**Asset Management Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_17dp8vu) **4**

[**Scope**](#_3rdcrjn) **4**

[**Policy**](#_26in1rg) **4**

[**Asset Types**](#_lnxbz9) **4**

[**Asset Tracking Requirements**](#_35nkun2) **4**

[**Asset Fixing**](#_1ksv4uv) **5**

[**Asset Return**](#_44sinio) **5**

[**Onboarding/Offboarding**](#_2jxsxqh) **5**

[**Onboarding**](#_z337ya) **5**

[**Offboarding**](#_3j2qqm3) **5**

[**Asset Disposal and Reuse**](#_1y810tw) **5**

[**Disciplinary actions**](#_4i7ojhp) **6**

[**Change, Review, and Update**](#_2xcytpi) **6**

[**Responsibility**](#_1ci93xb) **6**

[**Reference**](#_3whwml4) **6**

[**Related Documents**](#_2bn6wsx) **6**

# 

# Purpose

The purpose is to create effective asset management essential to the continuity, development, and growth of *[CompanyName]*, to confirm that capital expenditure by the *[CompanyName]* is planned, evaluated, authorized, implemented, monitored, and reported systematically to meet the objective of best practice.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses *[CompanyName]* information assets or information resources and services.

# Policy

* The asset management is done in Jira Asset Management Board.
* All critical assets used for *[CompanyName]* are reviewed annually in the UD Critical Asset Registry.
* All devices have the assigned user, or when the asset is not in use it stays with “unassigned” status and controlled by the Asset Manager. The temporary owner is responsible for the protection of the assigned asset.

## Asset Types

## Asset Tracking Requirements

There is a board in Jira to track the current state of assets, and Asset Manager maintains it. Description of the asset varies according to the value of the asset and its usage history.

* Asset name
* Asset number
* Asset type (labeling)
* Model
* Photo
* Short description and comments
* Usage history
* Assignee
* Status (Acquired, Issued, Under Repair, Disposed)
* More detailed characteristics (RAM, SSD, processor) - for laptops only

## Asset Fixing

The Asset Manager is accountable for fixing all information assets in the company. It can be performed at the employee’s request, or during regular asset review. When the broken asset is found, the Asset Manager approves this matter with CFO and brings it to the service center for repair.

## Asset Return

Employees must return any corporate assets, so in the case of theft or loss, they are responsible to pay a fee based on asset value.

## Onboarding/Offboarding

### Onboarding

* HR or PM creates an issue in the Jira with the necessary characteristics for the laptop (SSD, preferable OS, RAM - when the employee needs to have it for specific purposes), assigns this request to Asset Manager, and marks the first working day.
* Asset Manager prepares the laptop for a new hire:
  + Performs formatting for a chosen laptop (if not done before).
  + Checks the general state and enabled full disk encryption.
  + Installs the security packet, which includes the Splunk forwarder to do the monitoring.
  + Assigns this appliance to the new hire in the Jira Asset Management Board.
* Asset Manager gives the laptop to the new employee and confirms that he/she changes username to [First\_Name Last\_Name], and the default passwords for the disk encryption, locking.

### Offboarding

* HR or PM creates an issue in the Jira, assigns this request to Asset Manager, and marks the last working day.
* The employee brings the laptop and any other appliance to the office on the last working day and checks it with the Asset Manager.
* Asset Manager claims that the laptop and other assets are returned and confirms that in the Jira Asset Management Board.
* Asset Manager performs formatting for the returned laptop.

## Asset Disposal and Reuse

When disposing of any asset, sensitive data must be removed before disposal. Asset Manager will determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using formatting and degaussing techniques.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# Related Documents

* UD Asset Management Procedure