AP TRANSCO

TRANSMISSION CORPORATION OF ANDHRA PRADESH LIMITED

(A Government of Andhra Pradesh Undertaking)

IT & CYBER SECURITY POLICY - 2024

Confidentiality Statement:

This IT & Cyber security 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 & Cyber security policy document at any time.

Document Control

Document Name	IT & Cyber security Policy - 2024
Document Reference Number	APTRANSCO / ISP / 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 Content

IT & Cyber Security Policy for APTRANSCO

Section –I
IT & Cyber Security Policy for IT (Administrative)

1. IT & Cyber Security Policy

1.1 Introduction

- The APTransco came into existence on 1st February 1999 in the erstwhile state of Andhra Pradesh with Hyderabad as its headquarters. From 1999 to 2005 the company remained as single buyer of power from various power generators and seller to Electricity Distribution companies. Subsequently, the power purchase function was taken over by the Distribution companies.

- After bifurcation of the erstwhile state of Andhra Pradesh, the APTransco in the residual state of Andhra Pradesh started operations from June 2014 onwards. At present the headquarters of APTransco is located in Vijayawada.

- Transmission Corporation of Andhra Pradesh Limited (APTRNSCO) is one of the pivotal organizations of Andhra Pradesh, engaged in the business of power transmission in the entire State of Andhra Pradesh. Apart from operation & Maintenance of 400/220/132/33KV Sub-Stations, it has undertaken the execution of construction of ongoing & new transmission infrastructure scheduled under capacity addition programme. It is also taking up renovation & modernization works of the old sub stations.

- In Day-to-Day life, internet has made the world a smaller place, enabling instant communication with people across the globe. Email, social media, and messaging apps have redefined how we stay in touch with friends, family, and colleagues. Video calls have allowed us to see and hear ones, bridging the gap of physical distance.

- More and more companies are developing their own software to meet their IT system to their partners and suppliers. Therefore, it is essential to know which of the company's resources need protection to control the system access and the user rights of the information system. The same is true when opening company access on the Internet. Moreover, because of today's increasingly nomadic lifestyle, which allows employees to connect to information systems from virtually anywhere, employees are required to carry a part of the information system outside of the company's secure infrastructure. Industries have become a popular target for cyber criminals because of the rich rewards a data breach can yield. With the increased use of Cloud-based business transformation technologies, organizations operating in power sectors will face a diverse and evolving threat landscape, making cybersecurity more important than ever.

1.2 Vision

APTRANSCO will strive to ensure confidentiality, integrity, and availability of its Information and operation assets to meet all relevant Business, Legal, and Statutory requirements.

1.3 Mission

APTRANSCO is committed to meet the Information Security requirements of the Government of India, Government of Andhra Pradesh. IT & Cyber security policies are a set of written practices and procedures that all other stake holders including employees must follow to ensure the

confidentiality, integrity, and availability of data and resources. Creating security policies is considered to be the most critical element of an IT security program

1.4 Objective

APTRANSCO has fully digitized the official workflow and usage of email, and has integrated all the major work process in digital form. The adoption of e-Tendering has increased reliance on Internet based applications. Post Covid, all major decisions are taken via online e-Meetings. Therefore, IT applications are covering all aspects of APTRANSCO. This has added new dimension of cyber security threats when organization has gone boundary less. Hence, need has been felt to have defined IT & Cyber security policy and procedures to establish and constantly improve IT & Cyber security, in line with technology advancement at APTRANSCO.

The objectives of Cyber Security Policy are:

1.4.1 To create a security assurance framework

1.4.2 To strengthen the regulatory framework

1.4.3 To develop suitable indigenous security technologies

1.4.4 To improve visibility of the integrity of Information and Communications Technology (ICT) products

1.4.5 To enable protection of information and safeguard privacy and confidentiality of data.

1.4.6 To create a culture of cyber security

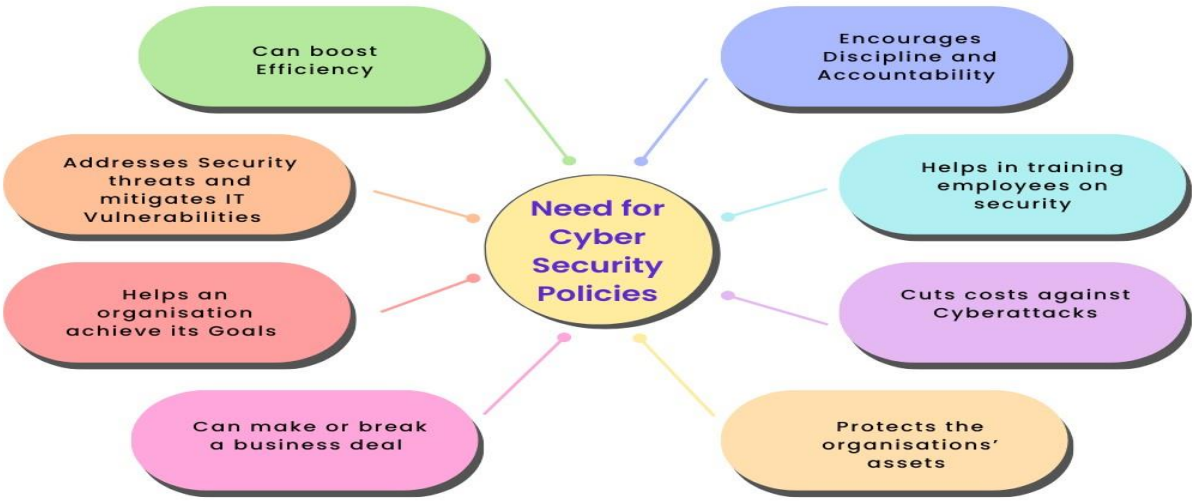
1.4.7 To deal with the Cyber threats effectively to ensure business continuity, lower downtime by quick recovery measures. Threats may belong to any of the following categories viz:

1.4.7.1 **Intentional :** Intentional Threats are malicious actions performed by malicious insiders who use technical means to disrupt or halt an organization's regular business operations, identify IT weaknesses, gain protected information, or otherwise further an attack plan via access to IT systems (i.e., intelligent; e.g., an individual cracker or a criminal organization)

1.4.7.2 **Accidental** (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado)

1.4.7.3 **Unintentional, By-chance:** In addition, poorly written software applications and scripts, not performing regular security audits, un-patched servers and network devices, inappropriate network architecture, improper segregation, allow attackers to compromise the Cyber/IT security systems or collect data from backend databases.

- **Need for Cyber security policies :** Facilitates data confidentiality ,integrity and availability, , the effective information security policies standardize the rules and processes it protect against vectors threatening data confidentiality ,integrity and availability.



- **Confidentiality:** Confidentiality protects information (data) from unauthorized access.

- **Integrity:** Integrity is the accuracy and consistency of data as well as the completeness and reliability of systems.

- **Availability:** Availability is the ability for users to access systems and information when needed, even under duress.

1.5 Scope

1.5.1 Typically, IT & Cyber security policy defines the rules to protect IT/OT related data and competing resources to achieve security objectives.

1.5.2 The policy also outlines the guidelines for IT administrator in APTRANSCO in terms of technical and managerial solutions that are required to be implemented for securing the IT & OT infrastructure and related assets.

1.6 Management of IT & Cyber Security

1.6.1 The Cyber Security management is an evolving task and it caters to the whole spectrum of APTRANSCO's users, systems and providers. The IT & Cyber Security Policy formulates the framework for defining and guiding the actions related to security of cyberspace. The policy provides specific guidelines to effectively protect information, information systems & networks of APTRANSCO. Through proper management of this policy and defined procedures, APTRANSCO aims to create a cyber-security framework, which leads to specific actions and programs to enhance the security posture of organization's cyber space.

1.6.2 The management of "APTRANSCO", is committed to ensure integrity, confidentiality, availability and security of its information at all times for serving the needs of the APTRANSCO in line with its Vision, Mission & objective, while meeting all regulatory requirements.

1.7 IT Systems in the Power Sector Segments.

As per APTRANSCO policy, which strictly prohibits Supervisory Control and Data Acquisition (SCADA) systems to be integrated logically or physically to any other IT network. These systems/networks are isolated and do not have any internet connectivity. The Substation systems have been identified and a policy document has been specifically written for security controls and practices to be implemented for them.

1.8 General Management Guidelines for Cyber Security at APTRANSCO

Cyber security standards enable organization to practice safe security techniques to minimize the number of successful cyber security attacks. These guidelines provide general outlines as well as specific techniques for implementing cyber security.

1.8.1 **Standards and guidelines**

The following general guidelines and specific standards will be used at minimum to help in benchmarking the Information Security practices in an ICT system deployed at APTRANSCO to reduce cyber security concerns.

1.8.1.1 A web application (New Application / Modification of the existing application / Trouble shooting / API's) must be Cyber security audited & certified by CERT-in empaneled auditor, before Go-Live.

1.8.1.2 Cyber Security Nodal Officer (coordinator) will coordinate all matters related to cyber/IT security in the organization and further the cause of establishing best cyber security practices at APTRANSCO.

1.8.1.3 Designated IT personnel concerned will be advised to join security forums and enhance cooperation with related Cyber security agencies, like Computer Emergency Response Team (CERT), Data Security Council of India, National Critical Information Infrastructure Protection Centre (NCIIPC), Govt of Andhra Pradesh (ITE & C department), Andhra Pradesh Technology Services (APTS), etc.

1.8.1.4 To conduct, support and enable cyber security workshops / seminars with a regular and defined periodicity, to establish APTRANSCO level, to deal with any Cyber-attack in organization, through incident management process.

1.9 Defenses & mitigating factors

It does no good to find vulnerabilities unless we mitigate or fix them. Each mitigation solution is different and is customized to particular needs.

1.9.1 **Process management:**

1.9.1.1 Continuous evaluation of vulnerabilities.

1.9.1.2 Device Configuration and Network management.

1.9.1.3 Security audit process and management

1.9.1.4 Necessary screening before choosing process for outsourcing and managing third party compliance.

1.9.1.5 Change and incident management.

1.9.1.6 Asset and Access Management, and Data Classification.

1.9.1.7 Asset owner's identification & responsibility matrix

1.9.1.8 Access Management

1.9.1.9 Data Classification.

1.9.2 **Personnel & Training Management:**

1.9.2.1 Authorized users of secured control rooms in the Power Sector should be adequately trained and certified.

1.9.2.2 Certification, work experience and personnel record of a user shall have due weightage for appointing a person with administrative permissions to critical cyber assets on "need to know" basis.

1.9.2.3 Other Users with restricted access to the critical cyber assets shall be trained for Cyber security awareness

1.9.2.4 If required, User system activity will be logged and be available for review.

1.9.2.5 Conducting Awareness training on Cyber security at End user level, to acquire specific knowledge and skills for a particular job or task. It is usually a short-term activity concerned with improving an employee's current job performance.

1.9.3 **Countermeasures for Cyber Security:**

- In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or attack, eliminating or preventing it by minimizing the harm it can cause. It can also include discovering and reporting vulnerabilities so that corrective action can be taken.

- Technology & defense should be in place, as far as possible as specified below:

1.9.3.1 IT Application – Application Screening, Application Hardening, Antivirus.

1.9.3.2 OS - Operating system and application security patches must be up to date.

1.9.3.3 Host – OS hardening, Authentication, Patch Management. No local administrator privilege to end users.

1.9.3.4 Internal Network – network Segmentation, Intrusion Prevention System, Network Intrusion Detection System (NIDS), Network Access Control (NAC).

