**Company Assets Policy**

## 

## **Objective**

The objective of this policy is to protect assets belonging to <Company Name> by preventing unauthorized use, movement, storage, disposal, lease, sharing or any such action that may lead to loss or interruption in business activities. It also minimizes the risk of sensitive information leakage to unauthorized persons.

**Scope and Applicability**

This policy applies to all individuals who have access, use or control of <Company Name here> owned resources. This includes but is not limited to <Company Name here>’s employees, contractors, consultants and other workers, including all personnel affiliated to external organizations with access to <Company Name here>’s assets or property.

**Definition/Interpretation**

| Term / Abbreviation | Definition / Expansion |
| --- | --- |
|  |  |
|  |  |

**Policy / Process**

**1. Inventory of Assets**

All procurement of Company Assets have to be routed through the Procurement Team. The assets have to be clearly identified by name, number and codes for the purpose of inventory of all assets. The asset inventory includes the following information:

√ Asset Class (Fixed, Movable, Immovable, Equipment, Machinery, etc)

√ Asset Type (Building, Vehicle, Computer, Laptop, Server, Mobile, etc)

√ HSN Code (as per Government regulation)

√ Location

√ Asset Make & Model (GE, Mitsubishi, Honda, etc)

√ Asset Owner and

√ Asset Value

**2. Ownership of Assets**

All assets and its properties are primarily owned by <Company name> and is recorded in the Asset Register and books of accounts. Internally, the Company may hand over the asset for use by its employees, who will carry the responsibility of temporary ownership. The asset owner will be responsible for:

√ Ensuring that the asset and any data or information associated with it are classified and protected as per the Asset Handling Policy.

√ Defining & periodically reviewing access controls, IT security and compliance for electronic equipment.

**3. Asset Handling Policy**

√ The most common assets that are handed over to employees for their business needs is the computers/laptops/mobile

√ Employees must ensure the safety, maintenance and upkeep of these assets

√ These assets are covered under the company’s data protection and security policy and must be adhered to at all times.

√ Employees should be aware that the data they create on the Information Systems remains the property of <Company Name Here>.

√ Employees must bear responsibility for exercising good judgment regarding the reasonable personal use of Company assets. Individuals shall be responsible for the use of Internet / Intranet services appropriately.

√ Laptop users shall agree to take shared responsibility for the security of their laptop and the information it contains.

√ The stores or IT department issuing these assets will obtain the user's details and signature on the issuing form before handing over laptops/mobiles or any such accessories.

√ For security and network maintenance purposes, authorized individuals within <Company Name Here> shall monitor equipment, systems and network traffic at any time and review them.

**4. Return of Assets**

√ All employees, contractors and third-party users will return all of the Company’s assets in their possession upon termination or change of their employment, contract or agreement as per the termination process defined in the Human Resource Policies.

√ The termination procedure includes but not be limited to:

o To return all previously issued software, documents, and equipment by <Company Name Here>. Other organizational assets such as mobile computing devices, credit cards, access cards, and information stored on electronic media shall also be returned.

o To ensure that all relevant information is transferred to the organization and securely erased from the equipment in case an employee, contractor or third-party user purchases the organization’s equipment or uses their own personal equipment.

o To document and transfer information to <Company Name Here> in cases where an employee, contractor or third-party user has knowledge that is important to ongoing business operations.

**Special Circumstances and Exceptions**

Any Deviation to this policy has to be approved by Management. Any changes to the policy have to be approved by the IT team.

**Non-compliance and Consequence**

Violation of this policy is subject to disciplinary action, up to and including termination.