This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert entity logo by clicking on the outlined image.

Asset Management Policy Template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual’s full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual’s full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to the asset management of <organization's name>'s systems, data and information to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all assets (e.g., physical, data, business application, software and technology assets) in <organization name> and applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1 General Requirements

1-1 All information and technology assets in <organization name> must be identified and recorded.

1-2 All information and technology assets in <organization name> must be in maintained asset inventories and updated annually.

1-3 Each asset in <organization name> must have an appointed owner, responsible for the creation, maintenance and accuracy of the asset inventory.

1-4 All assets in <organization name> must be configured as per <organization name>'s Secure Configuration and Hardening Policy.

1-5 All assets must be configured in accordance with published <organization name>'s configuration processes, procedures, standards and guidelines.

1-6 All asset users and owners must read and sign the asset Acceptable Use Policy approved by <organization name> before being granted access to any asset.

1-7 Any breach of the <organization name>'s Acceptable Use Policy may lead to disciplinary action against the individual or individuals breaching the policy. Disciplinary action may include dismissal or termination from <organization name>.

1-8 Asset owners must be identified and involved within the asset management lifecycle for critical systems and their components.

1-9 Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements for asset management.

2 Definition of assets

2-1 Assets must be grouped into the following types:

2-1-1 Classified information asset, which contain classified information as "Top Secret" and "Secret" information (as defined in the <organization name>'s Asset Classification Standard).

2-1-2 IT equipment, such as servers, laptops, mobile devices, firewalls, Wi-Fi routers and VPN concentrators, etc.

2-1-3 Software and systems, such as:

2-1-3.1 Business applications such as customer relationship management (CRM), enterprise resource planning (ERP), databases and collaboration platforms.

2-1-3.2 Software and tools such as operating systems, virtualization software and productivity software.

2-1-3.3 Documentation related to critical systems.

2-1-3.4 Telework systems and associated assets.

2-1-4 Social media accounts and associated assets.

2-1-5 Third parties and suppliers and their associated assets.

2-1-6 Cloud services providers, cloud computing and hosting providers and managed services and their associated assets.

3 Asset ownership

3-1 In addition to their responsibilities mentioned above, asset owners must be responsible for:

3-1-1 Understanding, identifying and managing information risks throughout the information lifecycle.

3-1-2 Determining and approving business (including cybersecurity) requirements.

3-1-3 Addressing how cybersecurity affects operational technology.

3-1-4 Promoting cybersecurity awareness and positive security behaviors.

3-1-5 Establishing priorities, budgets and allocating resources.

3-1-6 Ensuring information and systems are protected in line with related cybersecurity controls in the organization.

3-1-7 Authorizing changes to the assets they control.

3-1-8 Supporting cybersecurity reviews and audits.

3-2 Asset owners must receive a training to enable them to carry out their role and responsibilities.

3-3 Owners of physical, business applications and software assets must be responsible and not limited to the following:

3-3-1 Creating baseline security configurations, obtaining approval, publishing the configurations for the appropriate processes, procedures, standards and guidelines.

3-3-2 Implementing the baseline security configurations.

3-3-3 Reviewing baseline security configurations at least once a year. If changes are required, owners must update the baseline security configurations, update processes, procedures, standards and guidelines and ensure the changes are implemented using <organization name>’s Change Management Policy.

4 Asset inventory

4-1 An asset inventory must be created for each type of asset as per statement 1-2 in this policy.

4-2 The asset inventory must be created in electronic format. The asset inventory can be implemented in one of the following examples: Configuration Management Database (CMDB), asset management software, specialized asset management tool, spreadsheet or database.

4-3 An asset inventory must be created for all cloud services and information and technology assets related to the cloud services.

4-4 An asset inventory must be created for critical systems and social media accounts including all information and technology components.

4-5 Asset inventories must be updated periodically or whenever a change occurs.

5 Asset classification and labeling

5-1 All <organization name> assets must be classified, labeled and handled in accordance with <organization name>'s policies and related cybersecurity legal and regulatory requirements.

5-2 Physical assets (network, IT, etc.) must be labeled with a tamper-proof label, stating the unique identification assigned to the asset.

5-3 Information in digital and paper form must be labeled in accordance with the <organization name>'s Asset Classification Standard.

6 Secure disposal

6-1 All assets owned by <organization name> must be disposed of in a secure and approved manner as per related legal and regulatory requirements.

6-2 An Asset Disposal Committee must be established, and it must supervise all disposal activities.

6-3 The disposal committee must include the asset owner and a representative of the <cybersecurity function>.

6-4 A secure disposal process for hardware, removable drives, USB devices, software, paper-based records, data, etc. must be defined, approved, and implemented.

6-5 Classified information stored on an asset must be securely wiped before the asset is disposed.

6-6 Disposal activities must be recorded and signed by the disposal committee including.

6-7 The disposal record must include all information about the disposed asset as per <organization name>'s Asset Management Standard, including but not limited to the date, asset type, quantity, label or ID, classification, asset owner, disposal method, etc.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All employee of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.