<Business Name>

Information Security Policy

Version 1.0

Revision History

|  |  |  |
| --- | --- | --- |
| Revision Date | Revision Made | Revision Author |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1. Asset Management Policy 4](#_Toc69251246)

[a. Purpose 4](#_Toc69251247)

[b. Policy 4](#_Toc69251248)

[c. Media Destruction 4](#_Toc69251249)

[d. Backup 4](#_Toc69251250)

[e. Removable Media 4](#_Toc69251251)

[2. Auditing 5](#_Toc69251252)

[a. Purpose 5](#_Toc69251253)

[b. Policy 5](#_Toc69251254)

[3. Access and Identity Management 5](#_Toc69251255)

[a. Purpose 5](#_Toc69251256)

[b. Policy 5](#_Toc69251257)

[Access Control 5](#_Toc69251258)

[Identity Management 6](#_Toc69251259)

[Administrator Access 6](#_Toc69251260)

[4. Email Policy 7](#_Toc69251261)

[a. Purpose 7](#_Toc69251262)

[b. Policy 7](#_Toc69251263)

[5. Password and Authentication Management Policy 7](#_Toc69251264)

[a. Purpose 7](#_Toc69251265)

[b. Policy 7](#_Toc69251266)

[6. Remote Access 8](#_Toc69251267)

[a. Purpose 8](#_Toc69251268)

[b. Policy 8](#_Toc69251269)

# Asset Management Policy

## Purpose

This policy provides procedures and protocols supporting effective organizational asset management specifically focused on electronic devices for <Business Name>

## Policy

* All hardware, software, and applications must be approved through <Business Name>’s IT department vendors risk assessment process.
* Any new software, hardware installation must be approved through the change management channels before implementation.
* Authorize cloud computing services should only be used for sharing, storing, or transferring internal or confidential information.
* Logs of hardware, software, and applications should be kept up to date and reviewed annually.
* All hardware, software, and applications should have an assigned owner.
* Upon termination of employment, contract, or agreement, all <Business Name>’s assets must be returned to IT Management.

## Media Destruction

* Media that contains confidential or internal information must be adequately erased, destroyed. Until completed, the media should be deemed unusable prior to disposal or reuse.
* All decommissioned media must be stored in a secure area prior to destruction.
* Media reuse and destruction practices must be tracked and documented.
* All data must be destroyed when no longer needed, included encrypted media.

## Backup

* This is discussed in the Disaster Recovery Plan found:
  + <https://github.com/OneStopCyberSecurity/Cyber-Security-Documents/blob/main/Disaster%20Recovery%20Plan.doc>

## Removable Media

* Use of removable media must first be approved by IT Management regarding reason of use.
* The media must be approved, and company issued allowing for proper logging.
* Personally owned removable media is not permitted.
* Unknown media is not permitted to be used and is required to be turned into IT if found on company property.
* Confidential and internal (District/Organization) information should not be stored on removable media without the use of encryption.
* The loss or theft of a removable media device that may have contained (District/Organization) information must be reported to the (District/Organization) IT.

# Auditing

## Purpose

This policy provides the requirements for conducting audit-related reviews regarding the information systems of <Business Name>

## Policy

* All information resources that create, collect, store, and/or process confidential information must be audited on a basis pre-determined by the auditing and business tool’s team.
* System security audits must be led by information security personnel with the specialized training necessary to conduct such audits.
* Personnel conducting system security audits should communicate the following information to information resource owners, custodians, and users, prior to conducting an audit:
  + The date in which the audit will begin,
  + The date in which the audit will end,
  + The scope of the audit,
  + The purpose of the audit,
  + The potential, even if slight, of service disruption.
* Information resource owners and custodians must provide reasonable access to information resources for audit personnel to conduct security audits in accordance with the documented purpose and scope of the audit.
* All pertinent security audit activities and results must be documented.
* Audit summary reports must be created for each system security audit conducted, and the reports must be provided to management at the conclusion of the audit.
* Every security audit deficiency must be accompanied with a recommendation.

# Access and Identity Management

## Purpose

This policy provides the requirements necessary to ensure that accounts and information resources that access or contain internal, confidential information are properly managed in accordance with business requirements, information security requirements and any other polices that may apply.

## Policy

### Access Control

* Access to an information resource must be justified with business requirements prior to approval.
* “Need to know” basis is applied for confidential information.
* Access to confidential information must be logged
* Access to confidential information must require further user authentication (multi-factor, etc.)
* Areas of information recourses involving internal or confidential information must be mapped and kept up to date.

