**General Information**

**Security Policy**

**COMPANY NAME**

**Version #**

**Last Revision Date**

Document Classification

**Table of Contents**

[Introduction 4](#_Toc58096846)

[Authority 4](#_Toc58096847)

[Purpose 4](#_Toc58096848)

[Scope 4](#_Toc58096849)

[Exceptions 4](#_Toc58096850)

[Roles and Responsibilities 4](#_Toc58096851)

[Principles 5](#_Toc58096852)

[3.1 -Access Control. 5](#_Toc58096853)

[3.2 - Awareness and Training (AT) 5](#_Toc58096854)

[3.3 - Audit and Accountability (AU) 5](#_Toc58096855)

[3.4 - Configuration Management (CM) 5](#_Toc58096856)

[3.5 - Identification and Authentication (IA) 5](#_Toc58096857)

[3.6 - Incident Response (IR) 5](#_Toc58096858)

[3.7 - Maintenance (MA) 5](#_Toc58096859)

[3.8 - Media Protection (MP) 5](#_Toc58096860)

[3.9 - Personnel Security (PS) 5](#_Toc58096861)

[3.10 - Physical Protection (PE) 6](#_Toc58096862)

[3.11 - Risk Assessment (RA) 6](#_Toc58096863)

[3.12 - Security Assessment (SA) 6](#_Toc58096864)

[3.13 - System and Communications Protection (SC) 6](#_Toc58096865)

[3.14 - System and Information Integrity (SI) 6](#_Toc58096866)

[Requirements 7](#_Toc58096867)

|  |  |
| --- | --- |
| **Prepared By** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Description** | **Pages Affected** |
| 1.0 | [DATE] | Initial version of SSP | All |
|  |  |  |  |
|  |  |  |  |

Introduction

Authority

To protect the confidentiality, integrity and availability of the company information, the company shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards, and procedures.

Purpose

The purpose of this policy is to enable the company to conduct business safely and to set a framework for managing information security risk at the appropriate tolerance.

Scope

This policy applies to [COMPANY NAME]. In addition, the requirements of this policy apply to third parties that store, process, or transmit data on behalf of the company. Applicable local laws, regulations, and other restrictions will apply to the extent of any conflict with this document.

Exceptions

Exceptions to the requirements of this policy must be authorized by the System Security Officer. All exceptions must be documented, including the business reason or criteria for requiring the exception, and formal approval retained. Policy exceptions must be reviewed quarterly to ensure the associated risk remains mitigated to an acceptable level.

Roles and Responsibilities

The **System Security Officer** Is responsible for the correct and thorough implementation of the principles and requirements of this policy. Reviews and approves requested exceptions to this policy; and Ensures all personnel understand their responsibilities with respect to this policy and the correct use and management of controls for the protection of company information systems and assets

Principles

3.1 - Access Control.

The Company has a formal process to grant or deny requests to use information, use information processing services and enter company facilities.

3.2 - Awareness and Training (AT)

Personnel are made aware of the security risks associated with their roles and they understand the applicable laws, policies, standards, and procedures.

3.3 - Audit and Accountability (AU)

Awareness of security-related events is maintained through the centralized collection and analysis of event logs from systems, applications, and services.

3.4 - Configuration Management (CM)

The integrity of information technology products and systems is maintained through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC).

3.5 - Identification and Authentication (IA)

The identity of a user, process, or device is verified as a prerequisite for granting access to resources in a system. Technical measures are in place that prevent unauthorized individuals or processes from entering a system.

3.6 - Incident Response (IR)

The Company is ready to respond. An actionable Cybersecurity incident handling capability is established that includes adequate preparation, detection, analysis, containment, recovery and reporting activities.

3.7 - Maintenance (MA)

Systems are kept in good working order to minimize risks from hardware and software failures. Technology assets are managed throughout the lifecycle of the asset, from procurement through disposal. Company controls the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

3.8 - Media Protection (MP)

The company protects system media, both paper and digital, limits access to information on system media to authorized users, and sanitizes or destroys system media before disposal or release for reuse

3.9 - Personnel Security (PS)

A security and privacy-minded workforce is fostered through sound hiring practices and ongoing personnel management. The company ensures that individuals occupying positions of responsibility within the company (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensures that company information and systems are protected during and after personnel actions such as terminations and transfers, and employs formal sanctions for personnel failing to comply with company security policies and procedures.

3.10 - Physical Protection (PE)

The company limits physical access to systems, equipment, and the respective operating environments to authorized individuals, protects the physical plant and support infrastructure, provides supporting utilities for systems, protects systems against environmental hazards, and provides appropriate environmental controls in facilities containing systems

3.11 - Risk Assessment (RA)

The risk to operations (e.g., mission, functions, image, reputation), assets, and employees, which may result from the operation of company systems and the associated processing, storage, or transmission of company information is periodically assessed

3.12 - Security Assessment (SA)

The company regularly assesses the security requirements of systems to determine if the requirements are effective in their application, develops and implements plans of action & milestones designed to correct deficiencies and reduce or eliminate vulnerabilities in company systems, authorizes the operation of company systems and any associated system connections, and monitors security requirements on an ongoing basis to ensure the continued effectiveness of the requirements, and documents these actions in the System Security Plan.

