Information Security Policy

Organization name or logo

Date

Provided by



## Introduction

This policy outlines the implementation of Center for Internet Security (CIS) Version 8 tailored to Implementation Group 1 (IG1) within Organization. CIS Controls v8 IG1 is designed for small to medium-sized enterprises with limited cybersecurity resources. It focuses on essential security measures to establish basic cyber hygiene and protect against common threats. The goal is to provide a foundational security framework to help organizations mitigate the most common cyber threats.

This policy applies to all employees, contractors, and third-party users who interact with Organization systems and data.

## Policy Enforcement

All employees are expected to adhere to this policy and report any violations or security incidents to the Organization’s IT Security Team immediately. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, the Organization may pursue legal action against individuals or entities that violate this policy.

## Review and Update

This access control policy must be reviewed and updated at least annually or when siginificant enterprise changes occur that might affect current safeguards to ensure its effectiveness and alignment with the Organization’s security requirements and industry best practices.

## Approval

This policy has been approved by the Organization’s senior management and is effective as of the date indicated below.

**Effective Date**: Date  
**Approved By**: Name/Title

## Review, Update, and Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description of change | Approved by |
| 1.0 | 1/1/2024 | Initial draft. | MC3 Technologies |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Introduction 2](#_Toc170896604)

[Policy Enforcement 2](#_Toc170896605)

[Review and Update 2](#_Toc170896606)

[Approval 2](#_Toc170896607)

[Review, Update, and Version Control 2](#_Toc170896608)

[Policy 5](#_Toc170896609)

[1. Inventory and Control of Hardware Assets 5](#_Toc170896610)

[Purpose 5](#_Toc170896611)

[Scope 6](#_Toc170896612)

[1.1 Establish and Maintain Detailed Enterprise Asset Inventory 6](#_Toc170896613)

[1.2 Address Unauthorized Assets 6](#_Toc170896614)

[2. Inventory and Control of Software Assets 6](#_Toc170896615)

[Purpose 6](#_Toc170896616)

[Scope 6](#_Toc170896617)

[2.1 Establish and Maintain a Software Inventory 7](#_Toc170896618)

[2.2 Ensure Authorized Software is Currently Supported 7](#_Toc170896619)

[2.3 Address Unauthorized Software 7](#_Toc170896620)

[3. Data Protection 7](#_Toc170896621)

[Purpose 7](#_Toc170896622)

[Scope 7](#_Toc170896623)

[3.1 Establish and Maintain a Data Management Process 8](#_Toc170896624)

[3.2 Establish and Maintain a Data Inventory 8](#_Toc170896625)

[3.3 Configure Data Access Control Lists 8](#_Toc170896626)

[3.4 Enforce Data Retention 8](#_Toc170896627)

[3.5 Securely Dispose of Data 8](#_Toc170896628)

[3.6 Encrypt Data on End-User Devices 8](#_Toc170896629)

[4. Secure Configuration of Enterprise Assets and Software 8](#_Toc170896630)

[Purpose 8](#_Toc170896631)

[Scope 9](#_Toc170896632)

[4.1 Establish and Maintain Secure Configuration Process for Enterprise Assets and Software 9](#_Toc170896633)

[4.2 Establish and Maintain Secure Configuration Process for Network Infrastructure 9](#_Toc170896634)

[4.3 Configure Automatic Session Locking on Enterprise Assets 9](#_Toc170896635)

[4.4 Implement and Manage a Firewall on Servers 9](#_Toc170896636)

[4.5 Implement and Manage a Host-Based Firewall on End-User Devices 9](#_Toc170896637)

[4.6 Securely Manage Enterprise Assets and Software 9](#_Toc170896638)

[4.7 Manage Default Accounts on Enterprise Assets and Software 10](#_Toc170896639)

[5. Account Management 10](#_Toc170896640)

[Purpose: 10](#_Toc170896641)

[Scope: 10](#_Toc170896642)

[5.1 Establish and Maintain an Inventory of Accounts 10](#_Toc170896643)

[5.2 Use Unique Passwords 10](#_Toc170896644)

[5.3 Disable Dormant Accounts 10](#_Toc170896645)

[5.4 Restrict Administrator Privileges to Administrative Accounts 10](#_Toc170896646)

[6. Access Control Management 11](#_Toc170896647)

[Purpose: 11](#_Toc170896648)

[Scope: 11](#_Toc170896649)

[6.1 Establish an Access Granting Process 11](#_Toc170896650)

[6.2 Establish an Access Revoking Process 11](#_Toc170896651)

