

IT Asset Lifecycle Management Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Version:1

VERSION NO	REVISION DATE	AUTHOR	REVIEWED BY	. APPROVED BY	DESCRIPTION
1	15/10/2024	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed

Purpose

The purpose of this **IT Asset Lifecycle Management Policy** is to establish a comprehensive framework for managing IT assets throughout their entire lifecycle. This includes the acquisition, usage, maintenance, and eventual disposal or retirement of IT equipment. The goal is to ensure proper tracking, security, and compliance with legal, regulatory, and organizational requirements. The policy aims to enhance operational efficiency, reduce risks, and ensure that assets are disposed of securely and sustainably.

Scope

This policy applies to all IT assets owned, leased, or managed by the organization, including but not limited to:

- Hardware (e.g., computers, servers, mobile devices, network equipment)
- Software (e.g., operating systems, applications, tools)
- Licenses and subscriptions
- Peripheral devices (e.g., printers, monitors, storage devices)

It applies to all departments, teams, and individuals responsible for procuring, using, maintaining, or disposing of IT assets within the organization.

Policy Statement

The organization is committed to ensuring that all IT assets are managed efficiently, securely, and in compliance with relevant laws and regulations throughout their lifecycle. This includes the following key phases:

1. Acquisition and Procurement

- **Approval Process:** All IT assets must be procured through a centralized procurement process. Each acquisition requires approval from the designated IT or procurement department.
- **Vendor Selection:** IT assets will be sourced from approved vendors who comply with industry standards and environmental regulations.

○

Asset Registration: Once procured, all assets must be registered in the asset management system with relevant details (e.g., type, serial number, warranty information, software licenses).

2. Deployment and Usage

- **Asset Assignment:** Assets must be assigned to specific users or departments, and records must be maintained regarding the assignment.
- **Usage Guidelines:** Employees must follow company policies regarding the proper use of IT assets, ensuring that assets are only used for approved purposes.
- **Maintenance and Support:** All IT assets must be maintained according to manufacturer guidelines and company standards. Regular updates, patches, and hardware upgrades should be performed as necessary.

3. Monitoring and Reporting

- **Inventory Management:** A real-time inventory of all IT assets must be maintained. This includes tracking asset status, usage, and any changes in location or user assignments.
- **Audits:** Regular internal audits of IT assets should be performed to ensure compliance with this policy and identify underutilized, missing, or outdated assets.
- **License Compliance:** All software assets must be tracked for compliance with licensing agreements. Unauthorized software installations or violations will be addressed immediately.

4. Retirement and Disposal

- **End of Life (EOL) Management:** When IT assets reach the end of their useful life, they must be identified and flagged for decommissioning or replacement.
- **Data Sanitization:** Before disposal or repurposing, all data stored on IT assets (e.g., hard drives, mobile devices) must be securely wiped using industry-standard methods to ensure no sensitive information remains.
- **Disposal or Recycling:** IT assets must be disposed of through certified, environmentally responsible vendors who adhere to applicable laws for electronic waste disposal. A Certificate of Destruction should be obtained for all assets that are physically destroyed.
- **Documentation:** All retired or disposed assets must be documented, and the process should be reviewed to ensure compliance with data protection regulations (e.g., GDPR, HIPAA).

5. Security and Compliance

Security: The organization will ensure that all IT assets are protected against unauthorized access, theft, or damage. This includes using encryption, physical security measures, and software security tools.

- **Regulatory Compliance:** The organization will comply with all applicable legal and regulatory requirements regarding IT asset management, including data protection laws, software licensing laws, and environmental regulations concerning the disposal of electronic waste.
- **Incident Reporting:** Any incidents involving lost, stolen, or damaged IT assets must be reported immediately to the IT department for investigation and appropriate action.

6. Roles and Responsibilities

- **IT Department:** Responsible for managing the asset lifecycle, maintaining the asset inventory, ensuring asset security, and overseeing disposal.
- **Procurement Team:** Responsible for asset purchasing, vendor management, and ensuring compliance with licensing agreements.
- **End Users:** Responsible for adhering to the organization's IT usage policies and reporting issues or discrepancies with assigned assets.
- **Compliance Officer:** Ensures that all IT asset management processes align with legal, regulatory, and organizational compliance standards.

Asset Lifecycle Management Process

1. Procurement and Registration:

- Request for IT assets is submitted and reviewed by IT and procurement teams.
- Once approved, assets are purchased, logged in the asset management system, and tagged with identification numbers (e.g., barcode or RFID tags).

2. Deployment:

- Assets are deployed to employees or departments as per the assignment records.
- A proper inventory tracking system monitors the deployment status, ensuring that the correct assets are used by the appropriate individuals or departments.

3. Maintenance and Upgrades:

- Assets undergo regular maintenance, software updates, and patch management as part of an ongoing lifecycle support plan.

Older hardware may be upgraded or replaced as necessary to meet organizational needs.

4. End-of-Life (EOL) Management:

- When assets reach their end-of-life, the IT department identifies them for retirement.
- Assets are either repurposed, redeployed, or securely disposed of according to the company's disposal and data sanitization policies.

5. Disposal:

- Assets that are no longer needed are disposed of through certified recycling partners, ensuring that all sensitive data is wiped, and environmental standards are met.
- A report documenting the disposal process is generated for compliance and audit purposes.