1.9.3.5 Perimeter – Next Gen Firewalls, VPN, Next Gen IPS.

1.9.3.6 Physical Security – Guards, Locks, Electronic Security Surveillance.

1.9.3.7 Policy, Procedures & Awareness – Admin & User Education

1.9.3.8 Implement policy for acceptable usage of mobile devices.

1.9.3.09 User Awareness and training.

1.9.3.10 Use of genuine and latest Operating system and Software's

1.9.3.11 Do not follow unsolicited web links or attachments in email messages

1.9.3.12 Exercise caution while visiting/ accessing links to Web pages

1.9.3.13 Not visiting / accessing untrusted websites

1.9.3.14 To download applications from the trusted sources under the guidance of IT Wing with the approval of CISO/ Framework for adopting of open-source software in e-Governance systems issued by MeitY.

1.9.3.15 Auto-play feature as a safe practice should be Disabled.

1.9.4 **Establish Acceptable System Usage**

1.9.4.1 Install and enable:

a) Personal System firewall

b) Anti-virus / Anti-spyware

c) Host-based firewall.

1.9.4.2 Keep up-to-date patches and fixes on the operating system and application software

1.9.4.3 Enable/Install anti-phishing toolbars such as “Phishing Filter”, “Web Forgery” etc.

1.9.4.4 Use latest Internet Browsers having capability to detect phishing/malicious sites.

1.9.4.5 Exercise caution while opening unsolicited emails and not to click on a link embedded within

1.9.4.6 Only open email attachments from trusted parties

1.9.4.7 Practice limited account privilege.

1.9.4.8 Report suspicious emails/system activities to CISO

1.9.5 **Risk Assessment**

1.9.5.1 IT wing will perform continual cyber security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

1.9.5.2 Risk assessments will be conducted on any entity within APTRANSCO. RAs will be conducted on APTRANSCO IT/OT systems, to include IT applications,

servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

1.9.6 **Webserver Security guideline**

Web servers are often the target of numerous exploit attempts. When improperly secured they introduce a significant risk to the networked computing environment. The APTRANSCO IT Management will establish basic steps to follow to secure a Web server environment.

1.9.6.1 Responsibilities and Procedures

1.9.6.2 Patch and/or upgrade operating system on routine basis.

1.9.6.3 Administrators need to monitor appropriate mailing lists and/or web sites for security-related announcements.

1.9.6.4 Configure the operating system to meet system best practices. This includes but is not limited to the following:

1.9.6.5 Enable necessary services and applications, Disable all others.

1.9.6.6 Create user accounts following the principle of least-privilege

1.9.6.7 Set all account passwords appropriately to meet APTRANSCO's password policy.

1.9.6.8 Remove or disable unneeded default accounts

1.9.6.9 Change any default passwords as installed by application software to meet APTRANSCO's password policy.

1.9.6.10 Configure Web server to meet recommended best practices.

1.9.6.11 Install the Web server software on a dedicated host

1.9.6.12 Enable necessary web services; Disable all others.

1.9.6.13 Apply any patches or upgrades for known vulnerabilities

1.9.6.14 Web servers should be configured to prohibit access to files that may not be intended for public consumption.

1.9.6.15 Create log files for future investigations and/or recovery purposes.

1.9.6.16 Establish different log file names for various virtual Web sites that are part of the same single physical Web server

1.9.6.17 Ensure mechanisms are in place to prevent log files from filling up the hard drive

1.9.6.18 Ensure the log files capture failed login attempts, account privilege changes and/or other potentially suspect activities

1.9.6.19 Only authorized personnel shall have access to web server logs.

1.9.6.20 Separate Web server content and related subdirectories from operating system and application directories.

1.9.6.21 Perform regular backups of Web content and occasional backups of operating system and application configurations.

1.9.6.22 Employ Web authentication and encryption technologies such as SSL/TLS based upon the nature of Web server data (e.g., restrictive, confidential, internal etc.).

1.9.6.23 Establish internal change control methodology.

1.9.7 **Business Continuity Plan**

The Business Continuity Plan (BCP) for addressing cyber terrorism and other threats describes the framework for incident response coordination among Departments of APTRANSCO. The BCP will define disaster recovery sites, data backups, role & responsibility, mock drills etc. The BCP practice at APTRANSCO will establish an overall cyber-security risk management framework, whereby preventive and detective controls based on risk assessment will be implemented, monitored and continually improved.

1.9.8 **Vulnerability Management**

It is a continuous, proactive, and often automated process that keeps computer systems, IT networks, and IT applications safe from cyberattacks and data breaches.

1.9.8.1 APTRANSCO has a defined process for notification, testing, and installation of security-related patches on devices connected to APTRANSCO's networks.

1.9.8.2 Authorized IT Security Officials conduct routine scans of devices connected to APTRANSCO networks to identify vulnerabilities. These activities may also be outsourced to specialized agencies.

1.9.8.3 Exceptions to vulnerability scanning may be granted for systems with alternate security measures in place to mitigate risk. Any such requests must be submitted in writing to the CISO for review and obtaining approval from APTRANSCO Management.

The Exception requests must be included.

a) Why the scanning exception is being requested.

b) Risk to the enterprise, if not scanning the device.

c) Mitigation controls that have been implemented, and date of implementation.

d) End date for the exception.

e) In the case of systems or applications managed by IT staff, endorsement of the request by the relevant IT staff

1.9.8.4 The exception list maintained by the CISO and is reviewed before each BCP test cycle.

1.10 Non-Compliance to IT & Cyber Security Policy

The Non-compliance to IT & Cyber security policy may attract, at the full discretion of the APTRANSCO, disciplinary action, as per the IT-Act Policy.

1.11 Do's and Don'ts of Cyber Security Policy

DO'S	DON'TS
• Implement Strong Authentication: Use multi-factor authentication (MFA) for all administrative accounts to enhance security.	• Don't Use Default Credentials: Avoid using default usernames and passwords for systems and devices; always change them to strong, unique credentials.

- Regularly Update and Patch Systems: Ensure that all software, operating systems, and applications are kept up-to date with the latest patches and updates.
- Monitor Network Activity: Continuously monitor network traffic for unusual or suspicious activities using security information and event management (SIEM) systems.
- Conduct Regular Security Audits: Perform regular security audits and vulnerability assessments to identify and mitigate potential risks.
- Don't Ignore Alerts: Do not ignore security alerts and notifications from your security systems; investigate and respond promptly.
- Don't Overlook Physical Security: Avoid sharing administrative credentials with others; use individual accounts for each administrator.
- Don't Delay Updates: Do not delay applying security patches and updates, as this can leave systems vulnerable to exploitation.

1.12 Point of Contact:

Chief Information Security Officer (CISO)

2. Access Control Policy

2.1 Objective

Access control policy has been designed to help IT Wing to decide on the level of access required by a user and assign the rights and permissions accordingly.

2.2 Scope

The policy covers the access control for information systems and services in the organization.

2.3 Policy

2.3.1 To access systems and facilities by all users, appropriate access rights shall be provided by the System administrators.

2.3.2 The access rights to be given to a user must be forwarded by the head of IT Wing. The system administrator will provision the access right only on receiving the approval from the CISO.

2.3.3 Access creation activities shall be recorded in an Access Control List and marked as confidential document.

2.3.4 Access controls shall be set at an appropriate level to maintain availability and minimize information security risk.

2.3.5 All users shall be assigned rights and permissions based on the requirements of the roles and responsibilities of the employees.

2.3.6 All Access failure events for critical servers shall be logged to identify misuse of systems or information. The logs will be saved centrally and will be available for review for any incident. The logs will be retained for a minimum of Six Months.

2.3.7 Systems logs or application audit trails are disclosed only to the authorized personnel or those who investigate information security incidents.

2.3.8 The HR wing concerned shall inform to Head of IT wing within 24 Hours, about the resignation, superannuation etc for updating the details.

2.3.9 System Administrator shall carry out the required changes in the Access Control privileges and update/delete the rights and permissions assigned on the IT system.

2.3.10 In case of any threat to the security of the systems or network from the resources being used by a user, the resources being used may be deactivated immediately by IT Wing.

2.3.11 Unique user IDs and Passwords should be given to enable users to be linked to and held responsible for their actions. In case of new user creation, the password is set to default with 'change password at next logon.

2.3.12 User access rights should be reviewed by IT Wing HOD on quarterly basis / whenever is required or immediately as information is received from HR. HR shall report change in employment status as per clause 2.3.8

2.3.13 Authorization for special privileged access to System Administrator and Application rights should be reviewed for critical servers within one day of the last audit.

2.3.14 Privileges should be allowed to users on a need-to-use basis in line with the access control policy i.e., the minimum requirement for their functional role only when needed.

2.3.15 The access privileges associated with each system product e.g., operating system, database management and each IT application, and the users to which they need to be allocated should be identified and approved in written document or through software (as the case may be). The same should be recommended by concerned wing.

2.3.16 An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.

2.3.17 Password Policy though being a part of Access Control has been separately framed and defined by the organization.

2.3.18 Firewall/proxy server shall necessarily be setup for restricting the unauthorized access.

2.3.19 Password protected screen savers should be enabled after a predefined time of inactivity; and educating the users on locking the workstation and locking all business related physical papers, while going away from workstation.

2.3.20 The user accounts which are not used for a period of consecutive 60 days shall get locked automatically.

2.3.21 Only those Employees who “need-to-know” or require access to function in their role should have access to Personal Data only.

2.3.22 The disclosed Personal Data will be strictly limited to what is necessary and reasonable to carry out the Agreed Purposes.

2.3.23 Processing of Employee data i.e., modifications, corrections, sanctions, approvals with proper permissions.

2.4 Access Control to Program Source Code

2.4.1 To prevent any corruption of the application program, the access to program source library of the operational application system is restricted to only authorized personnel.

2.4.2 Access to production programs is given to developers.

2.4.3 The source libraries of the operational systems are maintained by the development teams.

2.4.4 Maintenance and copying of program source libraries are done by only authorized personnel.

2.4.5 Adequate training to be given to the application developers on secure coding practices.

2.1.6 Vulnerability Assessment must be done at code level.

2.5 Do's and Don'ts of Access Control Policy

DO'S	DON'TS
• Implement Access Controls: Enforce the principle of least privilege, granting users and administrators only the access they need to perform their jobs	• Don't Use Default Credentials: Avoid using default usernames and passwords for systems and devices; always change them to strong, unique credentials
• Backup Critical Data: Ensure regular backups of critical data and systems are performed and stored securely, with periodic tests of backup integrity.	• Don't Ignore Alerts: Do not ignore security alerts and notifications from your security systems; investigate and respond promptly.
• Log and Review Activities: Keep detailed logs of administrative activities and regularly review them.	• Don't Overlook Physical Security: Do not neglect the physical security of servers and network equipment.

2.6 Point of Contact

CISO/Designated Authority

3 Endpoint Security/Anti-Malware policy

3.1 Objective

Endpoint Security/Anti-Malware policy aims at creating and maintaining a virus-free work environment at APTRANSCO without exception, Endpoint Security/Anti-Malware software's is to be deployed with regular virus definition updates and scanning across the servers, PCs and laptop for accessing APTRANSCO network.

3.2 Scope

This policy applies to all computers like desktop computers, laptop and computers that access the APTRANSCO network

3. Policy

3.3.1 There shall be single corporate standard End-Point Security/Anti-Malware solution across the organization. This shall be centrally managed for connected locations.

3.3.2 IT Wing should ensure that End-Point Security/Anti-Malware software is installed on all servers, gateway and client and would always be active.

3.3.3 Antivirus at the gateway would detect and remove viruses from inbound and outbound SMTP, FTP, and HTTP traffic in real time

3.3.4 The Gateway should stop any message containing VBS (Virtualization-based Security) scripts as attachments - this prevents viruses.

3.3.5 The Gateway anti-virus system should stop any message containing any executable programs e.g. .EXE files, as attachments to prevent Trojans and viruses.

3.3.6 Anti-virus solution deployed shall be widely accepted antivirus solution.

3.3.7 Anti-virus solution deployed shall provide for facility to generate periodic reports for reviewing by the security administrator and take appropriate actions.