[6.3 Require Multi-Factor Authentication (MFA) for Externally-Exposed Applications, Remote Network Access, and Administrative Access 11](#_Toc170896652)

[7. Continuous Vulnerability Management 12](#_Toc170896653)

[Purpose 12](#_Toc170896654)

[Scope 12](#_Toc170896655)

[7.1 Establish and Maintain a Vulnerability Management Process 12](#_Toc170896656)

[7.2 Establish and Maintain a Remediation Process 12](#_Toc170896657)

[7.3 Perform Automated Operating System Patch Management 12](#_Toc170896658)

[7.4 Perform Automated Application Patch Management 12](#_Toc170896659)

[8. Audit Log Management 12](#_Toc170896660)

[Purpose: 12](#_Toc170896661)

[Scope: 13](#_Toc170896662)

[8.1 Establish and Maintain an Audit Log Management Process 13](#_Toc170896663)

[8.2 Collect Audit Logs 13](#_Toc170896664)

[8.3 Ensure Adequate Audit Log Storage 13](#_Toc170896665)

[9. Email and Web Browser Protections 13](#_Toc170896666)

[Purpose: 13](#_Toc170896667)

[Scope: 13](#_Toc170896668)

[9.1 Ensure Use of Only Fully Supported Browsers and Email Clients 14](#_Toc170896669)

[9.2 Use DNS Filtering Services 14](#_Toc170896670)

[10. Malware Defenses 14](#_Toc170896671)

[Purpose: 14](#_Toc170896672)

[Scope: 14](#_Toc170896673)

[10.1 Deploy and Maintain Anti-Malware Software 14](#_Toc170896674)

[10.2 Configure Automatic Anti-Malware Signature Updates 14](#_Toc170896675)

[10.3 Disable Autorun and Autoplay for Removable Media 14](#_Toc170896676)

[11. Data Recovery 15](#_Toc170896677)

[Purpose: 15](#_Toc170896678)

[Scope: 15](#_Toc170896679)

[11.1 Establish and Maintain a Data Recovery Process 15](#_Toc170896680)

[11.2 Perform Automated Backups 15](#_Toc170896681)

[11.3 Protect Recovery Data 15](#_Toc170896682)

[11.4 Establish and Maintain an Isolated Instance of Recovery Data 15](#_Toc170896683)

[12. Network Infrastructure Management 15](#_Toc170896684)

[Purpose: 15](#_Toc170896685)

[Scope: 15](#_Toc170896686)

[12.1 Ensure Network Infrastructure is Up-to-Date 16](#_Toc170896687)

[13. Security Awareness and Skills Training 16](#_Toc170896688)

[Purpose: 16](#_Toc170896689)

[Scope: 16](#_Toc170896690)

[13.1 Establish and Maintain a Security Awareness Program 16](#_Toc170896691)

[13.2 Train Workforce Members to Recognize Social Engineering Attacks 16](#_Toc170896692)

[13.3. Train Workforce Members on Authentication Best Practices 16](#_Toc170896693)

[13.4 Train Workforce on Data Handling Best Practices 16](#_Toc170896694)

[13.5 Train Workforce Members on Causes of Unintentional Data Exposure 17](#_Toc170896695)

[13.6 Train Workforce Members on Recognizing and Reporting Security Incidents 17](#_Toc170896696)

[13.7 Train Workforce on How to Identify and Report out-of-date Software 17](#_Toc170896697)

[13.8 Train Workforce on the Dangers of Connecting to Public Networks 17](#_Toc170896698)

[14. Service Provider Management 17](#_Toc170896699)

[Purpose: 17](#_Toc170896700)

[Scope: 17](#_Toc170896701)

[14.1 Establish and Maintain an Inventory of Service Providers 17](#_Toc170896702)

[15. Incident Response Management 18](#_Toc170896703)

[Purpose: 18](#_Toc170896704)

[Scope: 18](#_Toc170896705)

[15.1 Designate Personnel to Manage Incident Handling 18](#_Toc170896706)

[15.2 Establish and Maintain Contact Information for Reporting Security Incidents 18](#_Toc170896707)

[15.3 Establish and Maintain an Enterprise Process for Reporting Incidents 18](#_Toc170896708)

[Appendix A: Definitions 19](#_Toc170896709)

# **Policy**

## Inventory and Control of Hardware Assets

***Control References: CIS Control- 1.1, 1.2***

Purpose:

Organization shall actively manage (inventory, track, and correct) all enterprise assets to ensure that only authorized devices are granted access according to enterprise policies. This control helps in maintaining a comprehensive and accurate understanding of all enterprise assets, reducing the risk of unauthorized access, and ensuring proper asset lifecycle management.

