
| Policy number | Title: | Effective Date: |
|---|---|---|
| <your ID format> | INFORMATION SECURITY POLICY<br>MOAP (mother of all policies) | <your date format> |

## REFERENCE

NIST CSF ID.AM, ID.RM, PR.AT, PR.DS, PR.IP, PR.PT, DE.CM,

## SUPPORTING DOCUMENTS

- **This is a contents link space for any related documentation**

## CONTENTS

## PURPOSE

This policy defines the mandatory minimum Information Security requirements for **<company name>** as defined below in Scope.This policy acts as an umbrella document to all other security policies and all associated standards.

This policy defines the responsibility to:

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
- Manage the risk of security exposure or compromise.
- Assure a secure and stable Information Technology (IT) environment.
- Identify and respond to events involving information asset misuse, loss, or unauthorised disclosure.
- Promote and increase the awareness of Information Security.

## SCOPE

This policy encompasses all systems, automated and manual, for which **<company name>** has administrative responsibility, including systems managed or hosted by third parties on behalf of **<company name>**. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

## POLICY

## 1.0 INFORMATION STATEMENT

### 1.1 Organisational Overview

Information Security requires both an Information Risk Management function and an Information Technology Security function. Depending on the IT Department structure, an individual or group can serve in both roles, or a separate individual or group can be designated for each role.

**<company name>** must designate an individual or group to be responsible for the risk management function assuring that:

- risk-related considerations for IT assets and individual information systems, including authorization decisions, are viewed as an enterprise - regarding the overall strategic goals and objectives of carrying out its core missions and business functions; and
- the management of IT assets and information system-related security risks is consistent and is considered along with other types of risks to ensure mission/business success.

**<company name>** must designate an individual or a group to be responsible for the Information Security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the designated security representative. This function will be responsible for evaluating and advising on Information Security risks.

- Information Security risk decisions must be made through consultation with both the Risk Management function and an Information Technology Security function.
- Although the Information Technology Security function may be outsourced to third parties, each entity retains overall responsibility for the security of the information that it owns.

## 1.2 Organizational Responsibilities

### Executive Management is responsible for:

- evaluating and accepting risk on behalf of **<company name>**.
- supporting the consistent implementation of Information Security policies and standards.
- supporting security through clear direction and demonstrated commitment of the necessary and appropriate resources.
- promoting awareness of Information Security best practices.
- implementing the process for determining information classification and categorization, based on industry recommended practices, organisation directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information.
- implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization.
- determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.
- participating in the response to cyber security incidents
- complying with the notification requirements in the event of a breach of private information.
- communicating legal and regulatory requirements to the wider IT team.
- communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

### The designated Security Representative(s) is / are responsible for:

- maintaining familiarity with business functions and requirements.
- assessing compliance with Information Security policies and legal and regulatory Information Security requirements.
- evaluating and understanding Information Security risks and how to appropriately manage those risks.
- representing and assuring security architecture considerations are addressed.
- advising on security issues related to procurement of products and services.
- escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures.
- disseminating threat information to appropriate parties.
- participating in the response to potential security incidents.
- participating in the development of enterprise policies and standards that considers **<company name>**'s needs.
- promoting Information Security awareness.
- monitoring networks for anomalies.
- monitoring external sources for indications of data breaches, defacements, etc.

**IT Management and IT Senior Management is responsible for:**

- supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s).
- providing the necessary resources needed to maintain a level of Information Security control consistent with this policy.
- identifying and implementing all processes, policies, and controls relative to security requirements defined by the IT security team and this policy.
- providing training to appropriate technical staff on secure operations (e.g., secure configuration).
- fostering the participation of Information Security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and
- implementing business continuity and disaster recovery plans.
- establishing and maintaining enterprise Information Security policy and standards.
- assessing compliance with security policies and standards.
- advising on secure system engineering.
- providing incident response coordination and expertise.
- maintaining ongoing contact with security groups/associations and relevant authorities.
- selecting the risk assessment approach, used based on the business needs and any applicable laws, regulations, and policies.

**The Workforce is responsible for:**

- understanding the baseline Information Security controls necessary to protect the confidentiality, integrity and availability of information entrusted.
- protecting information and resources from unauthorised use or disclosure.
- protecting personal, private, sensitive information from unauthorised use or disclosure.
- abiding by **<link to Acceptable Use Policy>**
- reporting suspected Information Security incidents or weaknesses to the appropriate manager and **<designated security representative>**

### 1.3 Separation of Duties (SoD)

- To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.
- The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

### 1.4 Information Risk Management

- Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- Information Security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- Risk assessment results, and the decisions made based on these results, must be documented.

