TRANSMISSION CORPORATION OF ANDHRA PRADESH LIMITED

IT - ASSET MANAGEMENT PROCESS POLICY

Confidentiality Statement:

This IT Asset Management Process Policy document is strictly private, confidential and it is only for use by the internal purpose. This document shall not be used, disclosed, copied, published, distributed or reproduced in whole or in part without the prior written consent of APTRANSCO.

APTRANSCO reserves the right to change/ modify IT Asset Management Process Policy document at any time.

Document Control:

Document Name	IT Asset Management Process Policy - 2024
Document Reference Number	APTRANSCO / ISMS/ IT-AMPP / 01
Classification	Internal
Version Number	1.0
Date	10-09- 2024
Reviewed by	CE /Telecom & IT / VS / APTRANSCO / Vijayawada
Approved By	APTRANSCO

Version History

Date	**Version**	**Description**	**Created by**
	1.0	Initial Version Release	GICU Team / VS/ Vijayawada

TABLE OF CONTENTS

1. Introduction

Asset Management:

Asset management is the process of planning and controlling the acquisition, operation, maintenance, renewal, and disposal of organizational assets. This process improves the delivery potential of assets and minimizes the costs and risks involved

Purpose

The purpose of this process is to identify all organizational assets and define appropriate responsibilities and to ensure that the information receives an appropriate level of protection in accordance with its importance from unauthorized disclosure, modification, removal, or destruction of information stored in any form.

Scope

This procedure covers IT assets of APTRANSCO.

2. Intended Audience

This process is addressed to every person entrusted to access APTRANSCO premises and IT Infrastructure and resources including, APTRANSCO Employees, out sourced employees, Contractors, Consultants, Trainees, Vendors, Sub-contractors, Visitors, and Client representatives.

3. Inputs

- Identified IT assets in APTRANSCO.
- Information Risk Register.

4. Roles and Responsibilities

Role	Responsibilities
IT Infra	• Ensures IT assets are inventoried. • Ensures appropriate classification and protection of asset. • Ensures proper handling and disposal of assets. • Define and review access restrictions • Maintains the asset.
User	• Uses assets as per the IT Acceptable Use Policy.

5. Inventory of assets

- Asset Inventory register shall be maintained by IT Infra for all IT assets procured by IT Infra. Other Wing may buy IT/OT assets in consultation with IT Infra for use in their projects. However, assets procured by other Wing shall be recorded in asset register of IT Wing.

5.1. Hardware and Software Inventory Updating

a) IT Infra concerned / designated Support member maintains an Inventory Register for Hardware and Software.
b) Hardware includes Network Devices, Servers, Desktops, Laptops, CCTV, Exchange Server Telephone line, Printers, Fire wall, Routers and Switches etc.
c) Software includes all licenses (e.g. OS, SSL certificate, all application etc.).
d) This register is updated in the following case:
   - New hardware/software is procured.
   - Allocation of hardware is changed to another user.
   - Software is installed/un-installed from a system.
   - Disposables / Removed Hardware

5.2. Inventory Audits

- IT wing HOD assigns to Team members of IT Wing, to conduct inventory audits of Desktops, printers and other devices etc.
- Team members cross check the entry in Inventory Register.
- The system is checked for the hardware information that includes make, model, configuration, Asset ID, IP address, host name, user, and department information etc.
- In case of any discrepancy noticed by the Team members, IT wing HOD will resolve the discrepancies.
- This check is done half yearly / yearly.

5.3. Ownership of assets

APTRANSCO is whole and sole owner of all IT/OT assets.

- IT Infra being the custodian for all IT assets like servers, storage devices, network devices, IT appliances, Access control systems, etc.
- The responsibility of IT wing concerned includes:
- Ensuring that all the IT assets are inventoried.
- Ensuring that all IT assets associated with information processing facilities are appropriately classified and protected.
- Ensuring proper handling when the asset is deleted or destroyed.

For OT assets the concerned field wing are responsible.

5.4. Acceptable use of assets

- Rules for the acceptable use of IT/OT assets are defined and communicated in IT Usage Policy.
- All users having access to the IT/OT assets need to be aware of the information security requirements associated with them.

5.5. Return of assets

- All users are required to return the IT/OT assets that they have in their possession on termination of their employment, contract, or agreement.
- All the separated employee is required to return their IT/OT assets as per the Employee Separation Process (Refer- APTRANSCO/ISMS/ESP: Employee Separation Policy).
- The checklist for issue of NO DUE CERTIFICATE to separating employees.

6. Information classification

6.1. Asset Identification and Classification

Identification and Classification of IT/OT assets is done on the basis of the organisation needs and the impact of asset loss on the continuity of business. The designated concern identifies the IT/OT assets in their respective Jurisdiction / Wings.

6.2. Classification of Information

Information and Operational Assets - All information and operational assets (soft/hard copy) are classified based on their confidentiality value ('C' of CIA value) as:

"C" - Confidentiality

"CIA" - Confidentiality, Integrity & Availability.

- Restricted
- Confidential
- Internal
- Public

Restricted: Restricted information is the most sensitive form of information. It is so sensitive that disclosure or usage would have a definite impact on APTRANSCO business. Extremely restrictive controls need to be applied.

Confidential: Confidential information is a sensitive form of information. This information is distributed on a "Need to Know" basis only. This information should be made available only to specific people within the Wing.

Internal: Such information is the property of APTRANSCO. APTRANSCO have the sole right over this information. This form of information must be used within APTRANSCO and not shared externally or with third parties unless authorized to do so. Any internal

information, not confidential, that needs to be communicated to non-APTRANSCO entities will fall in this category.

Public: Sharing of such information does not have any impact on the confidentiality of the information asset and thus has a very low confidentiality rating. This form of information comes from public sources or is provided by APTRANSCO to the general public.

6.3. Labeling of Physical Assets

Physical assets – Network Devices, Servers, Desktops, printers and Laptops etc. are identified by Asset ID.

Labelling of Documents – In case of electronic documents, headers/footers are to be added to clearly indicate the labelling.

7. Media Handling

7.1. Management of removable media

- Refer APTRANSCO/ISMS/ITAUP: IT Usage Policy

7.2. Disposal of media

Implementation Guidance- Formal protocols for secure disposal of media should be established to reduce the possibility of leakage of organisation sensitive information to unauthorized persons. The protocols for the secure processing of sensitive information media should be proportionate to the sensitivity of that material.

- The storage media (CDs and DVDs) can be reused after Purge sanitization. Hence destroy the storage media by using physical destruction techniques, such as shredding, pulverizing, and incinerating, to render data recovery infeasible.
- Disposal media containing sensitive information proper measures are taken so that organisation confidentiality of information is not compromised.
- Paper documents are shredded manually as per APTransco procedures
- Hard disks are formatted after the end of their life cycle.

7.3. Physical media transfer

Control: During physical media transfer Information should be protected from unauthorized access, misuse or corruption during transportation.

- Reliable transportation i.e. in safe envelope/box. It is transported through authorized person/courier only
- Management should agree on a list of authorized couriers.
- Procedures should be established for verifying courier identification.
- Packaging should probably be sufficient to safeguard the content from any physical damage likely to occur during transit and to protect the content against environmental factors such as exposure to heat, humidity, or electromagnetic fields which could reduce media recovering efficiency.
- Transfer Logs should be maintained, the content of the media should be established, the security applied, and times of transfer to custodians and reception should be reported at the destination.

8. Output

- Assets labeled as per the Process.
- Classified and labeled for IT/OT Assets.