Scope:

This policy applies to all physical and virtual devices capable of processing and storing data used within the enterprise, including but not limited to, end-user devices, servers, mobile devices, IoT devices, and network devices. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 1.1 Establish and Maintain Detailed Enterprise Asset Inventory

Maintain an accurate, detailed inventory of all enterprise assets, including devices connected physically, virtually, and remotely (including cloud environments). The inventory shall include the following fields:

* Asset type (e.g., desktop, laptop, server, mobile device)
* Manufacturer
* Model
* Serial number
* Asset tag
* Location (physical location or network location)
* Owner (individual or department responsible for the asset)
* Date of acquisition
* Operating system/version
* Network addresses (IP address, MAC address)
* Assigned users
* Security status (e.g., antivirus, encryption status)

Review and Update: The asset inventory must be reviewed and updated at least bi-annually to ensure accuracy and completeness.

### 1.2 Address Unauthorized Assets

Ensure that a process exists to address unauthorized assets on a weekly basis, ensuring immediate response to detect and remove unauthorized assets from the network. Organization may remove the asset from the network, deny access, or quarantine any suspected unauthorized asset.

## Inventory and Control of Software Assets

***Control References: CIS Control- 2.1, 2.2, 2.3***

Purpose:

Actively manage (inventory, track, and correct) all software within the enterprise to ensure that only authorized software is installed and can execute. This control aids in preventing the use of unlicensed or malicious software and ensures that all software is supported and up-to-date.

Scope:

This policy applies to all software applications used within the Organization, including on-premises, cloud-based, and third-party applications. It involves all departments, including IT, operations, and any user (internal and external) who installs or uses software on Organizational systems.

#### Organization shall:

### 2.1 Establish and Maintain a Software Inventory

Maintain a detailed inventory of all software applications, including those installed on devices connected physically, virtually, and remotely (including cloud environments). The inventory shall include the following fields:

* Software name / title
* Publisher
* Version
* License type and status
* Installation / use date
* Authorized user(s)
* Associated hardware
* Purpose or function
* License key
* Software classification (e.g., system, application, utility)
* Source of software (e.g., purchased, open source, in-house including URL or App Store)

Review and Update: The software inventory must be reviewed and updated at least bi-annually to ensure accuracy and completeness. All software must be properly licensed and tracked in the inventory.

### 2.2 Ensure Authorized Software is Currently Supported

Ensure that only currently supported software is installed in the environment. Verify that software versions are up-to-date and receive security patches from the manufacturer. Unsupported software should be upgraded, replaced, or removed. Exceptions to this rule must be documented, justified, and approved by the IT / Security Team.

### 2.3 Address Unauthorized Software

Ensure that a process exists to address unauthorized software. This includes detecting, identifying, and removing or authorizing and monitoring any unauthorized software on the network. The process must be conducted at least monthly.

## Data Protection

***Control References: CIS Control- 3.1, 3.2, 3.3, 3.4, 3.5, 3.6***

Purpose**:**

Protect Organizational data through effective management and technical security controls. This includes safeguarding data from unauthorized access, ensuring data integrity, and complying with relevant data protection regulations.

Scope**:**

This policy applies to all sensitive data processed, stored, or transmitted by the Organization. It includes data in databases, file systems, backup storage, and data in transit. All departments handling sensitive data must comply with this policy.

#### Organization shall:

### 3.1 **Establish and Maintain a Data Management Process**

Implement and maintain processes for managing sensitive data. This includes establishing a data classification scheme, data ownership, proper handling, data retention limits, and disposal requirements, based on the sensitivity of the data.

### 3.2 **Establish and Maintain a Data Inventory**

Establish and maintain a data inventory, based on the data classification scheme. At a minimum, inventory sensitive data. The inventory should include:

* Data type
* Data classification (e.g., public, internal, confidential, sensitive)
* Location of data (e.g., databases, file systems, cloud storage)
* Data owner
* Access controls in place
* Retention period
* Backup status
* Encryption status

### 3.3 **Configure Data Access Control Lists**

Configure data access control lists based on a need-to-know basis. Access to sensitive data must be restricted to authorized personnel only. This should apply to all local and remote systems, databases, and applications.

### 3.4 **Enforce Data Retention**

Retain data according to the enterprise’s data management processes and securely dispose of data when no longer needed. Data retention policies should include both minimum and maximum timelines and be aligned with applicable legal and regulatory requirements.