Link to the following documents if applicable

*Risk Management Standard*
*Secure System Development Lifecycle Standard*

### 1.5 Information Classification and Handling

- All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information must be classified on an ongoing basis based on its confidentiality, integrity, and availability.
- If the information is personal identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- **<company name>** must communicate the requirements for secure handling of information to its workforce.
- For non-public information to be released outside of **<company name>**, or shared between other entities, a process must be established that, at a minimum:
    - evaluates and documents the sensitivity of the information to be released or shared;
    - identifies the responsibilities of each party for protecting the information;
    - defines the minimum controls required to transmit and use the information;
    - establishes a schedule and procedure for reviewing the controls.

Link to the following documents if applicable

*Information Classification Standard*
*Secure Disposal Policy*

### 1.6. IT Asset Management

- All IT hardware and software assets must be assigned to a designated business unit or individual.
- **<company name>** is required to maintain an asset inventory list of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- Processes, including regular scanning, must be implemented to identify unauthorised hardware and/or software and notify appropriate staff when discovered.
- A written or electronic asset inventory list of all information assets must be maintained.

Link to the following documents if applicable

*Hardware Asset Management Policy*

### 1.7 Personnel Security

- The workforce must receive general security awareness training within 30 days of hire. All cyber security training must be reinforced at least annually and must be tracked by the entity.
- **<company name>** must require its workforce to abide by the **<link to Acceptable Use Policy>**, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.
- **<company name>** is responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Link to the following documents if applicable

*Acceptable Use Policy*

### 1.8 Cyber Incident Management

- **<company name>** must have a cyber incident response policy and plan, and consistent standards to effectively respond to security incidents.
- All observed or suspected Information Security incidents or weaknesses are to be reported to appropriate management and an IT security representative as quickly as possible.

Link to the following documents if applicable

*Cyber Incident Response Policy*

*Cyber Incident Response Plan*

### 1.9 Physical and Environmental Security

- Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
- A periodic assessment must be performed for storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.
- Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
- All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.
- Visitors to information processing and storage facilities, including maintenance personnel, must be always logged and escorted.

Link to the following documents if applicable

*Physical Access Policy*

### 1.10 Account Management and Access Control

- All accounts must have an individual employee or group assigned to be responsible for account management. This will be IT.
- Access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs and each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
- Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required.
- Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
- Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and approved by a <designated security representative>.
- Information owners are responsible for determining who should have access to protected resources within their authority, and what those access privileges should be (read, update, etc.).
- Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks.
- Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

- Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored, and the user should have no expectation of privacy.
- All remote connections must be made through managed points-of-entry.
- Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

Link to the following documents if applicable

*Account Management/Access Control Standard,*

*Remote Access Standard*

*Security Logging Standard*

## 1.11 Systems Security

Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

- An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of **<company name>**.
- Security must be considered at system inception.
- Each system must have a set of access controls commensurate with the classification of any data that is stored on or passes through the system.
- Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included:
    - All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
    - All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed
    - Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
    - Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
    - Privileged access to production systems by development staff must be restricted.

    - Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

- Network Systems:
    - All connections and their configurations must be documented, and the documentation must be reviewed by the information owner and the **<designated security representative>** annually, at a minimum
- A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    - Internet accessible systems and internal systems.
    - systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems
- Network management must be performed from a secure, dedicated network.
- Authentication is required for all users connecting to internal systems.
- Network authentication is required for all devices connecting to internal networks.
- Only authorized individuals or business units (IT) may capture or monitor network traffic.

Link to the following documents if applicable

*Secure System Development Lifecycle Standard,*
*Secure Coding Standard,*
*Secure Configuration Management Standard*

### 1.12 Vulnerability Management and Operational Security

**<company name>** must have a Vulnerability Management Policy to establish the rules for the review, evaluation, application, and verification of system protections to mitigate vulnerabilities in the IT environment and the risks associated with them.

The policy must cover the following:

- Scanning and Penetration Testing
- Patching Management
- Endpoint Protection and Detection
- Logging & Alerting

Link to the following documents if applicable

*Vulnerability Management Policy*
*Patch Management Plan*

## COMPLIANCE

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

## CONTACT INFORMATION

Submit all inquiries and requests for future enhancements to the policy owner at:

[email address]

DATE ISSUED/DATE REVIEWED

| | |
|---|---|
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |