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 Standard 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 standard aims to define the detailed cybersecurity requirements related to the asset management of <organization name>'s systems, data and information to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability.

The requirements in this standard 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 standard 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>.

Standards

1	Asset inventory
Objective	To create (and maintain) a secure repository of the information and technology assets owned and managed by <organization name>. The organization may create an asset inventory for each type of asset as defined in the Asset Management Policy
Risk implication	If <organization name> does not have or maintain an asset inventory, it will: • Have an incomplete view of the assets owned and managed by the organization • Find it difficult to locate assets • Be unable to ensure that assets are up to date and being maintained as appropriate • Be unsure that it has the correct licensing or use arrangements in place

	• Be unable to protect all its assets from cybersecurity threats.
Requirements	
1-1	The asset inventory must be stored in a secure location.
1-2	The asset inventory must be protected by logical access controls (such as those defined in <organization name>'s Identity and Access Management Policy).
1-3	The asset inventory must be protected from unauthorized change by limiting access to only authorized individuals.
1-4	The asset inventory must be backed up on a regular basis and protected in accordance with the <organization name>'s backup and recovery policy and standard.
1-5	The asset inventory must be kept up to date, by adding assets once they have been owned or acquired and after they are deployed or disposed.
1-6	Details recorded in the asset inventory must be checked at least once a year for accuracy to ensure that the details are complete, comprehensive, correct and timely.
2	Asset inventory contents: critical and sensitive information assets
Objective	To record critical and sensitive information held by <organization name>
Risk implication	Having no or an incomplete inventory of critical and sensitive information will impair the ability of <organization name> to understand: • What needs to be protected • Where it is stored

	• Which legal, regulatory and policy compliance obligations are associated with critical and sensitive information • How critical and sensitive information can be protected and handled.
Requirements	
2-1	For each critical and sensitive information asset (such as a merger and acquisition contract, salary details or marketing forecasts), the following information must be recorded in the asset inventory: a) type of information being classified b) level of classification of the information as defined in the <organization name> Data Classification Policy c) date for reclassification d) compliance requirements (e.g. recording whether asset is in scope of privacy, data retention or other statutory obligation) e) systems, applications or processes that are dependent on the information for correct operation f) identity of the information owner g) asset location h) asset owner (e.g. asset custodian)
3	Physical assets
Objective	To record the physical assets owned and managed by <organization name>.
Risk implication	Having no or an incomplete inventory of physical assets will impair the ability of <organization name> to understand: • what needs to be protected • maintenance, licensing and protection requirements.
Requirements	

3-1	For each physical asset (network, IT, and specialist equipment), the following information must be collected and stored in the asset inventory: a) type of asset (such as network, IT, and specialist equipment) b) description of asset (such as firewall, server, Or PC) c) manufacturer, make and model of asset d) business purpose and/or business processes supported by the asset e) owner (e.g. the individual who is accountable for the asset) and corresponding business unit f) unique description or identifier (e.g. using serial numbers, network addresses or product numbers) g) applications supported by the physical asset h) physical location i) level of criticality to <organization name> or classification given to asset j) compliance requirements (e.g. asset is in scope of NCA or other regulator) k) systems, applications or processes that are dependent on the physical asset for correct operation
3-2	The following information may be added to the asset inventory, though it is not mandatory: a) associated hardware addresses (e.g. MAC address) b) associated network addresses (e.g. IP address) c) details of any software installed d) details of any active ports, services or protocols on the device e) whether hardware devices are approved for network connectivity f) current connectivity status (e.g. is the equipment currently connected to corporate networks) g) cybersecurity test results
4	Business applications and software