### Identity Management

* All employees must sign <Business Name>’s Policy Acknowledgment form before gaining access to the company’s assets.
* All accounts created must have an associated, and documented, request and approval.
* Segregation of duties must exist between access request, access authorization, and access administration.
* Elevated accounts must be required to have multi-factor authentication or passwords stored in a monitored vault.
* Elevated account users must be mapped and kept up to date.
* Owners of the information resource are responsible for approving new access requests
* Account names must be in accordance with company naming standards pre-determined by IT Management.
* All accounts are required to have their password expired after a pre-determined time by IT Management.
* Access to information resources should be granted to groups not individual users.
* Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
* Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
* Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
* Users are required to report improper access assignment

### Administrator Access

* Personnel with Administrative/Special access accounts must only perform the tasks required to complete their job function
* Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
* Admin accounts passwords if possible, where access to the password is controlled and can be rotated after each checkout. If not, the account’s password should be changed regularly and after a user with knowledge of the password has a role change.
* In the case where a system has only one administrator, there must be a procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency.

# Change Management Policy

## Purpose

The purpose of this procedure is to provide guidance for Information Systems Department personnel and other employees with regard to change management within the company. This procedure sets standards for how employees should go about putting a change into production.

This procedure will balance the concerns between security risks and operational risks. It has been determined that automated patching would not cover the full scope of issues, and thus this procedure must be followed regarding patching software. Making a change in hardware/software will be done and kept up to date to ensure integrity of data and applications. If a major service needs to be altered immediately, IT and the department responsible will coordinate for the update and communications should be sent out to those affected properly.

## Policy

* Using the risk assessment guide, evaluate the change to determine the risk associated and identify its score.
  + The score rankings are outlined within the Change Management Risk Assessment Document.
* Submit a Change Request for any requests to be deployed which must be approved by IT and Business management.
  + A change request will include basic information and a risk assessment guide which will include items such as; environment affected, number of employees affected, downtime required, ability to revert change, and ability to go into a non-production environment.
  + If a non-production environment is not available for the application, ensure the change is monitored and done during hours outside business operations.
* An ability to revert changes is required when a patch is being deployed straight into the production environment.
* If there is no non-production environment for a third-party application, the vendor must be engaged during the patching event.
* Deploy patches into a non-production environment to be smoke-tested by IT and monitored.
  + If there are any issues, provide detailed documentation to the software development team so they can revise the patch and resubmit it for further testing.
* Before production rollout, ensure backups have been synced.
* If there will be downtime on a system, a communication should be sent to any affected teams/employees.
* Deploy patches into the production environment during off-hours after 1 week of successful smoke-testing.
  + Monitor for any issues; if something occurs, refer to 4a.
* Document the patch management process, including any setbacks or issues that occurred.
* Once devices have been patched, images must be updated to the recent patches.

# Email Policy

## Purpose

This policy provides the requirements of a user to practice proper use of <Business Name>’s email system. It is to define to the employee what is acceptable behavior.

## Policy

* Email use should be compliant with positive practice regarding ethical conduct, safety, and compliance to the law.
* <Business Name>’s email accounts should be primarily used for business use. Personal basis is permitted but is subject to review. Non-<Business Name>’s related commercial use is prohibited.
* Data included in an email must adhere to data protection standards.
* Employees are prohibited to setting up automatic forwarding to a third-party email account/system. Any email leaving <Business Name>’s network must not contain confidential or internal information. Pre-authorization is required, and it must be sent securely using encryption.
* Any business-related work should be conducted on the business email and not personal, non-work email accounts.
* There is no standard of privacy when using company email whether be inbound, outbound, or storage.
* <Business Name> is not required to provide notice upon monitoring, or investigation an employees mailbox.

# Password and Authentication Management Policy

## Purpose

This policy provides the requirements that are needed to practice safe authentication management. This includes on the user’s side and administrator duties.

## Policy

* Personnel are required to maintain the confidentiality of personal authentication information.
* All passwords should meet the predetermined password requirements determined by IT Management. As safe practice they should not include
  + Common words, phrases and not tied to personal information.
* Previous passwords should be kept preventing the refusal of previous passwords.
* If a password management system is employed, it must be used in compliance with the authentication standards.
* Computing devices should not be left unattended without enabling a password protected screensaver or logging off the device.
* If a user’s password is compromised or discovered, the password must be immediately changed, and the security incident reported to <Business Name>’s IT support.

# Remote Access

## Purpose

This policy provides the requirements that are needed for an employee to safely remote access into <Business Name>’s network.

## Policy

* All remote access connections to <Business Name>’s networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
* The ability to print or copy confidential information remotely must be disabled.
* Remote sessions must be terminated after a defined period of inactivity.
* Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.
* Any loss of company assets or information must be reported to IT Security personnel immediately after discovery.
* Safe accessing practices should be implemented by end users and should be taught, handed out upon approval of remote access.