### 3.5 **Securely Dispose of Data**

Securely dispose of data as outlined in Organization 's data management process. This includes using methods such as shredding, degaussing, and secure erasure for electronic data, commensurate with the sensitivity of the data.

### 3.6 **Encrypt Data on End-User Devices**

Encrypt data on end-user devices containing sensitive data. Encryption should be in accordance with industry standards and Organizational policies.

## Secure Configuration of Enterprise Assets and Software

***Control References: CIS Control- 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7***

Purpose:

Establish and maintain secure configurations for hardware and software to reduce vulnerabilities and prevent unauthorized access. This helps in ensuring that all enterprise assets are securely configured and regularly updated.

Scope:

This policy applies to all hardware and software configurations across the Organization 's IT environment, including servers, workstations, network devices, and applications. It is relevant to all IT staff and any personnel responsible for configuring and maintaining IT systems.

#### Organization shall:

### 4.1 Establish and Maintain Secure Configuration Process for Enterprise Assets and Software

Establish and maintain a secure configuration process for all enterprise assets and software. This includes developing and enforcing baseline configurations and ensuring compliance with security best practices. At minimum, review this process documentation annually, or when significant enterprise changes occur.

### 4.2 Establish and Maintain Secure Configuration Process for Network Infrastructure

Establish and maintain a secure configuration process for network infrastructure. This involves configuring network devices such as firewalls, routers, and switches with secure settings to protect against vulnerabilities. At minimum, review this process documentation annually, or when significant enterprise changes occur.

### 4.3 Configure Automatic Session Locking on Enterprise Assets

Configure automatic session locking:

* On enterprise assets after no more than 15 minutes of inactivity.
* On end-user and mobile devices after no more than two minutes of inactivity.

This helps to prevent unauthorized access when devices are left unattended.

### 4.4 Implement and Manage a Firewall on Servers

Implement and manage firewalls on servers (where supported), ensuring only necessary services and ports are allowed. Regularly review and update firewall rules to align with security policies.

### 4.5 Implement and Manage a Host-Based Firewall on End-User Devices

Implement and manage a host-based firewall or port-filtering on end-user devices, ensuring only necessary services and ports are allowed. Use a default-deny rule where possible. Regularly review and update firewall rules to align with security policies.

### 4.6 Securely Manage Enterprise Assets and Software

Securely manage enterprise assets and software throughout their lifecycle. This includes secure deployment, configuration, maintenance, and decommissioning of assets. Only allow secure network protocols such as SSH and HTTPS.

### 4.7 Manage Default Accounts on Enterprise Assets and Software

Manage default accounts (such as root, administrator, or vendor accounts) on enterprise assets and software, ensuring they are either disabled, removed, or secured. Default accounts should have strong, unique passwords and minimal privileges.

## Account Management

***Control References: CIS Control- 5.1, 5.2, 5.3, 5.4***

## Purpose:

Organization shall actively manage user accounts to ensure only authorized users have access to systems and data. This control helps in maintaining a comprehensive and accurate understanding of all user accounts, reducing the risk of unauthorized access, and ensuring proper account lifecycle management.

## Scope:

This policy applies to all user accounts within Organization, including but not limited to end-user accounts, administrative accounts, and service accounts. It encompasses all departments and locations where Organization operates.

#### Organization shall:

## 5.1 Establish and Maintain an Inventory of Accounts

Maintain an accurate, detailed inventory of all accounts, including:

* Account type (e.g., end-user, administrative, service)
* Account owner (individual or department responsible for the account)
* Account name
* Username
* Date of account creation / removal
* Last activity date
* Account status (active, inactive, disabled)  
    
  The account inventory must be reviewed, validated, and updated at least quarterly to ensure accuracy and completeness.

## Use Unique Passwords

Ensure that all user accounts utilize unique passwords. Passwords must have at least 14-characters: including numbers, uppercase letters, lowercase letters, and special characters.

## 5.3 Disable Dormant Accounts

Disable or delete any dormant accounts that have not been used for 45 days. Regular reviews will be conducted to identify and address dormant accounts at least quarterly.

## 5.4 Restrict Administrator Privileges to Administrative Accounts

Restrict administrative privileges to dedicated administrative accounts. Users must not use administrative accounts for non-administrative activities such as web browsing, email, etc.. Administrative accounts should be reviewed at least quarterly and monitored for compliance.

## Access Control Management

***Control References: CIS Control- 6.1, 6.2, 6.3, 6.4, 6.5***

## Purpose:

Organization shall implement robust access control mechanisms to ensure that only authorized users have access to its information systems and data. This control aims to prevent unauthorized access, reduce the risk of data breaches, and ensure that access permissions are managed efficiently and effectively.