3.13 - System and Communications Protection (SC)

Information transmitted or received by company systems are monitored, controlled, and protected at the external boundaries and key internal boundaries of systems. Architectural designs, software development techniques, and systems engineering principles that promote effective information security are used.

3.14 - System and Information Integrity (SI)

Information and system flaws are identified, reported, and corrected in a timely manner, Protection from malicious code is provided at appropriate locations within company systems, and systems are monitored for security alerts and advisories.

Requirements

*The following security requirements are required to accomplish the principles established above:*

* 1. **Access Control**
     1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
     2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.
     3. Control the flow of CUI in accordance with approved authorizations.
     4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
     5. Employ the principle of least privilege, including for specific security functions and privileged accounts.
     6. Use non-privileged accounts or roles when accessing non-security functions.
     7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
     8. Limit unsuccessful logon attempts.
     9. Provide privacy and security notices consistent with applicable CUI rules.
     10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
     11. Terminate (automatically) a user session after a defined condition.
     12. Monitor and control remote access sessions.
     13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
     14. Route remote access via managed access control points.
     15. Authorize remote execution of privileged commands and remote access to security-relevant information.
     16. Authorize wireless access prior to allowing such connections.
     17. Protect wireless access using authentication and encryption.
     18. Control connection of mobile devices.
     19. Encrypt CUI on mobile devices and mobile computing platforms.
     20. Verify and control/limit connections to and use of external systems.
     21. Limit use of organizational portable storage devices on external systems.
     22. Control CUI posted or processed on publicly accessible systems.
  2. **Awareness and Training**
     1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
     2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
     3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.
  3. **Audit and Accountability**
     1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
     2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
     3. Review and update logged events.
     4. Alert in the event of an audit logging process failure.
     5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
     6. Provide audit record reduction and report generation to support on-demand analysis and reporting.
     7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
     8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
     9. Limit management of audit logging functionality to a subset of privileged users.
  4. **Audit and Accountability** 
     1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
     2. Establish and enforce security configuration settings for information technology products employed in organizational systems.
     3. Track, review, approve or disapprove, and log changes to organizational systems.
     4. Analyze the security impact of changes prior to implementation.
     5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
     6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
     7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
     8. Apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software.
     9. Control and monitor user-installed software.
  5. **Identification and Authentication**
     1. Identify system users, processes acting on behalf of users, and devices.
     2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
     3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
     4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
     5. Prevent reuse of identifiers for a defined period.
     6. Disable identifiers after a defined period of inactivity.
     7. Enforce a minimum password complexity and change of characters when new passwords are created.
     8. Prohibit password reuse for a specified number of generations.
     9. Allow temporary password use for system logons with an immediate change to a permanent password.
     10. Store and transmit only cryptographically protected passwords.
     11. Obscure feedback of authentication information.
  6. **Incident Response**
     1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
     2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
     3. Test the organizational incident response capability
  7. **Maintenance**
     1. Perform maintenance on organizational systems.
     2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
     3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.
     4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
     5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
     6. Supervise the maintenance activities of maintenance personnel without required access authorization.
  8. **Media Protection**
     1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
     2. Limit access to CUI on system media to authorized users.
     3. Sanitize or destroy system media containing CUI before disposal or release for reuse.
     4. Mark media with necessary CUI markings and distribution limitations.
     5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
     6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
     7. Control the use of removable media on system components.
     8. Prohibit the use of portable storage devices when such devices have no identifiable owner.
     9. Protect the confidentiality of backup CUI at storage locations.
  9. **Personnel Security**
     1. Screen individuals prior to authorizing access to organizational systems containing CUI.
     2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
  10. **Physical Protection**
      1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
      2. Protect and monitor the physical facility and support infrastructure for organizational systems.
      3. Escort visitors and monitor visitor activity.
      4. Maintain audit logs of physical access.
      5. Control and manage physical access devices.
      6. Enforce safeguarding measures for CUI at alternate work sites.
  11. **Risk Assessment**
      1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
      2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
      3. Remediate vulnerabilities in accordance with risk assessments.
  12. **Security Assessment**
      1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
      2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
      3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
      4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
  13. **System and Communications Protection**
      1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
      2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
      3. Separate user functionality from system management functionality.
      4. Prevent unauthorized and unintended information transfer via shared system resources.
      5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
      6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
      7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
      8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
      9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
      10. Establish and manage cryptographic keys for cryptography employed in organizational systems.
      11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
      12. Prohibit remote activationof collaborative computing devices and provide indication of devices in use to users present at the device.
      13. Control and monitor the use of mobile code.
      14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
      15. Protect the authenticity of communications sessions.
      16. Protect the confidentiality of CUI at rest.
  14. **System and Information Integrity**
      1. Identify, report, and correct system flaws in a timely manner.
      2. Provide protection from malicious code at designated locations within organizational systems.
      3. Monitor system security alerts and advisories and take action in response.
      4. Update malicious code protection mechanisms when new releases are available.
      5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
      6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
      7. Identify unauthorized use of organizational systems.