Policies around asset management

Template

Contents

[Using this document 3](#_Toc169269215)

[Authority and review 3](#_Toc169269216)

[Document control and review 3](#_Toc169269217)

[Version control 3](#_Toc169269218)

[Target 4](#_Toc169269219)

[Definitions 4](#_Toc169269220)

[Responsibilities 4](#_Toc169269221)

[Asset Owners 4](#_Toc169269222)

[Staff 4](#_Toc169269223)

[Life cycle of assets 5](#_Toc169269224)

[Inventory of Assets 6](#_Toc169269226)

[Primary assets 6](#_Toc169269227)

[Secondary assets 7](#_Toc169269228)

[(Virtual) hardware 7](#_Toc169269229)

[software 7](#_Toc169269230)

[Use and Maintenance 8](#_Toc169269231)

[Use 8](#_Toc169269232)

[Preventive Maintenance 8](#_Toc169269233)

[Corrective Maintenance 8](#_Toc169269234)

[Security of Assets 8](#_Toc169269235)

[Physical Security 8](#_Toc169269236)

[Network Security 8](#_Toc169269237)

[Access Management 8](#_Toc169269238)

[Data Protection 9](#_Toc169269239)

[Safe removal and destruction of assets 9](#_Toc169269240)

[Controlled removal 9](#_Toc169269241)

[Uncontrolled removal 9](#_Toc169269242)

[Incident Management 10](#_Toc169269243)

[Training and awareness 10](#_Toc169269244)

[Compliance and audit 10](#_Toc169269245)

[Changes and deviations 10](#_Toc169269246)

# Using this document

This document contains guidelines and examples that organizations can follow to support the development of their own policies around asset management. The template is not exhaustive. Each organization's policy around asset management should be tailored to its unique operating environment, priorities, resources and commitments. This text is intended as an example only and should not be used as the basis for your own policy around asset management.

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document Control** |  |
| Author |  |
| Owner |  |
| Date created |  |
| Last revised by |  |
| Last revision date |  |

.

## Version control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of approval** | **Approved by** | **Description of change** |
|  |  |  |  |

# Target

The purpose of this policy is to establish guidelines and procedures for the management of Assets at **[organization], in accordance with** the standards of ISO 27002, CIS Controls version 8, and IEC 62443. This policy is intended to ensure the availability, integrity and confidentiality of all physical and digital Assets of [organization**]**. A good asset management policy is a foundation for an organization's security, efficiency, and effectiveness. It provides a structured approach to managing all assets, leading to cost savings, improved security, regulatory compliance, and better risk management. All of this contributes to the overall health and success of the organization.

This policy applies to all employees, contractors and third parties involved in the use, management, maintenance or security of **[organization's]** (information) assets and industrial automation and control systems (IACS)**.**

This policy document is part of a set of policy documents that support **[Organization]** in establishing a sound cybersecurity strategy.

# Definitions

|  |  |
| --- | --- |
| **Assets** | All data, information, and information systems owned or operated by **[organization], including** hardware, software, databases, networks, domain names, (physical) documentation,... |
| **Critical assets** | Critical assets are resources or components of an organization that are essential to its operation and success. |
| **IACS Assets** | All hardware, software, network components, and information that are part of **[organization's]** industrial automation and control systems**.** |
| **Asset owner** | A designated person or team responsible for managing specific information and IACS Assets within the organization. |
| **Media** | All physical devices that store data, such as hard drives, SSDs, USB sticks, CDs/DVDs, tapes and mobile devices,... |
| **Sensitive Data** | Information that is confidential, personally identifiable, or business critical and must be protected from unauthorized access. |

# Responsibilities

Asset Owners   
Responsible for maintaining accuracy of asset records, identifying security requirements, and coordinating maintenance and repair.

Staff  
 Responsible for the proper use and maintenance of assigned information and IACS Assets and reporting any issues or incidents in line with cybersecurity policies.

# Life cycle of assets

Identifying and tracking assets is an important process. To protect a network, an enterprise must first know what is on the network. In addition, many other security controls depend on asset inventory, such as data management, secure configuration of assets, access control and more. The figure below shows the key "steps" of the Asset Lifecycle.

# 

**Acquisition/development**

* Acquisition and/or development of new assets or acquisition of new assets by transfer from another business unit.

**Discovery/monitoring/inventory**

* Identifying new assets by actively searching for systems connected to the corporate network. This process takes place continuously throughout the life cycle of an asset.