3.3.8 Install security appliance like Firewall, Anti Spy ware, IDS / IPS etc. at Gateway level to avoid unsuspected attacks.

3.3.9 Antivirus software should be installed with administrator control on end user systems and must be configured for real time scanning.

3.3.10 All clients should be controlled using the centrally manageable Anti-Virus Server.

3.3.11 The scheduler should run the AV (Anti-virus) software at least once in a day and it should be properly scheduled, preferably during the lunch hours of the office. Users should not be able to stop the Anti-virus check.

3.3.12 All Endpoint devices capable of running an antivirus software program are required to do so before connecting to the APTRANSCO's internal network. Additionally, any such antivirus software must be running the latest virus definitions to accurately detect the latest viruses and malware, and be set to automatically update when newer definitions become available.

3.3.13 Disabling or removing of Antivirus software, or disabling of Antivirus software definition updates on endpoints is prohibited.

3.3.14 All Endpoint devices capable of running local Firewall software are required to do so to protect the device from external threats such as hacking by unauthorized parties.

3.3.15 Always delete the drive securely to clear the contents.

3.3.16 Make sure that there is no hidden file and folders present in the media.

3.4 Updating End-Point/ Anti-Malware Definitions (Files) Patches.

3.4.1 Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so.

3.4.2 Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.

3.4.3 End-point/Anti-Malware software's shall automatically update all the computers with the latest patches.

3.4.4 There shall be weekly reporting about regular updating of new patches**.**

3.4.5 There shall be immediate reporting of any attack that has occurred to the network admin of IT Wing.

3.5 Do's and Don'ts of Endpoint Security/ Malware Policy

DO'S	DON'TS
• Install and Update Anti-Malware Software: Ensure that all endpoints have reputable antimalware software installed and regularly updated to protect against the latest threats.	• Don't Disable Security Features: Avoid disabling anti-malware software, firewalls, or other security features for convenience, as this exposes endpoints to threats.
• Enable Real-Time Protection: Enable real-time protection features in antimalware software to detect and block threats as they occur.	• Don't Ignore Security Alerts: Do not ignore alerts and notifications from endpoint security solutions; investigate and respond to them promptly.
• Regularly Scan Systems: Schedule regular full system scans to detect and remove any potential malware.	• Don't Overlook Network Segmentation: Ensure proper network segmentation to prevent the spread of malware across the network.

3.6 Point of Contact

CISO/ Designated Authority

4 Backup Policy

4.1 Objective

Day-to-day data storage must ensure that current data is readily available to authorized users and that archives are both created and accessible in case of need. Backup policy shall provide guidelines to the users and the IT Wing for the purpose of backing up data and systems as per the requirements of APTRANSCO. Backup of Centralize data at APTRANSCO premises is the responsibility of IT Wing. However, backup of user data is the responsibility of concern / respective users or user department through local IT Team.

4.2 Scope

This policy covers all IT and OT related data including Servers, Database, e-mail. Any non-corporate data assets are considered out of scope of this backup policy.

4. Policy 3

4.3.1 Identify a dedicated Backup Administrator who shall maintain a register of all critical servers, application packages & Databases for which a regular backup is required.

4.3.2 Backup Administrator shall ensure:

4.3.2.1 The availability and reliability of the data/information, when and where required by taking regular backups.

4.3.2.2 The regular backups of all the data/applications. The backups are updated as and when any change or update patch is applied to the system.

4.3.2.3 All the backup activities shall be properly documented.

4.3.3 Testing the backup media:

4.3.3.1 Data and system files that are backed up and backup of data files shall be tested. Any discrepancies or errors found during the backup testing shall be reported to the database administrator/ system administrator and also to the concerned departmental head. The test results shall be documented and the backup process modified to avoid similar discrepancies in future.

4.3.4 Management should ensure that backup media of database is maintained at an offsite location in a secured fire-rated cabinet and moisture-free environment and preferably at a different & far location from Data center.

4.3.5 The backup media must have label as per labeling convention e.g., Backup type, date etc. Backup media should be labeled to a consistent standard and should comply with the information classification requirements.

4.3.6 The backup media is not used for any other purpose except either for updating the backup or for restoring the data. Drives available for taking backups/restoration shall be enabling only at the time of taking/restoring backups by authorized officers only. These must be disabled immediately after the backup/restoration operation is complete.

4.3.7 Backup Policy should include procedures to be followed on receiving the backup media at offsite location.

4.3.8 Formal guidelines should be defined for backup scheduling, storage and retention processes such as Backup media shall be erased/ zeroed before sending for repairs, disposal for preventing retrieval of any data from such media. A retention schedule shall be drawn up identifying records and the period of time for which they should be retained.

4.3.9 All offline/ archived information should be made available to the authorized user/ regulator or any other statutory authority when requested. Access to the archived data shall be provided after the written approval of concerned business head and CISO.

4.3.10 The list of media going offsite and the coming from the offsite location will be documented.

4.3.11 Data Life Cycle Management – This refers to a framework that standardizes data processes in the organization, from data creation through storage and archiving until its final deletion.

4.3.12 Data Back-up and Recovery – This includes the backup support mechanisms for data once data is created.

4.3.13 Data Access Management Controls – This includes that the data related shall be used only by authorized user/s. The records of the same shall be kept IT department.

4.3.14 **Backup Frequency**

4.3.14.1 One Time backup

4.3.14.1.1 Systems software loaded on APTRANSCO server(s) shall be backed up and stored both onsite and offsite so that in case of a system crash, the downtime of server is maintained at the minimum level.

4.3.14.1.2 Backups shall be updated as and when; any change or update patch is applied to the system.

4.3.14.2 Scheduled Backup

4.3.14.2.1 Daily incremental backup shall be performed for all the servers including the database server. The backup tapes/media shall be rotated on a weekly basis.

4.3.14.2.2 Weekly differential backup shall be performed for all the servers including the database server. The backup tapes/media shall be rotated on a bi-monthly basis.

4.3.14.2.3 Monthly full backup shall be performed for all the servers including the database server and the backup tapes/media shall be rotated on yearly basis.

4.3.14.2.4 Yearly full backup shall be performed for all the servers and tapes/media shall be sent to the archive library.

4.3.15 **Restoration**

4.3.15.1 A request with approval from the functional /departmental head shall be forwarded to the IT Wing for any restoration requirement.

4.3.15.2 Backup Administrator shall be responsible for restoring the data/system from the backup tapes/media and shall log all the activities in a register maintained at the respective location.

4.3.15.3 Procedure to be followed for Restoration failure:

4.3.15.3.1 Inform the CISO about any such event.

4.3.15.3.2 Inform all concerned users about this failure and simultaneously file a complaint to the respective vendor.

4.3.15.3.3 After informing the above, try and rectify the problem in-house by ways of troubleshooting.

4.3.15.3.4 Else access and restore the data from the Tape/Media.

4.3.15.3.5 If reformatting is required, make sure that backup exists.

4.3.16 **Data Back-up Content.**

4.3.16.1 Data to be backed up should include the following information:

4.3.16.1.1 User data stored on the hard drive.

4.3.16.1.2 System data

4.3.16.1.3 The registry

4.3.16.2 Systems to be backed up include:

4.3.16.2.1 File server

4.3.16.2.2 Mail server

4.3.16.2.3 Production web server

4.3.16.2.4 Production database server

4.3.16.2.5 Domain controllers

4.3.16.2.6 Test database server

4.3.16.2.7 Test web server

4.3.16.2.8 Application server

4.3.17 **Tape/Media Storage Locations**

Offline tapes/Media used for daily backup shall be stored in another location.

4.4 Backup Guidelines

4.4.1 Backup of all ERP Database and e-mail must be retained such that all systems are fully recoverable. This may be achieved by using a combination of different cartridges/media with full, incremental, differential backups or other techniques.

4.4.2 At a minimum, one fully recoverable version of all the complete data must be stored in a secure, off-site location.

4.4.3 All cartridges/media whether onsite or offsite will be at a secure location. Proper environmental controls, temperature, humidity and fire protection, will be maintained at all storage locations.

4.4.4 All backup cartridges/media that are not re-usable will be thoroughly destroyed as per Removable Media Policy.

4.4.5 Windows hosting server shall be fully backed up every end of the month.

4.4.6 Configuration files of firewall, switches, routers etc., shall be backed up from the Backup server to a Tape Drive / or respective media.

4.4.7 Proper documentation of Disaster Recovery will be documented with backup of OS and configuration.This will be kept at the off-site secure location. DR files for the following will exist:

4.4.7.1 Windows Server

4.4.7.2 Linux Server

4.4.7.3 Anti-Virus

4.4.7.4 Anti-Virus Backup

4.4.7.5 Mail server backup

4.4.7.6 ERP Server

4.5 Backup Monitoring

4.5.1 Administrator will monitor the backup operations and resolve all contentions. Every Backup failure is recorded and analysis is performed on it with cause effect analysis

4.5.2 IT Wing will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

4.6 Do’s and Don’ts in Backup Policy

DO’S	DON’TS
Implement Regular Backup Schedules: • Establish and adhere to regular backup schedules, ensuring that all critical data is backed up consistently.	**Don’t Ignore Backup Failures:** • Do not ignore or postpone addressing backup failures; investigate and resolve issues promptly to ensure data protection.
Use Redundant Storage: • Store backups in multiple locations,	**Don’t Disable Backup Notifications:** • Avoid disabling notifications and alerts

including off-site or cloud storage, to protect against physical damage or localized data loss.

Test Backup Restorations:

- Regularly test backup restorations to verify the integrity and reliability of the backup data.

Monitor Backup Processes:

- Use monitoring tools to track backup processes and receive alerts for any failures or issues.

from backup systems, as these are critical for timely awareness of issues.

Don't Share Backup Credentials:

- Do not share access credentials for backup systems; ensure that access is controlled and monitored.

Don't Allow Unencrypted Backups:

- Never store backups without encryption, especially if they contain sensitive or confidential information.

4.7 Point of Contact

CISO/ Designated Authority

5 Desktop Security Policy

5.1 Objective

All desktops shall adhere to this policy to ensure desktop security and organization security as a whole, since desktop in the organization contains critical documents and information.

5.2 Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information. This policy and all standards apply to all protected systems in any form.

5.3 Policy

5.3.1 The purpose of the Policy is to protect the organization's information and operational assets from all threats, whether internal or external, deliberate or accidental.

5.3.2 All desktop computers and laptops shall be installed with latest antivirus software.

5.3.3 Boot level (ROM based) password shall be enabled on the system while issuing PC to user / while installing new Operating system in to computer.

5.3.4 Design a Screen saver with IT guidelines for usage of PC & make it mandatory to be used as screen saver for all employees' computers.

5.3.5 Provide Uninterrupted Power Supply to all the PCs to prevent damage to Computer Hardware, Software and data due to power fluctuation.

5.3.6 User authentication shall be enabled for any user to login to the desktop and access IT systems.

5.3.7 There shall be no Floppy Disk Drive/CD(R/W) in any desktop except identified desktops.

5.3.8 Physical movement of desktops/Server/networking equipment shall be only done by the IT Wing. All records of such movement must be maintained.

5.3.9 All critical desktops shall have latest Operating System installed.

5.3.10 Enforce Software installation restriction to all computers (through active directory).

5.3.11 Enforce Download of executable files restriction to all computers (through proxy).

5.3.12 Enforce Execution of unknown program files restriction to all computers (through active directory).

5.3.13 Enforce Sharing of hard disk drives or other folders restriction.

5.3.14 Usages of USB/COM ports shall not be allowed strictly, allow on need basis only.

5.3.15 While installing the Operating System, only the utilities/services required by the user shall be installed/ enabled.

5.3.16 Unwanted services/processes, which come installed by default, shall be removed immediately after installation of Operating System and Applications by the installer of the computer.