## Scope:

This policy applies to all employees, contractors, and third-party users who have access to Organization 's information systems and data. It encompasses all physical and virtual environments, including on-premises and cloud-based systems.

#### Organization shall:

## 6.1 Establish an Access Granting Process

Establish and follow a process, preferably automated, for granting access to systems and data upon new hire, rights grant, or role change of a user. This process shall include:

* Verification of the user's identity.
* Approval from the user's manager or designated authority.
* Documentation of the access granted, including the user's name, role, and access level.
* Regular reviews of access permissions to ensure they remain appropriate.

## 6.2 Establish an Access Revoking Process

Establish and follow a process, preferably automated, for revoking or disabling access to systems and data. This process shall include:

* Immediate revocation of access upon termination, rights revocation, or role change.
* Notification to relevant system administrators to remove access promptly.
* Documentation of the access revoked, including the user’s name, role, and access level.
* Regular audits to ensure that access revocation procedures are followed correctly.

## 6.3 Require Multi-Factor Authentication (MFA) for Externally-Exposed Applications, Remote Network Access, and Administrative Access

Require multi-factor authentication (MFA) for ALL:

* Externally-exposed enterprise or third-party applications
* Remote network access
* Administrative and privilileged accounts

This requirement aims to enhance security by adding an extra layer of authentication beyond just a username and password, reducing the risk of unauthorized access. Consider using a directory service or SSO provider for ease of implementation and management of this requirement.

## Continuous Vulnerability Management

***Control References: CIS Control- 7.1, 7.2, 7.3, 7.4***

## Purpose

The purpose of this policy is to establish and maintain a comprehensive vulnerability management program to identify, evaluate, treat, and report on security vulnerabilities in systems and applications used by the organization. This ensures the protection of the Organization 's information assets from exploitation.

## Scope

This policy applies to all systems and applications within the Organization, including on-premises and cloud environments, across all departments and locations where the Organization operates.

#### Organization shall:

### 7.1 Establish and Maintain a Vulnerability Management Process

Establish and maintain a documented vulnerability management process to identify, assess, and remediate vulnerabilities in a timely manner. Regularly review public and private industry sources for updates on emerging threats and vulnerabilities.

### 7.2 Establish and Maintain a Remediation Process

Establish and maintain a risk-based remediation process to address identified vulnerabilities promptly. This process must ensure that vulnerabilities are remediated according to their risk level and include a verification step to confirm remediation. Review at least monthly.

### 7.3 Perform Automated Operating System Patch Management

Perform automated operating system updates at least monthly to ensure that all enterprise assets are protected against known vulnerabilities. This process must include regular patch cycles and testing patches before deployment (when possible) to production systems.

### 7.4 Perform Automated Application Patch Management

Perform automated application updates at least monthly to protect enterprise assets from known vulnerabilities in applications. This process must ensure regular updates and monitoring to verify successful deployment.

## Audit Log Management

***Control References: CIS Control- 8.1, 8.2, 8.3***

## Purpose:

Organization shall establish and maintain an audit log management process to ensure that all relevant log data is collected, analyzed, and stored to support security monitoring and incident response efforts. This control helps in maintaining a comprehensive and accurate understanding of activities within the Organization 's network, reducing the risk of undetected security incidents, and ensuring proper log management practices.

## Scope:

This policy applies to all enterprise assets capable of generating audit logs, including but not limited to end-user devices, servers, network devices, and applications. It encompasses all departments and all locations where Organization operates.

#### Organization shall:

### 8.1 Establish and Maintain an Audit Log Management Process

Establish and maintain an audit log management process that includes:

* Defining which log data is to be collected.
* Identifying systems that should collect and analyze log data.
* Determining circumstances under which log data should be reviewed and analyzed.
* Ensuring that audit logging configurations are standardized across the Organization.

### 8.2 Collect Audit Logs

Ensure that logging, per the defined process, is enabled on all enterprise assets. This includes:  
- Enabling logging on end-user devices, servers, network devices, and applications.  
- Aggregating logs from different sources into a centralized log management system.  
- Ensuring that logs capture sufficient detail to support forensic investigations and incident response efforts.

### 8.3 Ensure Adequate Audit Log Storage

Ensure that logging destinations maintain adequate storage capacity to retain log data over time. This includes:

* Monitoring log storage capacity and expanding storage as needed to prevent loss of log data.
* Reviewing stored log data periodically to ensure data integrity and relevance.
* Implementing data retention policies to define the duration for which log data should be stored, based on regulatory and business requirements.