Objective	To record the business applications and software used by <organization name>.
Risk implication	Having no or an incomplete inventory of business applications and software assets will impair the ability of <organization name> to understand: • what needs to be protected • maintenance, licensing and protection requirements.
Requirements	
4-1	For business applications, the following information must be recorded in the asset inventory: a) business application name b) application version number c) application patch level d) type of application such as customer relationship management (CRM) and collaboration platforms e) business purpose and/or business processes supported by the asset f) owner (e.g. the individual who is accountable for the asset) and corresponding business unit g) information processed by each application, such as financial transaction data, sensitive business information or personally identifiable information h) technical details about each application (e.g. supplier and licensing requirements) i) cybersecurity test results j) vendor support point of contact
4-2	For software, the following information must be recorded in the asset inventory: a) name of software b) software version number c) software patch level d) type of software (e.g. operating system, productivity software)

	e) business purpose and/or business processes supported by the asset f) owner (e.g. the individual who is accountable for the software) and corresponding business unit g) technical details about the software (e.g. supplier and licensing requirements) h) cybersecurity test results i) vendor support point of contact
5	Third parties and suppliers
Objective	To record the third parties and suppliers that supply <organization name> with goods and services
Risk implication	Having no or an incomplete inventory of third parties and suppliers will impair the ability of <organization name> to understand: • the goods and services provided • the information exchanged, shared, processed, transmitted or stored with third parties and suppliers • the information and physical assets that need to be protected at <organization name> and the third parties and suppliers.
Requirements	
5-1	For each third party and supplier, the asset inventory must contain the following information: a) unique identifier b) third party or supplier name c) business purpose and/or business processes supported by the asset d) owner (e.g., the individual who is accountable for the third party or supplier) and corresponding business unit e) contract held between <organization name> and the third party or supplier f) types of goods or services provided

	g) criticality of goods or services provided to <organization name> and its operations h) third party or supplier point of contact(s)
5-2	Each contract with a third party or supplier must have an individual entry and unique identifier
5-3	For each third party and supplier, the asset inventory must contain the details of all hardware or software provided by the organization to the third party as part of the contract The inventory must contain the information required by the relevant hardware or software inventory
6	Update and review
Objective	To review the asset inventory on a regular basis and ensure it is up to date
Risk implication	If the asset inventory is out of date, then <organization name> will possess an incorrect overview of its assets, leading to missed upgrades, maintenance requirements, licensing requirements and cybersecurity status.
Requirements	
6-1	The asset inventory must be kept up to date, by adding assets once they have been purchased and before they are deployed
6-2	Details recorded in the asset inventory should be checked at least once a year for accuracy to ensure that the details are complete, comprehensive, correct and timely
6-3	The asset inventory must be reviewed by an independent organization at least every two years. This review may occur as part of annual business or financial auditing
7	Secure disposal

Objective	To dispose of IT equipment and sensitive information in digital and physical formats in a secure manner.
Risk implication	Sensitive information, trade secrets, bespoke software and algorithms can be exposed when IT equipment, documentation and paper-based records such as reports, designs and analysis studies are incorrectly disposed. Such exposure may lead to regulatory fines, loss of reputation, commercial harm and loss of trust from governments, customers and individuals.
Requirements	
7-1	Data storage (including disk drives, USB drives and removable USB devices) must be removed from all IT assets prior to disposal.
7-2	Paper-based records must be securely destroyed by using a cross-cut shredder that meets Deutsches Institut für Normung (DIN) 66399 standard as P-3 or higher
7-3	Paper-based records marked as classified “Top Secret” and “Secret” must be securely destroyed by using a cross-cut shredder that meets DIN 66399 standard as P-5 or P-6; or by incineration.
7-4	All identifying marks, such as asset tags, must be removed from any IT asset to be donated, sold or returned to a leasing organization.
7-5	All physical and hardware media assets that contained classified data must be destructed in a secure manner that ensures impossibility of data retrieve.
7-6	An approved information destruction supplier may be contracted by <organization name> to carry out the secure disposal process.

7-7	Certificates of destruction must be issued by the destruction supplier as a confirmation that the secure disposal process has been carried out.
7-8	The asset inventory must be updated with the relevant information about the disposal of the asset.
7-9	A disposal record must be created and include all necessary information about the disposal activities such as: a) Date of disposal. b) Asset disposed. c) Type of asset. d) Quantity. e) Label or ID of asset. f) Classification. g) Who oversaw the disposal. h) Disposal method. i) Certificate of destruction if carried out by a supplier.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

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

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

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

Update and Review

<cybersecurity function> must review the standard 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- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All employees at <organization name> must comply with this standard.

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