5.3.17 Logging of user activities on the desktops shall be enabled.

5.3.18 Sensitive Organizational Data inside official laptop issued for official purpose should be encrypted.

5.3.19 A logical port holds the key to security and its consequences.

5.3.20 Every logical port is vulnerable to a system threat, but some commonly used ports require more attention from malicious hackers.

5.3.21 Preventing spoofing and impersonation by unauthorized network devices.

5.3.22 The elimination of network loops and broadcast storms caused by malicious devices.

5.3.23 Block the open or unused port. In case of any requirement/ emergency the procedure as laid in Access management be followed.

5.3.24 Enable ports and services, which are required for normal operations (physical port/ Logical Port).

5.4 Do's and Don'ts of Desktop Policy

DO'S	DON'TS
Standardize Desktop Configurations:	**Don't Allow Unsecured Devices:**
• Use standardized configurations for all desktops to ensure consistency, ease of management, and security.	• Avoid connecting unsecured or unauthorized devices to the corporate network.
Enforce Strong Password Policies:	**Don't Use Default Configurations:**
• Require strong, complex passwords for desktop login and enforce regular password changes.	• Do not rely on default settings for operating systems and applications; customize them to enhance security
Use Endpoint Protection:	**Don't Ignore Security Alerts:**
• Install and maintain endpoint protection software (antivirus, anti-malware, firewall) on all desktops.	• Do not ignore security alerts from desktop protection software; investigate and address them promptly.
Enable Automatic Locking:	**Don't Disable Security Features:**
• Configure desktops to automatically lock after a period of inactivity to prevent unauthorized access.	• Avoid disabling security features such as firewalls, antivirus, or automatic updates.

5.5 Point of Contact

CISO/Designated Authority.

6 Internet Access and Email Usage Policy

6.1 Objective

Internet & E-mail facilities shall be used for official purposes, using criteria which are consistent with other forms of business communication.

6.2 Scope

This Internet Access and E-mail Usage Policy apply to all employees of APTRANSCO who have access to computers and the Internet to be used in the performance of their work. It states what is allowed and what is not with procedures to minimize risks.

6.3 Policy

6.3.1 Internet Access Policy

6.3.1.1 The users are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted

6.3.1.2 The users should be aware of the risks to the organization from downloading and uploading information/ Software from Internet.

6.3.1.3 The users should be aware of the authorized and unauthorized usage of Internet.

6.3.1.4 The users should be aware of not disclosing any information related to APTRANSCO in any Electronic media, public news group, forum or bulletin board.

6.3.1.5 Proxy server(s) or any other appropriate technological solution shall be installed and configured and all the access to Internet shall be controlled through the same.

6.3.1.6 Internet access to the employees shall be provided on a need-to-have basis as per the APTRANSCO IT policy.

6.3.1.7 Ensure that all employees with Internet access (including E-Mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet.

6.3.1.8 Proxy Servers or any other appropriate technological solution may use appropriate authentication scheme like use of user ID and passwords etc. for authenticating the user connecting to Internet.

6.3.1.9 Use of Instant Messenger services are strictly prohibited except authorized IM only for official purposes and with prior approval of HOD/ IT Wing.

6.3.1.10 System Administrator retains the right to access any data stored by the end user if needed with the permission of HOD / IT Wing.

6.3.1.11 Security mechanisms shall be deployed at gateway level to allow only the Approved services and network ports, restricting unauthorized access, inspection of the traffic for malicious content and intrusions.

6.3.1.12 All internet traffic shall be scanned and blocked if found infected at the gateway.

6.3.1.13 Content and URL filtering shall be configured at the gateway. This shall be done to restrict users from visiting sites other than those required for business purposes.

6.3.1.14 Modems / USB data card/ Mobile data shall not be allowed to use in APTRANSCO network for the purpose of connecting to the Internet by the end users.

6.3.1.15 In case a requirement driven by a business need arises, the computer being used to dial-up to connect to the Internet or a third-party network shall be disconnected from the corporate network. This shall require an approval from the CISO.

6.3.1.16 Conduct a threat-and-risk assessment prior to allowing internet access to protect departmental systems and information resources. The threat

assessment will consider the sensitivity of the departmental information and system resources at risk and the risks of providing access to the Internet.

6.3.1.17 Web monitoring software should not be used to spy on employees, but to verify that employees can be trusted to follow policies and to work efficiently during business hours.

6.3.1.18 All sites and downloads may be monitored and/or blocked by IT Wing if they are deemed to be harmful and/or not productive to business.

6.3.1.19 All systems on the intranet should be regularly updated with latest patch, OS, anti-virus anti-malware and security signatures etc.

6.3.1.20 Movable devices e.g., pen drives, hard drives etc. should be either prohibited in the intranet or should be assigned proper permissions after verification. Their usage should be monitored.

6.3.1.21 All the IT systems on the intranet should be hardened to perform only the minimum desired services.

6.3.1.22 Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

6.3.2 Email Usage policy

6.3.2.1 Size of external (incoming/outgoing) email attachments shall be restricted to a maximum limit of 10 MB /20 MB.

6.3.2.2 Auto-Forwarding of official emails to public email domains (e.g., Gmail, Yahoo mail, etc.) is prohibited.

6.3.2.3 Any e-mail addressed to a user, whose account has been deactivated/ deleted shall not be re-directed to another e-mail address.

6.3.2.4 Any case of inappropriate use of e-mail accounts shall be considered as a violation of the policy and may result in deactivation of the account. Further, such instances may also invite action as per company rules.

6.3.2.5 Users shall be trained to periodically archive their mails on the local systems and the manner in which the personal folders need to be protected.

6.3.2.6 Logs shall be reviewed at least once in a year by the administrator. If suspicious activity is identified, the same shall be handled as per the instruction of CISO.

6.3.2.7 Common or shared E-Mail ID shall be discouraged.

6.4 Do's and Don'ts of Internet Access and Email Policy

DO'S	DON'TS
• Implement Access Controls: Use role-based access controls to manage internet and email access, ensuring that users have the necessary permissions based on their job roles.	• Don't Ignore Security Alerts: Do not ignore or disable security alerts from monitoring tools; investigate and respond to them promptly.
• Monitor and Log Usage: Continuously monitor and log internet and email usage to detect and respond to suspicious activities and ensure compliance with policies	• Don't Use Default Configurations: Avoid using default settings for email servers and internet gateways; customize configurations to enhance security.
• Establish Clear Policies: Develop and communicate clear internet and email usage policies to all employees, outlining acceptable use, security practices, and consequences for violations.	• Don't Delay Software Updates: Ensure timely updates to operating systems, browsers, email clients, and security software to protect against vulnerabilities.
• Use Encryption: Implement email encryption for sensitive communications to protect confidential information from unauthorized access.	• Don't Disable Security Features: Avoid disabling essential security features such as firewalls, antivirus software, and email filters for convenience.

6.5 Point of Contact

CISO/ Designated Authority

7 Network Management Policy.

7.1 Objective

Organization's network and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized access to run APTRANSCO network infrastructure efficiently and smoothly

7.2 Scope

This policy applies to the network and communication systems of APTRANSCO.

7.3 Policy

7.3.1 IT Wing is responsible for the APTRANSCO's network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

7.3.2 The use of personal communications equipment (modems, USB cards, etc.) attached directly to personal computers with remote control software shall be

strictly controlled.

7.3.3 The designated system administrator shall routinely check & ensure that no unauthorized account with “Super user” permissions exists (if applicable).

7.3.4 Access permission for user accounts shall be restricted according to the work/ responsibility assigned to the user.

7.3.5 Restricted Access right to the sensitive systems and data through “SFTP” may be allowed, with the approval of CISO/ HOD of IT Wing

7.3.6 Network Administrator shall maintain a list of personnel from the IT team; vendors and others who can access the routers and other network devices including security devices.

7.3.7 **A)** Firewall/proxy server shall necessarily be setup for restricting the unauthorized access.

B) Installation of Firewall/UTM shall not be in default mode and the final configuration shall be documented. Firewall/UTM/System alerts shall be checked by system administrator on daily basis.

7.3.8 Firewall(s) shall be configured to deny any traffic from "un-trusted" source (Networks & Hosts) to APTRANSCO. Controls shall be implemented to prevent disclosure of internal network information to the outside world. State full inspection for all the packets shall be implemented.

7.3.9 Where possible, use of IP addresses rather than DNS names will be used in firewall policies. However, in some situations, the desired behavior by using IP addresses may not be achieved. For example, if trying to deny access to a site and the site’s IP address is assigned dynamically, or if the site has more than one IP address, blocking an IP address does not block the site reliably. In this case, fully qualified domain name (FQDN) must be used to block the site. For extra reliability, use both IP addresses and FQDNs in a rule. Note that separate rule elements for the IP addresses and for the FQDNs must be created.

7.3.10 The security rule-set on the firewall should be consistent and uniform within the organization's written/published policy on Intranet or communicated from time-to-time by IT Wing.

7.3.11 Review of the list of existing protocols must be done before defining additional protocols, to avoid overlapping of existing protocol definitions.

7.3.12 MIME (Multipurpose Internet Mail Extensions) types must be used as a criterion only in rules that apply solely to HTTP traffic.

7.3.13 Access between two networks must not allow access unless there is also a network rule defining the relationship between those two networks. This is also true for server publishing rules, but not for Web publishing rules.

7.3.14 A deny access rule must not be created for all protocols that includes a source port restriction.

7.3.15 Restrict membership in the Remote Management Computers, computer set to limited computers that require remote administration access,

7.3.16 Use Network Management Software for monitoring of network traffic.

7.3.17 Harden networks continuously.

7.3.18 Access to local system control utilities (e.g., Batch Files, Scripts etc.) shall be controlled.

7.3.19 Network Administrator shall review access control lists on routers.

7.3.20 Functional/department heads shall authorize the connectivity of third-party laptops to any unused ports only after approval from the CISO/ HOD of IT Wing

7.3.21 Periodic LAN/WAN utilization report shall be generated to monitor and identify future requirement of link bandwidth. This could also be used to identify any unfavorable link utilization by systems.

7.3.22 Regular port scanning of the nodes on LAN may be organized to see open services. Regular vulnerability scanning (self or through third party) shall be performed to assess vulnerabilities.

7.3.23 No Internet access shall be allowed to any critical Application server and Database Servers.

7.3.24 All network connected equipment must be configured to a specification approved by IT Team.

7.3.25 All hardware connected to the APTRANSCO's network is subject to APTRANSCO's IT Team management and monitoring standards.

7.3.26 The networking addresses for the supported protocols are allocated, registered and managed centrally by APTRANSCO IT Team.

7.3.27 The use of departmental firewalls is not permitted without the written authorization from APTRANSCO's IT Team and CISO.

7.3.28 Users must not extend or re-transmit network services in any way. This means user must not install a router, switch, hub, or wireless access point to the APTRANSCO's network without APTRANSCO's IT Team approval.

7.3.29 Users must not install network hardware or software that provides network services without APTRANSCO's IT Team approval.

7.3.30 Configuration of network and security devices of the network shall be maintained.

7.3.31 Physical/ Administrative access to network devices and security devices shall be allowed only through encrypted channel.

7.3.32 The systems, network and security devices shall have valid software subscriptions and use supported products.

7.3.33 Operating systems, network devices and security devices shall be regularly updated.

7.3.34 Authentication, Authorization and Accounting (AAA) mechanism shall be employed for network devices.

7.3.35 Users are not permitted to alter network hardware in any way.

7.3.36 Security annual review of all security devices, namely - firewall, Router, IPS (Intrusion Prevention System), Proxies, Anti-virus software shall be conducted. In case of any vulnerabilities found, the necessary changes shall be made through a formal change management process.

7.3.37 Audit logging shall be enabled on the firewall to ensure that all critical accesses and changes to firewall configuration and/or policy are tracked.