**Use**

* The authorized use of assets by users. In this document, users may be employees (whether on-site or remote), remote suppliers, contractors, service providers, consultants or other users who use assets.

**Controlled removal**

* Retire assets in a safe manner.

**Uncontrolled removal**

* Lost, stolen or otherwise unexplained assets. As a company grows, this becomes a regular problem and it is worth discussing the procedures around this before it becomes a problem

# Inventory of Assets

There should be an inventory of all relevant primary and supporting (secondary) assets. Dependencies or relationships between supporting and primary assets are also identified and kept up to date. An inventory can be automated or manual.

## Primary assets

Primary assets are the data, information and knowledge that **[Organization]** needs to carry out its activities and make decisions. They are always stored, processed or available somewhere through software, on paper or in people's minds. If primary assets are disrupted, the **[Organization]** cannot run and decisions cannot be made and management problems arise.

*\*Every Organization has a different list of primary assets, depending on the industry. The following list may be a source of inspiration:*

* your company data, orders, contracts, project data, etc.
* your customer data
* personal data of your employees
* your specific expertise
* Data about your products or technologies (e.g., source code)
* login credentials (for banking, other systems)
* all information marked as confidential
* business processes

The list should include at least the following information for each asset:

* Name
* Description
* Owner
* Classification of confidentiality, integrity and availability
* Records of the existence of personal data
* Managed by
* Supplier (if applicable)

Relevant primary assets hosted or maintained externally should also be part of the inventory and should also have an internal owner. This is usually the department responsible for the (outsourcing) contract. This vendor should be documented with contact information so it can be contacted if needed.

## Secondary assets

Supporting (secondary) information assets are software, hardware, physical infrastructure such as server rooms or other facilities, people and purchased services. These are any information and communications technologies, sites or services on which the primary assets depend.

In other words, if a support asset fails, the primary asset is also unavailable.

Support assets are assumed to support primary assets.

### (Virtual) hardware

There should be an inventory of all (virtual) hardware required for the relevant information systems. This inventory includes fixed and portable computers, servers, tablets, cell phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, network switches, routers, and other network components or devices. The inventory should include at least the following aspects:

* Asset identification code
* Date of purchase/depreciation
* Description
* Manufacturer
* Model number
* Serial number
* Firmware version if any
* Name of asset owner (e.g., administrator, user), role or business unit, if applicable.
* Physical location of company assets, if applicable
* Physical (Media Access Control (MAC)) address.
* Warranty expiration date

Enough attention should be paid to virtual assets. These are part of external (public) Cloud platforms. It is advisable to also record technical specifications, support information, customer information and vendor information, if applicable. Hardware managed externally (e.g. Cloud hardware) should meet the same requirements and data management should be contractually assured Of course, ICT asset management tools can be considered.

**Make sure administrative items-such as domain names, private Keys for certificates and other crypto-are not forgotten to include in this inventory**

### software

There must be an inventory of all software required for the relevant information systems. The inventory should include at least the following aspects:

* Name
* Description
* Owner
* Version
* License information (including contract term, number of licenses,...)
* Supplier contact information.
* Contract number.
* Optionally, you can also specify which dates the SW handles
* A distinction should be made between unsupported software and unauthorized software.

It is advisable to also record technical specifications and support information, if applicable. External administrators (SaaS) should meet the same requirements and this should be part of the contractual agreement with the external administrator.

**[The responsible department] should check the inventory of assets every six months or more often.**

# Use and Maintenance

## Use

* Users must handle all assets with care.
* **[Semi-annual]** or more frequent inspections of each asset must be performed in person or remotely unless supervisory management has authorized an exception.
* It is the responsibility of the asset owner to:
* Maintain control of the asset.
* Contact [The responsible service] in case of problems such as malfunctions, necessary repairs and underutilized equipment or loss of equipment.

## Preventive Maintenance

* Regular maintenance and updates on endpoints (laptops, desktops, workstations, servers,....) should be performed to ensure security and performance of Assets as described in the [Policy around vulnerability and patch management](https://atwork.safeonweb.be/sites/default/files/2024-03/Beleid%20rond%20het%20beheer%20van%20kwetsbaarheden%20en%20patches.docx)
* All maintenance activities should be documented. This can be kept in a separate logbook or in the pre-existing inventory.

## Corrective Maintenance

* Any defects or security incidents related to Assets must be addressed and documented immediately.
* Incidents should be analyzed and appropriate corrective actions taken to prevent recurrence.