## Email and Web Browser Protections

***Control References: CIS Control- 9.1, 9.2***

## Purpose:

Organization shall ensure the use of only fully supported and updated web browsers and email clients, and implement DNS filtering services to protect against malicious content and activities. This control helps in mitigating the risks associated with web and email-based threats, ensuring a secure browsing and communication environment.

## Scope:

This policy applies to all enterprise assets including end-user devices, servers, and network devices that use web browsers and email clients. It encompasses all departments and all locations where Organization operates.

#### Organization shall:

### 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients

Ensure that only fully supported and up-to-date web browsers and email clients are used across the Organization. This includes:

* Regularly updating browsers and email clients to the latest versions.
* Removing or disabling outdated and unsupported browsers and email clients.
* Configuring security settings to enforce the use of secure protocols and features.

### 9.2 Use DNS Filtering Services

Implement DNS filtering services on all enterprise assets to block access to known malicious domains and protect against phishing attacks. This includes:

* Configuring DNS filters to automatically block access to malicious or suspicious websites.
* Regularly updating DNS filter rules and lists to include new threats.
* Monitoring and reviewing DNS filter logs to detect and respond to potential threats.

## Malware Defenses

***Control References: CIS Control- 10.1, 10.2, 10.3***

## Purpose:

The purpose of this policy is to ensure the deployment, maintenance, and updating of anti-malware defenses across all enterprise assets. This helps protect the Organization 's information systems and data from malware threats, ensuring the confidentiality, integrity, and availability of information.

## Scope:

This policy applies to all enterprise assets, including but not limited to desktops, laptops, servers, mobile devices, and any other devices capable of storing or processing data. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 10.1 Deploy and Maintain Anti-Malware Software

Deploy and maintain anti-malware software on all enterprise assets. The anti-malware software must be capable of detecting, removing, and protecting against various forms of malware, including viruses, worms, trojans, ransomware, and spyware.

### 10.2 Configure Automatic Anti-Malware Signature Updates

Configure automatic updates for anti-malware signatures on all enterprise assets. This ensures that the anti-malware software remains up-to-date with the latest malware definitions, providing continuous protection against emerging threats.

### 10.3 Disable Autorun and Autoplay for Removable Media

Disable autorun and autoplay auto-execute functions for all removable media on enterprise assets. This measure prevents the automatic execution of malicious code from removable media, reducing the risk of malware infections.

## Data Recovery

***Control References: CIS Control- 11.1, 11.2, 11.3, 11.4***

## Purpose:

The purpose of this policy is to ensure the establishment and maintenance of robust data recovery processes. This policy aims to protect the Organization 's data integrity and availability by ensuring that critical data can be recovered in the event of data loss or corruption.

## Scope:

This policy applies to all enterprise data, including but not limited to databases, file systems, and application data. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 11.1 Establish and Maintain a Data Recovery Process

Establish and maintain a data recovery process that ensures timely and reliable recovery of critical data. This process must address the scope of data recovery activities, recovery prioritization, and the security of backup data.

### 11.2 Perform Automated Backups

Perform automated backups of in-scope enterprise data. Automated backups should be scheduled at least weekly, depending on the sensitivity of the data.

### 11.3 Protect Recovery Data

Protect recovery data with equivalent controls to the original data. This includes ensuring the confidentiality, integrity, and availability of backup data through encryption, access controls, and secure storage.

### 11.4 Establish and Maintain an Isolated Instance of Recovery Data

Establish and maintain an isolated instance of recovery data. This isolated instance should be separate from the primary data environment to prevent simultaneous loss or corruption of both primary and backup data. Consider utilizing version controlling backup destination through offline, cloud, or off-site systems or services.

## Network Infrastructure Management

***Control References: CIS Control- 12.1***

## Purpose:

The purpose of this policy is to ensure the proper active management (track, report, correct) and security of the Organization 's network infrastructure. This includes maintaining up-to-date network components, implementing security controls, and ensuring the overall integrity and availability of the network.

## Scope:

This policy applies to all network infrastructure components, including but not limited to routers, switches, firewalls, and other network devices. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 12.1 Ensure Network Infrastructure is Up-to-Date

Ensure that all network infrastructure components are kept up-to-date. This includes applying the latest firmware updates, security patches, and configuration changes to protect against vulnerabilities and ensure optimal performance. Review software versions at least monthly to verify software support.