7.3.38 The log reports of firewall and other security devices, shall be produced and, shall be monthly reviewed to determine if attacks have been detected.

7.4 Wireless Network Management

7.4.1 Dedicated DHCP (Dynamic Host Configuration Protocol) IP pool shall be created for "non-employees" that shall distinguish these users from local LAN users.

7.4.2 Service Set Identifier (SSID) broadcast from the wireless access point shall be preferably disabled. An exception to this shall be Wi-Fi SSID for Guest users.

7.4.3 Visitor Wi-Fi encryption key should be changed at least every fortnight.

7.4.4 WPA2 (Wi-Fi Protected Access) protocol should be used as a standard for Wi-Fi encryption.

7.4.5 Wireless network deployment in APTRANSCO shall be a controller managed wireless network.

7.4.6 Wireless access points shall be placed in secure locations unless otherwise approved by the CISO.

7.4.7 File sharing shall be disabled on wireless-enabled devices.

7.4.8 Wireless client systems and wireless devices shall not be allowed to connect to the APTRANSCO wireless access points without due to authentication.

7.4.9 To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

7.5 Activity Audit and logging

7.5.1 Auditing and logging shall be enabled for all critical servers, network devices and applications.

7.5.2 Network management reports and audit trails shall be maintained of all administrator roles.

7.5.3 Audit logging shall be enabled on the firewall to ensure that all critical accesses and changes to firewall configuration and/or policy are tracked. The log reports of firewall and other security devices, shall be produced in a defined format, shall be timely/daily/monthly reviewed to determine if attacks have been detected.

7.5.4 Audit controls shall be balanced with operational requirements and Controls shall be implemented to allow collection of appropriate audit data, while minimizing the risk of disruption to business processes.

7.5.5 Audit logs shall be maintained for critical user-activities including, failure of System access attempts, changes to System configuration etc.

7.5.6 All logs shall include at least the following key fields: user IDs, IP Address / device, timestamps, and details of key events.

7.5.7 Configuration changes to all the network devices shall be reviewed while tracking changes that have failed. All system access must be logged and the log files thus generated shall never be overwritten or deleted until they are backed up to off-line storage.

7.5.8 Logs shall be maintained, monitored and analyzed for the systems, applications, networks and security devices. Automated alert and notification system shall be deployed at the critical systems to inform network administrator.

7.5.9 Enabling Audit Trail and edit log of all manual entries, all entries arising out of sub-systems and all modifications in Master Data (Finance Module, HR Module, Contractor details, etc.) which impact the books of accounts for SAP ERP System.

7.5.10 Audit trail shall be maintained and reviewed at least once in a quarter. It shall be ensured that Audit Trail is never disabled and the Audit Trail feature is not tampered with.

7.5.11 It shall be ensured that the Audit Trail has been preserved by the Company as per the statutory records for record retention.

7.5.12 IT Wing to conduct System Audit through independent agency on every six months on the points mentioned at 7.5.10 to 7.5.12 above.

7.5.13 A log of password resets shall be maintained for auditing purposes.

7.5.14 Logs shall be reviewed by the administrator as a routine process on a daily basis and any suspicious activity shall be monitored. If suspicious activity is identified as a security incident or weakness, the same shall be handled as per the Incident Management Process.

7.5.15 All security-related critical & sensitive events must be logged and audit trails saved as follows:

7.5.15.1 All security related logs will be kept online for a minimum of 1 week.

7.5.15.2 Daily incremental backups will be retained for at least 1 month.

7.5.15.3 Weekly full backups of logs will be retained for at least 1 month.

7.5.15.4 Monthly full backups will be retained for a minimum of 6 month.

7.6 Do's and Don'ts of Network Management Policy

DO'S	DON'TS
• Implement Strong Access Controls: Use role-based access controls (RBAC) to ensure users and administrators only have the access necessary for their roles	• Don't Use Default Credentials: Avoid using default usernames and passwords for network devices; always change them to strong, unique credentials.
• Monitor Network Traffic: Continuously monitor network traffic for unusual or suspicious activity using tools like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	• Don't Ignore Security Alerts: Do not ignore or disable security alerts from network monitoring tools; investigate and respond to them promptly.
• Use Network Segmentation: Create VLANs for APTRANSCO network to avoid security breaches from one LAN to other LAN in the event of mal-operation by cyber actors.	• Don't Allow Unsecured Devices: Avoid connecting unsecured or unauthorized devices to the network to prevent potential vulnerabilities.
• Implement Redundant Systems: Use redundant systems and failover mechanisms to ensure network reliability and availability.	• Don't Forget to Isolate Guest Networks: Isolate guest networks from the main network to prevent unauthorized access to sensitive systems and data.

7.7 **Point *of Contact :*** CISO/ Designated Authority

8 Password Management Policy

8.1 Objective

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. Password Management Policy aims at providing the first line of defense for securing access to the IT Networks and the data/information stored and processed by them.

8.2 Scope

The scope of this policy includes all employees of APTRANSCO, Auditors, Service providers authorized by APTRANSCO etc., and who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any APTRANSCO facility, has access to the APTRANSCO network or stores any non-public APTRANSCO information.

8.3 Policy

8.3.1

General Guidelines

8.3.1.1 All system-level passwords must be changed on at least a quarterly basis.

8.3.1.2 All production system-level passwords must be part of the Information Security administered global password management database.

8.3.1.3 It must be enforced that all user-level passwords (e.g., email, web, desktop computer, etc.) are changed at least every 90 days.

8.3.1.4 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

8.3.1.5 Passwords must not be inserted into email messages or other forms of electronic communication. One time password may be sent by mail or electronic communication (i.e. mobile OTP etc.).

8.3.1.6 Users requiring access to network shall have unique user accounts and associated passwords.

8.3.1.7 Temporary/default passwords provided by the IT Wing shall be changed at the first log-on.

8.3.1.8 All the passwords for super-user level accounts, network administrator and those of the System Administrators shall be changed at intervals of maximum 90 days.

8.3.1.9 All default administrative/ super-user accounts shall be renamed. Any account that is not required at system level or at application level shall be deleted/ deactivated.

8.3.1.10 Allot Employee ID as User ID (for all accounts) and link official mobile number which is allotted by APTRANSCO for OTP confirmation to log In.

8.3.1.11 Enter OTP from user mobile which is linked with User ID, Displays last 3 digits of mobile Number.

8.3.1.12 Don't use a password that is the same or similar to one you use on any other accounts.

8.3.1.13 Allot Masked ID as User ID (for all accounts) duly storing the third-party Employee ID which was allotted by the company/ Contractor.

8.3.1.14 For password reset contact IT In charge/ADMIN.

8.3.2 **Guidelines for creation of Passwords**

8.3.2.1 Must contain at least eight (8) alphanumeric characters.

8.3.2.2 The Password shall contain at least one character each of the following categories:

(i) Alphabets letters (A-Z, a-z), Numerals (0-9) & Have digits and punctuation characters as well as letters e.g., 0-9,!@#$ %^&*()_+|~-=\{}[]:";'<>?,./).

(ii) User shall not create weak password like

a. Which are found in a dictionary (English or foreign)

b. Names of family, pets, friends, co-workers, fantasy characters, etc.

c. Computer terms and names, commands, sites, companies, hardware, software.

d. The words "APTRANSCO", "Faridabad", "Camera" or any derivation.

e. Birthdays & other personal information such as addresses and phone numbers.

f. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

g. Any of the above spelled backwards.

h. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

8.3.2.3 Passwords should not be inserted into email messages or other forms of electronic communication.

8.3.2.4 The password shall not be same as login name.

8.3.2.5 Passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the IT Team and must have a primary responsible contact person. Shared passwords used to protect network devices require a designated individual to be responsible for the maintenance of those passwords, and that individual will ensure that only appropriately authorized employees have access to the passwords.

8.3.2.6 If a password is suspected of being compromised, it should be changed immediately and the incident reported to the IT Team.

8.3.2.7 Last passwords shall not be used again. System should remember last 3 passwords.

8.3.2.8 Account lockout criteria is set for 3 unsuccessful login Disclaimers for users shall be formulated and displayed alike 'Account lockout because of three consecutive unsuccessful login attempts - Please contact the administrator.

8.3.2.9 That different layer of passwords, access rights and authorization viz. CMOS password, User ID, Network password, Application password with different level privileges are used.

8.3.2.10 User is wholly responsible for activities against his/her user-ids, sharing of passwords with others is not recommended as per good security practice.

8.3.2.11 Avoid keeping a paper record of passwords. User should not divulge passwords to other users. Authorized users are responsible for the security of their passwords

8.3.2.12 Do not include passwords in any automated log-on process, e.g. stored in a macro or function key or “remember password”.

8.3.2.13 As user is wholly responsible for activities against his/her user-ids, sharing of passwords with others is not recommended as per good security practice.

8.3.2.14 Avoid keeping a paper record of passwords. User should not divulge passwords to other users. Authorized users are responsible for the security of their passwords

8.3.3 **Password Management in Application Development**

8.3.3.1 Application developers must ensure their programs contain the following security precautions in applications developed by them:

8.3.3.1.1 Shall support authentication of individual users, not groups.

8.3.3.1.2 Shall not store passwords in clear text or in any easily reversible form.

8.3.3.1.3 Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

8.4 Do's and Don'ts of Password Management Policy

DO'S	DON'TS
• Implement Multi-Factor Authentication (MFA): Use MFA to provide an additional layer of security beyond just passwords.	• Don't Use Default Passwords: Never use default passwords; always change them to strong, unique passwords during the initial setup.
• Regularly Update Passwords: Enforce regular password changes, such as every 60-90 days, to reduce the risk of compromised credentials.	• Don't Reuse Passwords: Avoid reusing passwords across different accounts and systems to prevent a single breach from compromising multiple accounts.
• Use Password Managers: Encourage the use of reputable password managers to store and manage passwords securely.	• Don't Store Passwords in Plain Text: Never store passwords in plain text; always use encryption and hashing mechanisms.
• Educate Users: Provide training on creating strong passwords and the importance of password security.	• Don't Share Passwords: Prohibit the sharing of passwords among users to maintain accountability and security.

8.5 Point of Contact

CISO/Designated Authority

9 Physical and Environmental Security

9.1 Objective

APTRANSCO's Physical and Environmental policy intends to ensure that critical IT/OT High Security areas are adequately guarded to avoid any physical intrusion and to ensure equipment safety in case of any unforeseen happening. APTRANSCO shall enforce use of technologies like smart cards, biometrics, visitors register etc. to control the physical entry to IT/OT High Security areas.

9.2 Scope

This policy addresses threats to critical IT/OT resources that result from unauthorized access to facilities owned or leased by APTRANSCO including offices, data centers and similar facilities that are used to house such resources.

9.3 Policy

9.3.1 Physical Access Controls

9.3.1.1 Physical access controls shall be provided in sensitive and critical areas. Physical protection should be in proportion to the criticality or importance of functions in that area at APTRANSCO. These controls shall provide physical access to IT/OT installations only for authorized personnel, by competent authority.

9.3.1.2 The list of the authorized persons to enter into the data center, approved by CISO, shall be displayed clearly at the main entrance door.

9.3.1.3 No eatables shall be allowed at critical High Security areas.

9.3.1.4 Hazardous and inflammable material shall not be allowed in close proximity of the data center.

9.3.1.5 Visitors to data center are required to get authorization from in-charge of data center.

9.3.1.6 Visitors to data center: Control shall be implemented which must include any or all of the following features:

9.3.1.7 Visitor log register.

9.3.1.8 Sign-in/sign-out procedures with time recorded.

9.3.1.9 The work area shall be properly secured to protect both sensitive and critical information and ensure privacy. Server & associated equipment/peripherals shall be placed in a location that protects the confidentiality of data. Documents and media shall be stored in a secure manner.

