[Company]

ASSET MANAGEMENT POLICY

Assets and configuration

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Asset Management Policy

3.1 Purpose

The purpose of this policy is the identification and management of assets.

3.2 Scope

All employees and third-party users.

All company information and physical assets.

3.3 Principle

Company assets are known, identified, and managed with appropriate protection in place.

3.4 Inventory of Physical and Virtual Assets

Information and information processing, storing, and transmitting devices, both physical and virtual, are identified and an inventory of these assets is drawn up and maintained.

For each asset, at least the following, is recorded

- The asset name.
- The asset owner
- The importance of the asset

- The classification of the asset

For physical assets additionally, at least the following is recorded

- Asset number
- Serial number
- Whether in use
- Last checked by and date
- What the asset does
- A description of the information process, stored or transmitted

3.5 Inventory of Data Assets

Data and information assets are identified, and an inventory of these assets is drawn up and maintained.

For each asset, at least the following, is recorded

- The asset name.
- The asset owner
- The importance of the asset
- The classification of the asset

For data and information assets additionally, the following may be recorded

- Business Function using the asset
- Where the information is / the name of the application processing it
- Why we have the information
- Name of the controller
- Categories of data subjects
- How long we keep information / data retention
- Data Classification
- Categories of personal data
- Categories of recipients
- If international transfers take place and additional security measures
- Description of technical and organisational controls

- Lawful basis for processing
- Volume of data
- Risks to Data Subjects
- Risk Rating
- Actions to reduce or mitigate risks
- Date Last assessed
- Date of next assessment

3.6 Inventory of Software Licence Assets

Software and software licenses are identified, and an inventory of these assets is drawn up and maintained.

For each asset, at least the following, is recorded

- The asset name
- The asset version
- The asset owner
- Whether free or paid
- Number of licenses purchased
- Number of licenses used
- Location of the actual licenses
- Where the software is deployed
- Date Last assessed
- Date of next assessment

3.7 Ownership of Assets

Individuals, roles, or teams are assigned ownership of assets

Asset owners ensure assets are inventoried

Asset owners ensure assets are appropriately classified and protected

Asset owners ensure the proper handling when the asset is deleted or destroyed in line with the Information Classification and Handling Policy.

The asset owner may delegate routine tasks

3.8 Acceptable use of assets

Acceptable use of assets is in line with the Acceptable Use Policy.

3.9 Return of Assets

All employees and external party users return all organizational assets in their possession upon termination of their employment, contract, or agreement.

Where an employee or external party users purchases organization equipment or uses their own personal equipment procedures are in place to ensure all relevant information is transferred to the organization and securely erased from the equipment.

During notice periods of termination, the company controls unauthorised copying of company information by terminated employees or external party users.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.