## Security Awareness and Skills Training

***Control References: CIS Control- 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8***

### Purpose:

The purpose of this policy is to establish and maintain a security awareness and skills training program to ensure that all employees are aware of and adhere to the security policies, procedures, and best practices of Organization. This program aims to mitigate the risks of social engineering attacks, data breaches, and other security threats by educating the workforce on recognizing and responding to potential security incidents.

### Scope:

This policy applies to all employees, contractors, and third-party personnel who have access to the Organization’s information systems and data. The policy encompasses all departments and locations where the Organization operates.

#### Organization shall:

### 13.1 Establish and Maintain a Security Awareness Program

Establish and maintain a comprehensive security awareness program to educate the workforce on security policies, procedures, and best practices to ensure they interact with enterprise assets and data in a secure manner. Provide employee training upon hire and at least annually thereafter.

### 13.2 Train Workforce Members to Recognize Social Engineering Attacks

Provide employees training on how to recognize and respond to social engineering attacks, including phishing, pretexting, tailgating, and other manipulative tactics used by attackers to gain unauthorized access to enterprise resources. Training sessions should consist of periodic security reminders and simulated phishing exercises, where appropriate.

### 13.3. Train Workforce Members on Authentication Best Practices

Provide training on authentication best practices, including the use of strong passwords, multi-factor authentication (MFA), and secure credential management.

### 13.4 Train Workforce on Data Handling Best Practices

Train employees on best practices for handling and transferring sensitive data, including data classification, encryption, and secure data storage and disposal. Training may also include locking their screen while away from their computer and erasing physical and virtual whiteboards once meetings end.

### 13.5 Train Workforce Members on Causes of Unintentional Data Exposure

Educate employees on the common causes of unintentional data exposure, such as misdelivery of emails, improper sharing of files, and accidental publication of sensitive information. Training might include real-world examples and scenarios to help employees understand the impact of data exposure incidents.

### 13.6 Train Workforce Members on Recognizing and Reporting Security Incidents

Train employees to recognize signs of security incidents, such as unusual system behavior, unauthorized access attempts, and suspicious emails or communications. The Organization will establish clear procedures for reporting security incidents and ensure that employees are aware of these procedures.

### 13.7 Train Workforce on How to Identify and Report out-of-date Software

Provide training on how to identify and report out-of-date software patches or failures in automated processes and tools. Employees should be trained to report any failures to the designated IT staff.

### 13.8 Train Workforce on the Dangers of Connecting to Public Networks

Educate employees on the risks associated with connecting to public networks, such as unsecured Wi-Fi hotspots, and the best practices for securing their devices when accessing the internet outside the Organization ’s secure environment. Training will cover the use of virtual private networks (VPNs), personal firewalls, and secure browsing practices. For remote workers training must include guidance for securely configuring their home network infrastructure.

## Service Provider Management

***Control References: CIS Control- 15.1***

## Purpose:

The purpose of this policy is to establish and maintain a robust process for managing service providers. This includes ensuring that all service providers meet the Organization 's security requirements and adhere to best practices for data protection.

## Scope:

This policy applies to all external service providers that have access to the Organization 's data, systems, and networks. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 14.1 Establish and Maintain an Inventory of Service Providers

Establish and maintain an inventory of service providers. This inventory should include details such as:

* The type of services provided
* The type of data handled (classification, sensitivity level, etc.)
* Enterprise contact at the company

## Incident Response Management

***Control References: CIS Control- 17.1, 17.2, 17.3***

## Purpose:

The purpose of this policy is to establish and maintain a comprehensive incident response management capabilities that includes policies, procedures, procedures, defined roles, training, and communications. This policy ensures that the Organization is prepared to effectively and quickly respond to and manage security incidents to minimize their impact.

## Scope:

This policy applies to all employees, contractors, and third-party personnel involved in the incident response process. It encompasses all departments and all locations where the Organization operates.

#### Organization shall:

### 15.1 Designate Personnel to Manage Incident Handling

Designate one key person, and at least one backup, to manage incident handling. These individuals will be responsible for overseeing the incident response process and coordinating and documenting efforts to address security incidents.

### 15.2 Establish and Maintain Contact Information for Reporting Security Incidents

Establish and maintain contact information for reporting security incidents. This includes contact details for internal incident response personnel as well as external parties such as law enforcement, third-party vendors, cyber insurance providers, and relevant regulatory and government bodies. Review and update these contacts annually.

### 15.3 Establish and Maintain an Enterprise Process for Reporting Incidents

Establish and maintain an enterprise process for the workforce to report incidents. This process should include steps for identifying, documenting, and escalating incidents to ensure they are addressed in a timely and effective manner. Include reporting timeframe, personnel to report to, a mechanism for reporting, and minimum information to be reported. Ensure this process is available to the entire workforce.