9.3.1.10 All physical security systems must comply with applicable regulations but not limited to, building codes and fire prevention and suppression codes.

9.3.1.11 Physical access to all Information Resources restricted facilities must be documented.

9.3.1.12 Access to Information processing facilities must be granted only to APTRANSCO's support personnel, and contractors, whose job responsibilities require access to that facility.

9.3.1.13 Each individual that is granted regular access rights to an Information processing facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

9.3.1.14 Requests for access must come from the applicable APTRANSCO's data/system owner.

9.3.1.15 Access cards and/or keys must not be shared or loaned to others.

9.3.1.16 Access cards and/or keys that are no longer required must be returned to the person responsible for the information processing facility. Cards must not be reallocated to another individual bypassing the return process.

9.3.1.17 Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.

9.3.1.18 Cards and/or keys must have identified information enabling return of card.

9.3.1.19 All Information processing facilities that allow access to visitors will track visitor access with a sign in/out log.

9.3.1.20 Card access records and visitor logs for Information processing facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

9.3.1.21 The person responsible for the Information processing facility may remove the card and/or key access rights of individuals that change roles within APTRANSCO and must remove the card and/or key access rights of individuals separated from their relationship with APTRANSCO's.

9.3.1.22 Visitors must be escorted in Physical access-controlled areas of Information Resources facilities.

9.3.1.23 The person responsible for the Information processing facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

9.3.1.24 The person responsible for the Information processing facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

9.3.1.25 Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

9.3.1.26 The physical security of Servers, PLCs, Remote Terminal Units, communication network and other components shall be ensured by regular inspection and assigning specific responsibilities.

9.3.1.27 Closed-Circuit TV (CCTV) Surveillance Monitoring may be performed to ensure workforce safety and prevent property loss. Surveillance monitoring shall be limited to areas perceived as high risk unless otherwise required.

9.3.1.28 CCTV(s) shall be installed to detect intruders and monitor any suspicious. CCTV logs should be retained for at least 90 days for review purposes.

9.3.1.29 Records should be maintained for all suspected or actual faults and all preventive and corrective action. And only authorized maintenance personnel should carry out repairs and services.

9.3.1.30 Adequate insurance cover should be in place to protect equipment off site.

9.3.2 **Equipment Security**

9.3.2.1 Provisions shall be made to supply quality power for all the IT and OT equipment/ facilities.

9.3.2.2 All the servers and critical assets should be located in the physically secured Data Centre. Appropriate controls are used to protect against physical and environmental threats, e.g., fire, explosives, theft, smoke, chemical effects, supply interference, communications interference, electromagnetic radiation and vandalism.

9.3.2.3 Provisions for uninterruptible power supply (UPS) shall be made to provide uninterrupted power supply to all the IT and OT equipment/facilities. This shall ensure continuity of operations in case of power outage.

9.3.2.4 The assets may be covered under comprehensive insurance to provide cover to any financial loss that might suffer due to unforeseen happenings.

9.3.2.5 No IT and OT asset shall be shifted/removed from its location without prior approval of the IT Wing.

9.3.2.6 Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.

9.3.2.7 Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All critical applications shall be configured to switchover to an alternate power source immediately upon loss of power.

9.3.2.8 Equipment's having storage media is disposed off only after ensuring that all sensitive data and licensed software have been removed or securely overwritten. This is done only after authorization of asset owner

9.3.2.9 Storage media containing confidential or copyright information should be deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function.

9.3.2.10 Only authorized maintenance personnel should be allowed to carry out service of equipment and repair.

9.3.3 Environmental Security controls

9.3.3.1 Data Centre shall have the following:

9.3.3.1.1 Independent air conditioning and fire suppressing system.

9.3.3.1.2 Fire and smoke detectors.

9.3.3.1.3 Fire extinguishers shall be checked for extinguisher pressure as recommended by the OEM. The cylinder last checked date and next check date must be specified on the cylinder.

9.3.3.1.4 Toxic and inflammable material shall not be permitted in APTRANSCO's Data Centre.

9.3.3.2 Data Centre shall be declared as 'No Paper' & 'No Smoking' zone.

9.3.3.3 The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

9.3.3.4 Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

9.3.3.5 Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

9.3.3.6 Lightning protection is applied to all buildings and lightning protection filters are fitted to all incoming power and communication lines.

9.3.4 Cabling Security

9.3.4.1 Power and Telecommunications cabling - carrying data or supporting information services should be underground or subject to adequate alternative protection.

9.3.4.2 Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.

9.3.4.3 Only authorized personnel have access to patch panels and cable rooms.

9.3.4.4 Power cables should be segregated from communication cable to prevent interfere.

9.4 Do's and Don'ts of Physical and Environmental Security Policy

DO'S	DON'TS
• Conduct Regular Inspections and Audits: Perform routine checks on physical infrastructure and environmental controls.	• Neglect Policy Enforcement Don't ignore violations of physical and environmental policies.
• Develop and Update Policies: Establish comprehensive physical and environmental policies that address all relevant areas.	• Overlook Employee Training Don't skip regular training sessions on safety and environmental policies
• Implement Emergency Preparedness Plans: Develop and maintain emergency response and evacuation plans.	• Ignore Maintenance Issues Don't delay repairs or maintenance of physical infrastructure and safety systems.
• Maintain Building Security: Install and regularly maintain security systems like surveillance cameras, access control systems, and alarms.	• Avoid Regular Policy Reviews Don't let policies become outdated.

9.5 Point of Contact

CISO/Designated Authority.

10. Router Security Policy

10.1 Objective

All routers connected to networks are sensitive. A minimal security configuration for all routers and switches connecting to the production network must be defined for a secure Network across the organization.

10.2 Scope

All routers and switches connected to APTRANSCO production networks are affected. Routers and switches within internal, secured labs are not as critical in comparison.

10.3 Policy

10.3.1 The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization

10.3.2 Edge routers must ensure restrictions to the following:

(Edge routers represent the border crossing between internal and external networks, protecting your internal network devices, applications, infrastructure, and data from unauthorized external communications)

10.3.2.1 IP directed broadcasts

10.3.2.2 Incoming packets at the router sourced with invalid addresses such as RFC1918 address

10.3.2.3 TCP small servers

10.3.2.4 UDP small servers

10.3.2.5 All source routing

10.3.2.6 All web services running on router

10.3.3 Access rules at the router level shall be added as the business needs arise.

10.3.4 The Administrator shall have explicit permission to access or configure router.

10.3.5 The Administrator shall maintain the username, password & the location list of routers strictly in a confidential place.

10.3.6 The router shall be placed in a location where physical access is limited to authorize persons only.

10.3.7 No user accounts shall be configured on the router.

10.3.8 Routers shall have “AAA” enabled for authentication purposes.

10.3.9 Disallow the following:

10.3.9.1 Unauthorized Logon

10.3.9.2 Maintenance Operation Protocol (MOP)

10.3.9.3 Inbound TCP Connection Keep Alive.

10.3.10 Each router must have the following statement posted in clear view:

```
**************************************************************
*          All rights reserved (Year)          *
*          without the owner's prior written consent,       *
*          no decompiling or reverse-engineering shall be allowed. *
*          Notice:                                *
*          This is a private communication system.          *
*          Unauthorized access or use may lead to prosecution
**************************************************************
```

10.3.11 Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path and it is properly password protected. SSH is the preferred management protocol for such management.

10.4 Do's and Don'ts of Router Security Policy

DO'S	DON'TS
• Change Default Credentials: Always change default usernames and passwords for router access.	• Use Default or Weak Passwords Don't leave default passwords in place or use weak, easily guessable passwords.
• Regularly Update Firmware Keep the router's firmware up to date with the latest security patches and updates.	• Ignore Firmware Updates Don't neglect to update router firmware.
• Enable Strong Encryption : Use strong encryption methods like WPA3 for wireless networks	**Overlook Network Segmentation:** Don't place all devices on a single, flat network.
• Implement Access Controls: Restrict access to the router management interface to trusted IP addresses	Allow Unrestricted Remote Access: Don't allow unrestricted remote access to the router.

10.5 Point of Contact:

CISO/Designated Authority

11 Server Security Policy

11.1 Objective

To establish a standard security configuration for servers inside the organization's production network, to minimize unauthorized access to APTRANSCO information and technology systems.

11.2 Scope

This policy applies to server equipment owned and operated by APTRANSCO, and to servers registered under APTRANSCO-owned internal network domain. This policy is specifically for Server equipment on the internal APTRANSCO network.

11.3 Policy

11.3.1 All servers must be owned by the group responsible for system administration.

11.3.2 Servers shall be physically located in an access-controlled environment.

11.3.3 Access of servers over LAN shall be allowed only to respective administrators.

11.3.4 Approved server configuration guidelines must be established and maintained by respective group, based on business needs.

11.3.5 Configuration changes for production servers must follow the appropriate change management procedures.

11.3.6 Conduct exhaustive market survey prior to purchase of Servers with security features.

11.3.7 The following information regarding Servers in use shall be maintained by respective group:

11.3.7.1 Server location and its backup (if required).

11.3.7.2 Warranty Status.

11.3.7.3 Hardware and Operating System/Version.

11.3.7.4 Main usage

11.3.7.5 IP Address

11.3.7.6 Owner of the server

11.3.7.7 Custodian of the server.

11.3.8 Services and applications that are not required must be disabled.

11.3.9 Always use standard security principle of least required access to perform a function.

11.3.10 The most recent security patches must be installed on the servers as soon as possible (after testing the patches); the only exception being when immediate application would interfere with business requirements.

11.3.11 In case the installation of patching requires system shut down the same should be scheduled appropriately so that it does not interfere with the regular working of the users.

11.3.12 Security-breach events shall be reported to the System Administrator, who will review logs and report incidents to IT Team. Corrective measures shall be prescribed as needed. Security-breach events include, but are not limited to:

11.3.12.1 Port-scan attacks

11.3.12.2 Evidence of unauthorized access to privileged accounts

11.3.12.3 Anomalous occurrences that are not related to specific applications, on the host.

11.3.12.4 Service/port enabled which has not been approved or configured by administrator.

11.3.13 Access to the production server room is strictly prohibited for unauthorized persons.

11.3.14 Trust relationships between systems are a security risk, and their use shall be avoided. Do not use a trust relationship when some other method of communication will do.

11.3.15 Information in the corporate enterprise management system must be kept up-to date.

11.3.16 Operating System configuration should be in accordance with approved InfoSec guidelines.

11.3.17 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).

11.3.18 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

11.3.18.1 All security related logs will be kept online for a minimum of 1 week.

11.3.18.2 Daily incremental backups will be retained for at least 1 month.

11.3.18.3 Weekly full backups of logs will be retained for at least 1 month.

11.3.18.4 Monthly full backups will be retained for a minimum of 1 year.

11.3.19 The server should be installed with the approved Antivirus software and updated regularly.

11.3.20 Service pack updates shall undergo change management on all critical application/ servers.

11.3.21 Application security assessment for all sensitive/critical applications in the production System(s) shall be done once in six months.

11.4 Do's and Don'ts of Server Security Policy

DO'S	DON'TS
• Use Encryption: Encrypt sensitive data both at rest and in transit.	• Don't Ignore Physical Security: Ensure physical access to servers is restricted and monitored.
• Conduct Regular Security Audits and Penetration Testing: Perform regular security assessments to identify and mitigate vulnerabilities.	• Don't Rely Solely on Perimeter Security: Implement layered security measures beyond firewalls and antivirus software
• Implement Access Controls: Apply the principle of least privilege, granting users only the access necessary for their roles.	• Don't Use Default Configurations: Default settings often lack optimal security configurations.
• Monitor and Log Activity: Set up comprehensive logging to track user activity and system events.	• Don't Ignore Third-Party Risks: Assess and manage the security practices of third-party vendors and partners.

