©(ORGANISATION NAME)

ASSET MANAGEMENT POLICY

Subject: Asset Management Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 8	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

This document is the property of CcHUB. Circulation is restricted to the Organisation’s use. It must not be copied or used for any other purpose other than for which it is supplied, without the expressed written authority of CcHUB.

Except where provided for purposes of contractual requirements, CcHUB disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is addressable by CcHUB.

CONTENTS

1.0 OVERVIEW

This policy is to ensure that the Organisation takes measures to protect its physical assets and resources. This policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when physical assets are left unattended.

1.1 PURPOSE

To establish guidelines and procedures for managing access and classification of Organisation's information assets.

1.2 OBJECTIVES

The objectives of this document include:

- To improve the security and confidentiality of information.
- To ensure that the Organisation's information and information facilities are well protected.

1.3 POLICY DETAILS

- All physical assets shall be classified based on their value and importance. The classification will help determine the necessary controls to implement.
- Classification labels (physical or electronic) shall be given to physical assets to reflect the classification based on the criticality of the information they produce and on their use.
- A criticality rating of systems into Critical, Important or Low will be carried out, according to whether the highest rating of the information's confidentiality, integrity or availability is high, medium, or low respectively. The degree of protection to be accorded each system will be determined by its criticality rating; this rating will be carried out by business owners in conjunction with IT.
  A. Critical (description of physical asset classified as critical).
  B. Important (description of physical asset classified as important).
  C. Low (description of physical asset classified as low)

- All critical physical assets shall have a nominated owner or custodian.
- Information Custodians for all critical physical assets shall be identified. The Information Custodians shall be assigned the responsibility for maintaining appropriate controls over these assets.
- Inventories of all physical assets associated with information provision shall be maintained.
- A detailed inventory listing all physical assets shall be documented and maintained.

Documentation should include:

- **Information Custodian:** Every critical physical asset shall be assigned an appropriate Information Custodian who is responsible for the information asset.
- **Identification:** Every critical physical asset shall be uniquely identified. The identification scheme used for this must ensure that:
  - The location of the information asset is known.
  - The supplier of the information asset is known (supplier information must be available)
  - Maintenance contract(s) for the information assets are identified.
- **Description:** A short description should be available for every information asset. The description should include general information on the information assets, such as its main function and use.
- **Configuration:** Technical configuration documentation should be included and supported by business requirements explaining why the physical asset has been configured as such. This documentation should include licensing information.

- Physical assets include manuals, software (applications, tools, and utilities) CDs, equipment, and media.
- A formal process shall be in place to capture critical physical assets on the inventory register when purchased, deleted, sold, or taken out of use.
- Departing employee must return all information assets and equipment belonging to the Organisation, unless agreed otherwise with the designated owner responsible for the information asset.
- Information Custodians shall be educated on their responsibilities for ensuring adequate protection of their assets; they are ultimately responsible for their assets but may allocate routine administrative and security responsibilities to a designate.

1.4 RESPONSIBILITIES

- All users are required to understand this policy and put into action.
- Head, IT is responsible for enforcing this policy.
- Head, Information Security is expected to ensure adherence to this policy.
- Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

Violations of the physical asset and control policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

2.0 ASSET INVENTORY

2.0 OVERVIEW

Asset inventory involves gathering detailed information which is used to make decisions about information assets purchases and redistribution. It helps Organisations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources.

2.1 PURPOSE

To establish guidelines and procedures for managing asset inventory.

2.2 OBJECTIVES

The objectives of this document include:

- Track and report the state of the Organisation’s information assets on a routine basis.
- Provide specific guidance for calculating and reporting on the total cost of the Organisation’s information assets throughout the asset life cycle.
- Leverage the Organisation’s purchasing power by knowing the Organisation-wide need, the volume and timing of need for future IT hardware and software purchases.
- Ensure software licence optimisation and compliance.
- Establish an initial, current and disposal value for the Organisation’s Information assets.
- Plan for a common, shared, Organisation-wide information technology infrastructure; and
- Acquire the information needed for Organisation-wide information resources management decision-making.

2.3 POLICY DETAILS

- A formal Hardware and Software Inventory of all equipment shall be maintained always and kept up to date. Where the technology exists, systems / fixed assets Organisation-wide shall be managed using an inventory management solution for effective monitoring and depreciation of IT assets.
- Hardware devices shall be named in accordance with the IT Device Naming Convention specified in the IT policy.
- Theft, loss, or damage of all physical system assets shall be communicated by custodian /relevant department to the General Service department accordingly within 48 hours.
- All Organisation owned devices must be properly labelled. The label should carry the serial number and tag number of the device.

2.4 RESPONSIBILITIES

- All users are required to understand this policy.
- IT support staff and the responsible department for asset purchase shall be responsible for implementing this policy.
- Head, Information Security is expected to ensure adherence to this policy.
- Internal Audit – IS Audit is responsible for auditing the implementation of this policy.

Violations of the physical asset and control policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

3.0 RECOMMENDATIONS/ADVISORY ON ASSET MANAGEMENT

Organisations with 1 – 5 Staff	**Organisations with 6 – 20 Staff**	**Organisations with more than 20 Staff**
● Make use of excel sheet for asset management	● Make use of excel sheet for asset management ● Make use of Open source/free asset management solutions Asset Tiger solution Shelf Asset Management Solution Snipeit	● Make use of excel sheet for asset management ● Make use of Open source/free asset management solutions Asset Tiger solution Shelf Asset Management Solution Snipeit ● Make use of Enterprise asset management solutions Manage Engine Asset Management AMI Asset Track Setyl Asset Management