**Security Policy / Procedure:**

**Asset Management**

This policy / procedure complies with the requirements of the ISO 27001:2013 International Standard

Annex A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4

**1. Purpose**

This Asset Management Security Policy and Procedure establishes the requirements and activities for identifying and controlling protected information assets and supporting technology and infrastructure assets.

 **2. Scope**

This Asset Management Policy and Procedure applies to all [Company Name] employees, contractors, and suppliers who access, use, or are assigned ownership or custody of protected information assets or supporting technology or infrastructure assets.

**3. Responsibilities**

**Asset Manager (AM)** – [Company Name] having responsibility for managing controlled assets.

* The **AM** will maintain a comprehensive Asset Management Process consistent with the overall requirements of this procedure.
* Ensure the asset is properly classified and protected.
* Ensure proper handling if the status changes or is dispositioned.
* **Asset User (AU)** – [Company Name] employee who is accountable for the appropriate use and the protection of assigned assets.
* The **AU** is responsible to report any damage, theft or loss of an asset in accordance with the HR Security Policy and the Acceptable Use Policy.

**4. Policy**

[Company Name] assures that all assets, including information and the technology and infrastructure assets supporting the processing of related data within the ISMS scope, are identified, and controlled.

[Company Name] achieves this by monitoring and tracking the acquisition, deployment, operation, removal, and disposition of assets, over their service life and/or period of [Company Name] custody, to assure information protections and security are maintained.

**5. Procedure**

# 1. Acquire and Register Asset (A.8.1.1, A.8.1.2)

Whenever an information technology asset is acquired the **Asset Manager** will capture the following information about the asset in the Asset Register.

* Identifier (ID) – is the unique identifier for the asset.
* Type – Hardware, Software or Information asset.
* Categories: Enter the category for the asset. For example, a hardware asset might be a server or a storage device, while a software asset might be an operating system or an application.
* Document the date purchased.
* Record to whom ownership and/or custody has been assigned.
* For each type of asset capture other descriptive information that will help track the lifecycle of the asset, as guided by the Asset Register drop down selections.

Examples include hardware make, model, and serial numbers; software license numbers and revision levels; and information types and classifications.

# 2. Deploy Asset (A.8.1.3)

This step refers to transportation of the asset to its operational location, and performing any planning, development, setup, configuration, and testing processes necessary to place the asset into operation with appropriate ISMS Statement of Applicability controls, and without compromising the security of any other asset. Appropriate updates to the Asset Register are made by the **Asset Manager**.

# 3. Operate Asset (A.8.1.3)

This step refers to operation of assets supporting ongoing protected information processing while maintaining ISMS Statement of Applicability controls.

If changes occur to the Asset during its operational life, for example, any reassignment of an asset or change in deployment the **Asset User** will report the change to the **Asset Manager** who will record it in the Asset Register.

In the case of the loss or theft of an asset the **Asset User** will immediately inform the **Asset Manager** or their immediate Supervisor whowill trigger a Security Incident, and the Security Incident Management process.

# 4. Remove / Dispose of Asset (A.8.1.4)

This step refers to removal and/or disposal of assets from their operating environments and/or their assigned custodian.

The **Asset User** will notify the **Asset Manager,** who will determine the planning, preparation, and takedown, without negatively impacting business operations or compromising the protective controls for any other asset.

This disposition is recorded in the Asset Register by the **Asset Manager**.

# 5. Monitor, Track, and Review Assets (A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4)

* Changes to Assets: Status changes (e.g., location, assignment, classification…) are recorded in the Asset Register by the **Asset Manager** at the time of the change and throughout the service life of the Asset.
* Monitoring of Assets: This **Asset Management Procedure** is a focus of the Internal Audit activity to assure ongoing accuracy of the **Asset Register** and compliance to the procedure.
* Review of Assets: The Asset Security Management System, and the Asset Register, are included as agenda topics for ISMS Management Review.

A Physical Inventory of all assets will be conducted annually by the **Asset Manager** with the assistance of department managers**.**

The results of these inventories will be retained by the **Asset Manager** and covered during Management Review.

**6. Asset management records**

* Asset Register

**7. Reference Documents**

* Information Security Management System (ISMS) Plan
* Information Security Manual
* Asset Register
* HR Security Policy
* Acceptable Use Policy