11.5 Point of Contact:

CISO /Designated Authority

12 Application Software Development & Support

12.1 Objective

To determine the key issues related to in-house software development or bought-out software solution across the organization.

12.2 Policy

12.2.1 Appropriate software for desired applications shall either be developed in-house or market survey shall be conducted to identify requisite software solutions available in the market. In case of In-house development, IT/CISO shall approve or decide based on available skillset and available manpower.

12.2.2 A proper study of the software shall be done by the IT officials to meet the user's requirement.

12.2.3 Proper demonstration & training shall be ensured and the respective user's Wing shall be trained adequately.

12.2.4 Respective changes/patches in the existing software shall be made only after the receipt of the changes & modification requirement in prescribed format, reviewed by the HOD of IT Wing and the final changes suggested by the group leader are approved and accepted by the change request initiator.

12.2.5 The changes/patches & modifications shall be checked & verified by the end user / requester; only then modified program shall be implemented in live or production environment.

12.2.6 The testing of the program / patches shall be done in testing area which is different from the live or production environment.

12.2.7 Changes/patches/modifications made in application software shall be recorded in Change management register.

12.2.8 If the development is not possible in-house and there is no ready-made solution available in the market, it shall be got developed indigenously from reputed vendors/institutes. The source code of such application software shall be the sole property of the APTRANSCO and the vendor shall not have any rights after the same is handed over to the APTRANSCO. In case of ERP, it shall be done through approved vendor. The IT officials of the organization shall preferably be associated at the software development stage.

12.2.9 An undertaking shall also be taken from the vendor/institute that they would not reveal the source code and information to any outside agency without prior approval of the CISO/ HOD of IT wing.

12.2.10 The following criteria will be evaluated to assess the Access control capabilities of the application:

12.2.10.1 Access controllability

12.2.10.2 Access audit ability

12.2.10.3 Data Visibility & Data Flow

12.2.10.4 Auto-logout

12.3 In House Software Development

12.3.1 A Software engineering model should be developed and shall be applied to all in-house information system engineering activities

12.3.2 Security is designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility.

12.3.3 Secure engineering techniques providing guidance on user authentication techniques, secure session control and data validation, sanitization and elimination of debugging codes.

12.4 Outsourced Software Development

12.4.1 Where software development is outsourced, the following points are considered:

12.4.1.1 Selection of vendor based on software quality standards.

12.4.1.2 Licensing arrangements, code ownership and intellectual property rights.

12.4.1.3 Certification of the quality and accuracy of the work carried out.

12.4.1.4 Rights of access for audit of the quality and accuracy of work done.

12.4.1.5 Contractual requirements for quality of code.

12.4.1.6 Testing before installation to detect Trojan code.

12.4.1.7 The software development environment provided to the outsourced vendor is segregated from the production environment.

12.5 Do's and Don'ts of Application Software Development & Support Policy

DO'S	DON'TS
• Establish Clear Development Standards: Define and enforce coding standards and best practices.	• Don't Ignore Security Best Practices: Avoid neglecting security in the development process.
• Implement Secure Development Practices: Incorporate security from the start by following secure coding guidelines.	• Don't Overlook Documentation: Failing to document development processes and decisions can lead to confusion and inefficiency
• Adopt Continuous Integration/Continuous Deployment (CI/CD): Automate the build, testing, and deployment processes to improve efficiency and reduce errors.	• Don't Use Outdated Tools and Libraries: Avoid relying on outdated or unsupported tools, libraries, or frameworks.
• Perform Comprehensive Testing: Implement a robust testing strategy, including unit, integration, functional, and security testing.	• Don't Skip Testing Phases: Skipping or minimizing testing can lead to undetected bugs and vulnerabilities.

12.6 Point Of Contact

CISO /Designated Authority

13 User Management Policy

13.1 Objective

User Management Policy aims at assisting the System Administrators in carrying out user account management tasks including – user account creation/deletion, maintenance of user accounts, defining and maintaining user access privileges, etc.

13.2 Scope

The primary scope of this policy encompasses the creation, modification, suspension, and removal of user accounts across all systems, applications, and network resources.

13.3 Policy

13.3.1 All users requiring access to APTRANSCO's network shall be assigned unique user accounts and passwords.

13.3.2 Creation/Deletion and Maintenance of all the user accounts related to IT applications, SAP ERP and mail server shall be centralized.

13.3.3 All default user accounts on various systems shall be renamed.

13.3.4 All the user accounts created and maintained shall follow a standard naming convention.

13.3.5 Assign new user accounts to the vendors, business partners, and temporary employees/trainees with least access privileges and they shall have limited validity period.

13.3.6 All the accounts associated with an employee shall be handed over to the successor or controlling office on the last day of work for any employee leaving the organization. System administrator shall disable / delete the relived employee credentials.

13.3.7 System Administrators shall assign the rights and privileges to the user groups and not to the user accounts individually. User accounts shall thus inherit the right and access privileges from the groups they are members of.

13.3.8 System Administrator shall maintain a list of all the user name.

13.3.9 System administrator shall not access any user's accounts in any manner.

13.3.10 Cracking of user's password is strictly prohibited.

13.3.11 Account shall get locked out permanently after 3 continuous bad attempts. Account shall be unlocked through the request raised from user and approved by Departmental head and IT Wing.

13.3.12 Review of applications users' rights shall be done on yearly basis. The Roles & Rights of the officials, who have not posted any transaction in SAP ERP during the period, shall be revoked by concern SAP ERP module leader.

13.3.13 User and Administrative accounts which have not been used for a period of consecutive 60 days shall get locked.

13.3.14 Users shall be required to re-authenticate (Login) themselves after a specific period of inactivity (5 minutes). All applications/databases wherever possible shall use inactivity timeout for critical applications.

13.3.15 Two Simultaneous login from the same user ID shall not be allowed. Pseudo administrator accounts should be created for performing root and/or admin activities. No one should be allowed to use 'Administrator or Root' account other than the system administrator.

13.4 Do's and Don'ts of User Management Policy

DO'S	DON'TS
• Use Role-Based Access Control (RBAC): Assign permissions based roles, ensure users have the minimum necessary access.	• Don't Use Shared Accounts: Avoid using shared or generic accounts as they hinder accountability and security.
• Regularly Audit User Accounts: Conduct periodic audits of user accounts to ensure appropriate access levels.	• Don't Ignore Access Requests: Avoid granting excessive access by default or ignoring proper approval processes.
• Enforce Account Lockout Policies: Implement account lockout policies to prevent brute force attacks.	• Don't Neglect Password Policies: Avoid using weak or easily guessable passwords.
• Use Automated Tools for User Management: Employ automated tools for provisioning, de-provisioning, and auditing user accounts.	• Don't Ignore User Feedback: Address user feedback related to account management promptly to improve the process.

13.5 Point of Contact:

CISO/Designated Authority

14. Virtual Private Network (VPN) Policy

14.1 Objective

The policy provides guidelines for Remote Access Virtual Private Network (VPN) connections to the APTRANSCO's network.

14.2 Scope

This policy applies to all APTRANSCO employees, contractors, consultants, temporary employees, and other workers including all personnel affiliated with third parties utilizing VPNs to access the APTRANSCO network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

14.3 Policy

14.3.1 Employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software and paying associated fees.

14.3.2 Following should be taken into consideration while working on / with VPN:

14.3.2.1 It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to APTRANSCO's internal networks.

14.3.2.2 VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong Pass word / passphrase.

14.3.2.3 When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

14.3.2.4 VPN gateways will be set up and managed by network group.

14.3.2.5 All computers connected to APTRANSCO internal networks via VPN or any other technology must use the most up-to-date anti-virus software of corporate standard; this includes personal computers.

14.3.2.6 VPN users will be automatically disconnected from APTRANSCO's network after ten minutes of inactivity. The user must then logon again to reconnect to the network.

14.3.2.7 Users of computers that are not APTRANSCO owned equipment must configure the equipment to comply with APTRANSCO's VPN and Network policies.

14.3.2.8 Only approved VPN clients may be used.

14.3.2.9 Two-Factor token-based authentication shall be used.

14.3.2.10 Strong encryption and hashing protocols (3DES, SHA etc.) / passwords should be used while implementing VPN access.

14.3.2.11 Remote access should be strictly done through Secure APTRANSCO Virtual Private Networks (VPNs) and strong passwords should be used for VPN access

14.3.2.12 Limit VPN Users Access, duly limiting period and time, in case of any Requirement/ emergency the procedure as laid in Access management be followed.

14.3.2.13 Create VPN users' profile, before connect to a VPN and maintain their records.

14.3.2.14 Consider configuring mandatory 2 factor authentication, if using VPN services to access organizational networks

14.3.2.15 User ID (employee ID) with MAC address binding is mandatory for VPN users, before enabling VPN Access.

14.3.2.16 Ensure that the data from VPN users to machine is tunneled and encrypted.

14.3.2.17 Multiple simultaneous remote access by the same user should not be allowed.

14.3.2.18 Virtual Private Network Service (VPN Service) Providers (APTRANSCO), Shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the Registration as the case may be:

Proforma for VPN Registration

a. Validated names of subscribers/customers hiring the services:
b. Period of hire including dates:
c. IPs allotted to / being used by the members:
d. Email address and IP address and time stamp used at the time of Registration / on-boarding:
e. Purpose for hiring services:
f. Validated address and contact numbers:
g. Ownership pattern of the subscribers / customers hiring services:

h. **Certificates:**

- Certified that the VPN services will be utilized for official Purpose only.
- Certified that the VPN services will be availed in the interest of Official work only.
- Certified that the VPN will not be utilized other than official work.
- Certified that the confidential information of Organisation, VPN Login credentials and other relevant information will not be disclosed to others.

Signature of the VPN user **Signature of the concerned HOD**

Brief Description on VPN Service provided to VPN User:
……
……
……

Signature of the **Signature of the**

VPN Provider **Concerned HOD**

14.4 Do's and Don'ts of Virtual Private Network (VPN) Policy

DO'S	DON'TS
• Use Strong Authentication: Implement multi-factor authentication (MFA) for VPN access.	• Don't Use Default Settings: Avoid using default configurations for VPN servers and client.
• Implement Access Controls: Use role-based access control (RBAC) to grant VPN access based on user roles and responsibilities.	• Don't Allow Split Tunneling: Disable split tunneling to prevent data from bypassing the VPN and exposing sensitive information.
• Regularly Monitor and Audit VPN Usage: Monitor Logs & VPN connections for unusual or suspicious activity.	• Don't Grant Permanent VPN Access: Avoid providing indefinite VPN access to users.
• Enforce Security Policies: Ensure that connected devices comply with APTRANSCO security policies (e.g., updated antivirus, firewalls).	• Don't Overlook Endpoint Security: Don't neglect the security of devices connecting to the VPN.

14.5 Point of Contact : CISO/Designated Authority

15. Business Continuity Management Policy

15.1 Objective

15.1.1 The purpose of this policy is to formalize the Business Continuity program of APTRANSCO IT Wing and to provide guidelines for developing, implementing, rehearsing, maintaining and exercising Business Continuity Plans (BCPs).

15.1.2 This policy establishes the basic principles and framework necessary to ensure emergency response, resumption and recovery, restoration and permanent recovery of APTRANSCO's IT Wing operations and business activities during a business interruption event either man-made or natural.

15.2 Scope

15.2.1 The Business Continuity Policy is written for a generic situation, which assumes that the primary site is suddenly inaccessible or must be vacated without warning.

15.3 Policy

15.3.1 **Business impact analysis**

15.3.1.1 The CISO shall formulate the BCM team. The team is cross-functional and has representatives from each function.

15.3.1.2 Based on stake-holders' requirements, the BCM team shall identify the critical projects/ services/business processes, which have to be continued in case of a disruption.

15.3.1.3 All function heads shall identify their assets which support critical business processes and are needed for business continuity.

