and contractors must be aware of their surroundings at all times and ensure that no unauthorized individuals have access to see or hear sensitive information. All mobile and desktop devices must be locked when unoccupied. Session time-outs and lockouts are enforced through technical controls for all systems containing covered information.

All devices containing sensitive information, including mobile devices, shall be configured to automatically lock after a period of inactivity (e.g. screen saver).

Remote Work

Any Organization issued devices used to access company applications, systems, infrastructure, or data must be used only by the authorized employee or contractor of such device.

Employees or contractors accessing the Organization network or other cloud-based networks or tools are required to use HTTPS/TLS 1.2+ at a minimum to protect data-in-transit.

If employees are in a public space, they must ensure their sight lines are blocked and they do not have customer conversations or other confidential conversations. If someone is close to them, they must assume they can see and hear everything. Connecting directly to a public wireless network that doesn't employ, at minimum, WPA-2 or an equivalent wireless protocol is prohibited.

While working at home, employees and applicable contractors should be mindful when visitors (e.g. maintenance personnel) are at their residences, as visitors could become privy to sensitive information left up on computer screens.

System Access Security

Organization adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of privileges or changes to privileges and access permissions are documented and require approval by an authorized manager. System access is revoked immediately upon termination or resignation.

Account Audits

Audits of access and privileges to sensitive Organization applications, infrastructure, systems, and data are performed regularly and reviewed by authorized personnel.

Password Security

Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with anyone. Where possible, all user and system accounts must invoke password complexity requirements specified in the Access Control and Termination Policy. All accounts must use unique passwords not shared with any other accounts.

Rotation Requirements

If a password is suspected to be compromised, the password should be rotated immediately and the security team should be immediately notified.

Storing Passwords

Passwords must only be stored using a Organization approved password manager. Organization does not hard code passwords or embed credentials in static code.

Asset Security

Organization maintains a Configuration and Asset Management Policy designed to track and set configuration standards to protect Organization devices, networks, systems, and data. In compliance with such policy, Organization may provide team members laptops or other devices to perform their job duties effectively.

Data Management

Organization stores and disposes of sensitive data in a manner that; reasonably safeguards the confidentiality of the data; protects against the unauthorized use or disclosure of the data; and renders the data secure or appropriately destroyed. Data entered into Organization applications must be validated where possible to ensure quality of information processed and to mitigate the impacts of web-based attacks on the systems.

Data Classification

Organization defines the handling and classification of data in the Data Classification Policy.

Data Retention and Disposal Policy

The time periods for which Organization must retain customer data depends on the purpose for which it is used. Organization retains customer data as long as an account is active, as needed to provide services to the customer, or in accordance with the agreement(s) between Organization and the customer. An exemption to this policy would include if Organization is required by law to dispose of data earlier or keep data longer. Organization may retain and use customer data to comply with its legal obligations, resolve disputes, and enforce agreements.

Except as otherwise set forth in the Organization policies, Organization also disposes of customer data when requested by customers.

organization maintains a sanitization process that is designed to prevent sensitive data from being exposed to unauthorized individuals. Organization hosting and service providers are responsible for ensuring the removal of data from disks allocated to Organization use before they are repurposed or destroyed.

Change and Development Management

To protect against unauthorized changes and the introduction of malicious code, Organization maintains a Change Management Policy with change management procedures that address the types of changes, required documentation, required review and/or approvals, and emergency changes. Changes to Organization production infrastructure, systems, and applications must be documented, tested, and approved before deployment.

Vulnerability and Patch Management

Organization uses a proactive vulnerability and patch management process that prioritizes and implements patches based on classification. Such classification may include whether the severity is security-related or based on other additional factors.
Organization schedules third-party penetration tests and/or performs internal assessments at least annually.

If you believe you have discovered a vulnerability, please email email address and Organization will aim to address the vulnerability, if confirmed, as soon as possible.

Environment Separation

As necessary, Organization maintains requirements and controls for the separation of development and production environments.

Source Code

Organization controlled directories or repositories containing source code are secured from unauthorized access.

Logging and Monitoring

Organization collects and monitors audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services, as well as IAM user and admin activities.
Organization manages logging solution(s) and/or SIEM tool(s) to collect event information of the aforementioned systems and activities. Organization implements filters, parameters, and alarms to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts.

Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. Organization utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.

When events and alerts are generated from monitoring solutions and mechanisms, Organization correlates those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy and Change Management Policy.

Additionally, Organization utilizes threat detection solution(s) to actively monitor and alert on network and application-based threats.

Business Continuity and Disaster Recovery

Organization maintains a plan for continuous business operations if facilities, infrastructure or systems fail. The plan is tested, reviewed and updated at least annually.

Backup Policy

Backups are performed according to appropriate backup schedules to ensure critical systems, records, and configurations can be recovered in the event of a disaster or media failure.

Security Incident Response

Organization maintains a plan that defines responsibilities, detection, and corrective actions during a security incident. The plan will be executed following the discovery of an incident such as system compromise, or unintended/unauthorized acquisition, access, use or release of non-public information. The plan is tested, reviewed and updated at least annually.

Organization utilizes various monitoring and surveillance tools to detect security threats and incidents. Early detection and response can mitigate damages and minimize further risk to Organization .

A message should be sent to Organization if you believe there may be a security incident or threat.

Risk Management

Organization requires a risk assessment to be performed at least annually. For risks identified during the process, Organization must classify the risks and develop action plans to mitigate discovered risks.

Vendor Management

Organization requires a vendor security assessment before third-party products or services are used confirming the provider can maintain appropriate security and privacy controls. The review may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other security compliance evidence. Agreements will be updated and amended as necessary when business, laws, and regulatory requirements change.

Exceptions

Organization business needs, local situations, laws, and regulations may occasionally call for an exception to this policy or any other Organization policy. If an exception is needed, Organization management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other Organization policy or procedure may result in disciplinary action, up to and including termination of employment. Organization reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Organization does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Organization as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Organization reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Employee name.

This document was last updated on MM/DD/YYYY.