# Appendix A: Definitions

#### A

**ACL (Access Control List)**  
A list of permissions associated with an object, specifying which users or system processes are granted access to objects and what operations are allowed.

**APT (Advanced Persistent Threat)**  
A prolonged and targeted cyberattack where an intruder gains access to a network and remains undetected for an extended period, aiming to steal data.

**Asset Management**  
The process of tracking and managing physical and virtual assets to ensure they are properly utilized and protected.

#### B

**Breach**  
An incident where data is accessed, disclosed, or destroyed without authorization, resulting in the exposure of sensitive information.

**Brute Force Attack**  
A method used to gain access to a system or account by systematically trying every possible combination of passwords or keys.

#### C

**CIA Triad (Confidentiality, Integrity, Availability)**  
The fundamental principles of cybersecurity focusing on protecting data confidentiality, ensuring data integrity, and maintaining data availability.

**CSP (Cloud Service Provider)**  
A company that offers cloud-based platform, infrastructure, application, or storage services to other organizations and individuals.

**CIS Controls**  
A set of best practices for securing IT systems and data developed by the Center for Internet Security.

**Credential Stuffing**  
A type of cyberattack where attackers use lists of compromised usernames and passwords to gain unauthorized access to user accounts.

#### D

**DDoS (Distributed Denial of Service)**  
A type of cyberattack where multiple compromised systems attack a single target, causing denial of service for users of the targeted system.

**DMZ (Demilitarized Zone)**  
A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, typically the internet.

#### E

**Encryption**  
The process of converting information or data into a code to prevent unauthorized access.

**Endpoint Protection**  
Security solutions that protect endpoints, such as desktops, laptops, and mobile devices, from malicious threats.

#### F

**Firewall**  
A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

#### H

**HTTPS (Hypertext Transfer Protocol Secure)**  
An extension of HTTP used for secure communication over a computer network, typically the internet. HTTPS uses encryption protocols like TLS (Transport Layer Security) to ensure data integrity and privacy between the user's computer and the server.

**Honeypot**  
A security mechanism set to detect, deflect, or counteract attempts at unauthorized use of information systems by making the systems appear as attractive targets.

#### I

**IDS (Intrusion Detection System)**  
A device or software application that monitors a network or systems for malicious activity or policy violations.

**IoT (Internet of Things)**  
A network of physical objects—devices, vehicles, buildings—embedded with electronics, software, sensors, and connectivity to collect and exchange data.

**Incident Response**  
The approach taken by an organization to prepare for, detect, contain, and recover from a data breach or cyberattack.

#### M

**MFA (Multi-Factor Authentication)**  
An authentication method requiring two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification).

**Malware**  
Malicious software designed to harm, exploit, or otherwise compromise data or systems. Examples include viruses, worms, trojans, and ransomware.

**MITM (Man-In-The-Middle Attack)**  
A cyberattack where the attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.

#### P

**Phishing**  
A method of trying to gather personal information using deceptive emails and websites, often posing as a trustworthy entity.

**PII (Personally Identifiable Information)**  
Any data that could potentially identify a specific individual, such as name, social security number, and date of birth.

**Penetration Testing**  
A simulated cyberattack against a computer system, performed to evaluate the security of the system.

#### R

**Ransomware**  
A type of malicious software designed to block access to a computer system or data until a sum of money is paid.

**Risk Assessment**  
The process of identifying, evaluating, and prioritizing risks to an organization’s information assets.

#### S

**SIEM (Security Information and Event Management)**  
A system that collects, analyzes, and reports on security data from across an organization to detect and respond to security threats in real-time.

**SOC (Security Operations Center)**  
A centralized unit that deals with security issues on an organizational and technical level.

**SSH (Secure Shell)**  
A cryptographic network protocol for operating network services securely over an unsecured network. It is commonly used for secure logins, command execution, and data transfer.

**Spyware**  
Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

#### T

**Threat Actor**  
An individual or group that poses a potential threat to an organization's security.

**Two-Factor Authentication (2FA)**  
See **MFA (Multi-Factor Authentication)**.

**TLS (Transport Layer Security)**  
A cryptographic protocol designed to provide secure communication over a computer network.

#### V

**Vulnerability**  
A weakness in a system, network, or application that can be exploited by a threat actor to perform unauthorized actions.

**VPN (Virtual Private Network)**  
A service that encrypts your internet traffic and protects your online identity by creating a private network from a public internet connection.