# Security of Assets

Physical Security

Assets should be physically secured against unauthorized access, theft, and damage through measures such as access control, locks, and secure storage areas.

Network Security  
 Network segmentation should be implemented to separate critical IACS components from other network segments. Firewalls, intrusion notification systems (IDS) and other network security measures should be implemented as described in [the Network Security Policy](https://atwork.safeonweb.be/sites/default/files/2024-04/Netwerkbeveiligingsbeleid.docx) to protect the integrity and availability of networks

## Access Management

Access to Assets must be handled in accordance with [the](https://atwork.safeonweb.be/sites/default/files/2024-03/Toegangsbeleid_0.docx) organization's [Access Policy](https://atwork.safeonweb.be/sites/default/files/2024-03/Toegangsbeleid_0.docx) user responsibilities. Authentication and authorization mechanisms must be applied in accordance with [the](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx) organization's [Password Policy](https://atwork.safeonweb.be/sites/default/files/2024-03/Wachtwoordenbeleid.docx).

## Data Protection

Sensitive data should be encrypted during transfer and storage to ensure confidentiality. Backups of critical data should be made regularly as described in the [backup and recovery policy.](https://atwork.safeonweb.be/sites/default/files/2024-04/Backup-%20en%20herstelbeleid.docx)

# Safe removal and destruction of assets

Assets that are obsolete, non-repairable or economically uneconomic must be disposed of according to established procedures. All data on digital devices must be securely erased or destroyed prior to disposal.

## Controlled removal

* Assets (hardware, software) that are decommissioned or taken out of service must be returned to **[The responsible department]**.
* **[The responsible department]** should make a copy of the user data if necessary.
* **[The responsible department]** is responsible for securely erasing primary memory storage within the asset, if applicable. (encryption, shredding according to DIN-66399 standard, degausser,...)
* Remove old documents, policy notes, standard operating procedures, manuals,... and keep a log of these.
* **[The responsible department]** is responsible for updating the status of the asset within all enterprise management systems.
* Document the removal of the asset from the enterprise within the inventory of assets.
* Delete old domain names

Although the domain names may no longer be in use, it could still be a problem.

There is the possibility of domain hijacking, where expired domains are bought up by third parties, often scammers or cybercriminals. These may use the domain for malicious purposes such as phishing campaigns or posting inappropriate content. Many of these email domains still receive emails with sensitive (citizen) information and are often linked to cloud accounts (such as Dropbox, OneDrive, iCloud, Google Drive,...) that can be reset by the new owner of the domain, through the interception of password recovery links.   
When domain names are no longer in active use, it is strongly recommended that you still keep them in your own control for a transition period.

***Remember: the registration cost for a domain name is usually only a few tens of euros per year - the cost for that extra renewal does not outweigh the damage you may incur.***

**More info on managing old domain names can be found at DNS Belgium**

<https://www.dnsbelgium.be/nl/beheren-domeinnaam/niet-laten-vervallen>

<https://www.dnsbelgium.be/nl/je-domeinnaam-beheren/verwijderen>

## Uncontrolled removal

* All lost or stolen assets must be reported immediately to the **[The responsible department].**
* Business assets should also be removed from inventory.

# Incident Management

All (security) incidents involving Assets must be immediately reported and documented according to the **[organization's**] [Cyber Incident Response Plan](https://atwork.safeonweb.be/sites/default/files/2024-03/Cyber%20Incident%20Response%20Plan_0.docx)**.**

Incidents should be analyzed and appropriate corrective actions taken to prevent recurrence.

# Training and awareness

All employees should receive training on their responsibilities regarding the management and security of Assets. Regular awareness campaigns should be held to emphasize the importance of information security. There will be **4** training opportunities per year.

The content of the [10 Golden Rules of Cybersecurity](https://atwork.safeonweb.be/sites/default/files/2024-03/10%20gouden%20regels%20voor%20cyberveiligheid_0.docx) and the results of lessons learned in a cyber incident will always be taken into account when designing training opportunities.

If necessary, additional awareness campaigns will be prepared.

# Compliance and audit

Regular internal controls must be implemented to ensure compliance with this policy and relevant standards. All stakeholders must comply with applicable laws and regulations regarding information and IACS security.

# Changes and deviations

Changes to this policy must be approved by the management of **[organization].**

Variations from this policy may be granted only with the written approval of the **[Function].**