15.3.1.4 The factors to be considered for doing a Business Impact Analysis (BIA) should be outlined in BIA Methodology, Critical Business Processes/ Projects thus identified should be listed in the BIA Report and their corresponding Recovery Point Objective (RPO) & Recovery Time Objective (RTO) values should be recorded.

15.3.1.5 The dependencies or requirements from other functions should also be identified and filled in Requirements of projects/functions in BIA Report.

15.3.2 Recovery Strategy

15.3.2.1 The BCM team decides on the strategies that are most suited to the business goals and objectives. The response, recovery and restoration strategies are decided.

15.3.2.2 Various threats which may cause disruption of activities are identified. Disruptions could be minor (which do not need evacuation or make the premises inaccessible) or major (which need evacuation or make the premises inaccessible).

15.3.2.3 Preventive safeguards already in place are identified and listed in the BCP.

15.3.2.4 Actions to be performed in case of minor disruptions are identified and listed in the BCP.

15.3.2.5 In case of major disruptions, the emergency response procedures with responsibility are laid down.

15.3.2.6 A person in authority in the management is identified as the Whistle-blower, who assesses the situation in case of a disruption and invokes the BCP, if needed.

15.3.2.7 Recovery procedures detailing assessment of the situation and decision to continue from the DR site are laid down.

15.3.2.8 Once the operations start from the DR site, responsibility for restoration of the primary site and resumption of operations from there are identified and documented.

15.3.2.9 Estimation of loss and learning from the entire process is shared within the BCM team.

15.3.3 Business continuity implementation and monitoring

15.3.3.1 The BCP team decides on the type of tests and the schedule for carrying out the test. Tests are carried out as follows

15.3.3.1.1 Full Drill: This test is carried out once a year. Actual drill of emergency procedures is carried out to evaluate the readiness of organization personnel in performing these tasks. This includes contacting key personnel, sounding alarms, evacuation procedures, retrieval of backup from offsite location, recovering operations at the DR site.

15.3.3.1.2 Partial Test: This test is done once in every 6 months. Only critical emergency functions are carried out in the organization’s premises.

15.3.3.1.3 Table review of the plan: This test is carried out half-yearly. All the BCP operations people are involved and they discuss the various actions that each team has to carry out.

15.3.4 Monitor, review and update the plan

15.3.4.1 The BCP is reviewed by the CISO for any changed requirements and enhancements. An updated copy of the plan is also stored at the offsite backup facility.

15.3.4.2 The CISO will designate a coordinator who shall be responsible for preparing a schedule for testing the plan, updating it after conducting the test, schedule for review of BCP, schedule for training organization personnel in BCP procedures and maintaining an updated list of contact information of key personnel.

15.3.4.3 All test results are documented. Corrections and Corrective actions are decided.

15.4 Do's and Don'ts of Business Continuity Management Policy

DO'S	DON'TS
• Develop a Comprehensive Plan: Identify Critical Functions: Determine which business functions are essential and prioritize them.	• Don't Neglect Regular Testing: Conduct Regular Drills: Failing to test the BCM plan can result in gaps and inefficiencies.
• Establish a BCM Team: Assign Roles and Responsibilities: Designate a team responsible for implementing and managing the BCM policy.	• Don't Skip Documentation: Document All Procedures: Ensure all steps and procedures are thoroughly documented.
• Create Detailed Documentation: Document Procedures: Clearly outline the steps to be taken during an incident Implement Regular Testing and Drills: Regular Drills: Test the BCM plan regularly to identify gaps and areas for improvement.	• Don't Ignore Regulatory Compliance: Stay Compliant: Ensure that the BCM policy complies with all relevant regulations and standards. Don't Overlook Technological Conduct Solutions: Use Technology Wisely: Leverage technology to enhance BCM capabilities, such as automated notifications and backup solutions

15.5 Point of Contact

CISO /Designated Authority.

16 Change Management Policy

16.1 Objective.

The Purpose of this policy is to ensure that all the changes made in APTRANSCO's IT facilities and support systems must be in a controlled and consistent manner.

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and

procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

16.2 Scope of Change Management Policy

16.2.1 The change management policy applies to all changes to the following areas:

16.2.1.1 Changes to Operating systems, which must include service packs, configuration changes, and version upgrades.

16.2.1.2 Changes to applications, which must include application of patches, configuration changes, and version upgrades.

16.2.1.3 Changes to networks and network devices like routers, switches, firewall, etc. This must include changes to router and switch configurations, IOS, firewall policy changes, network layout/traffic changes and changes to intrusion detection systems.

16.2.1.4 Changes to IT hardware such as change of RAM, CPU and HDDs etc.

16.2.1.5 Additions of new application/new Hardware to the existing setup. Relocation of the application to a different server/location.

16.2.1.6 Changes relating to User Access Modifications.

16.3 Policy Details

16.3.1 Change Management and Documentation

16.3.1.1 The change management process must involve documenting and managing the change requests.

16.3.1.2 The documentation must provide for a brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking and controlling modifications and assigning a unique number to each request.

16.3.1.3 All changes must be scheduled and all the affected parties must be informed in advance of the change.

16.3.1.4 All Change Request initiated as per the standard change request procedure and shall be evaluated by corresponding module owners and further approved by the CISO before implementation.

16.3.1.5 All changes have to be reviewed after the roll out.

16.3.1.6 Post-implementation reviews shall be performed for the critical IT solutions developed to assess whether the system delivered the benefits envisioned in the most cost efficient and effective manner.

16.3.2 Change Approval

16.3.2.1 The immediate controlling authority of the user requesting the change must approve all change requests, based on business requirements. This request will be forwarded to the HOD of IT Wing or higher approving authority, which will then be forwarded post validation to the IT Wing or ask for more clarifications from the end user.

16.3.2.2 If the change request involves incorporating any data from a different application, the Data Owner of that application must also approve the request.

16.3.2.3 An assessment of the proposed system changes must be performed to assess its potential impact on APTRANSCO's computing systems, before its approval.

16.3.3 **Testing of Changes and Backup**

16.3.3.1 All changes/patches must be tested before being carried out in the live/ production environment, wherever required.

16.3.3.2 A quality assurance test of the changes /patches to be implemented and must be performed in a test environment prior to implementation in the production environment wherever applicable.

16.3.3.3 A backup of the system impacted by the change/patch must be made prior to it being updated.

16.3.4 **Unscheduled/Emergency Changes**

16.3.4.1 Unscheduled/emergency changes must be carried out only in case there are critical production issues, which require the change to be carried out.

16.3.4.2 Any unscheduled changes must not be done without proper approval of CISO APTRANSCO/Change Control Board

16.3.4.3 An audit trail of the emergency activity must also be generated which logs all activity, including but not limited to:

16.3.4.3.1 The user-ID making the change

16.3.4.3.2 Time and date

16.3.4.3.3 The commands executed

16.3.4.3.4 The program and data files affected

16.3.5 **User ID and Access Changes**

16.3.5.1 Any changes to user id including changes to the authorization levels must be done by following the procedure defined in Access Control policy.

16.3.5.2 The change must involve raising a request by his/her and approval of the same by HOD of IT wing

16.3.5.3 All changes must be documented and a trail must be maintained by means of preserving the change requests.

16.3.6 **Hardware Changes**

16.3.6.1 Any changes to hardware must be done by following the change management process which includes raising of change request, approval by the appropriate authorities and documentation of the same.

16.3.6.2 The custodian of the hardware must conduct all the hardware changes after due approval of the change.

16.3.6.3 Changes done to the hardware must be updated in the hardware/Asset register after the change is done.

16.3.6.4 Changes done to the hardware must be monitored after the change to ensure that there is no untoward affect due to the change.

16.3.7 **Operating System and Application Changes**

16.3.7.1 Any change to operating system (OS) or application must be strictly controlled by the use of the change management process, which will

include raising of change request, testing, approval by the appropriate authorities and documentation of the same.

16.3.7.2 All changes must be documented and a trail must be maintained by means of preserving the change requests.

16.3.7.3 Any change that involves downtime or disruption of services must be done after giving an appropriate notification to the affected users.

16.3.8 **Patch and Service pack management**

16.3.8.1 Application of patches must be done in a controlled manner.

16.3.8.2 Only tested versions of the patch or service pack must be considered for application, wherever needed.

16.3.8.3 The patch or service pack must be obtained directly from the vendor or downloaded from the vendor site only.

16.3.8.4 On successful testing by the nominated personnel defined and the functional users, the patch must be applied on the production systems with approval from HOD / IT wing or Management.

16.3.8.5 For desktop related patches, the application must be done in a scheduled manner.

16.3.8.6 Wherever patches need to be installed, they shall be tested and evaluated before being installed to ensure they are effective and do not result in complications that cannot be tolerated.

16.3.8.7 Service pack updates shall undergo change management.

16.3.9 **Addition of hardware/Software and any other IT resource**

16.3.9.1 All hardware or any other resource addition or removal of it from the production environment would be controlled and approved and a complete track of it maintained to ensure minimum-disruption to the operating environment.

16.4 Do's and Don'ts of Change Management Policy

DO'S	DON'TS
• Create a Change Advisory Board (CAB): Assemble a Diverse Team: Include representatives from various departments to provide comprehensive evaluations of proposed changes	• Don't Bypass the Approval Process: Avoid Unapproved Changes: Ensure all changes go through the proper approval channels
• Conduct Risk Assessments: Evaluate Risks: Assess the potential impact and risks associated with each proposed change.	• Don't Underestimate the Impact of Changes: Assess All Changes: Thoroughly evaluate the potential impact of all changes, regardless of size
• Implement a Change Request System: Use a Standardized Form: Implement a standardized change request form to capture all necessary information.	• Don't Ignore Stakeholder Communication: Keep Stakeholders Informed: Regularly update stakeholders on the status and impact of changes

- Conduct Testing and Validation:
  Test Changes: Thoroughly test changes in a controlled environment before implementation.
- Don't Neglect Documentation:
  Document Everything: Ensure that all aspects of the change process are thoroughly documented.

16.5 Point of Contact

CISO/Designated Authority

17 Clear Desk and Clear Screen Policy

17.1 Objective.

To establish a policy that will provide guidance in the protection of private information. The purpose of the Clear Desk and Clear Screen Policy is set guidelines which reduce the risk of a exposure of sensitive data to unauthorized individuals, such as cleaning staff or outside vendors, avoid security breach, fraud and information theft caused by documents being left unattended in the Authority's premises**.**

17.2 Scope

This policy applies to employees of APTRANSCO, including all personnel affiliated with third parties. This policy applies to all IT equipment that is owned or leased by APTRANSCO.

17.3 Policy

Computers/Computer Terminals should not be Left Logged On when unattended and should be Password Protected.

17.3.1 Employees are required to keep information and operational assets like printouts of project deliverables, notepads containing sensitive data, etc. in a secured place when not in use, especially after working hours.

17.3.2 Computer screens should be angled away from the view of unauthorized persons.

17.3.3 The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time (5 mins).

17.3.4 The Windows Security Lock should be password protected for reactivation.

17.3.5 Users should log off their machines when they leave the room and should be educated for the same.

17.3.6 Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

17.3.7 Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors must be locked if left unattended. At the end of each session all sensitive information should be removed from the workplace and stored in a locked area. This includes all identifiable information, as well as business critical information such as salaries and contracts.

17.3.8 Sensitive or classified information, when printed, should be cleared from printers immediately.

17.3.9 Keys used for access to confidential, restricted or sensitive information must not be

left in or on an unattended desk. Keys for desk drawers, cabinets and other secure areas must be stored in the dedicated key safe

17.3.10 Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down and left in an accessible location

17.3.11 Whiteboards containing restricted and/or sensitive information should be erased.

17.4 Do's and Don'ts of Clear Desk and Clear Screen Policy

DO'S	DON'TS
• Educate Employees: Provide Training: Conduct training sessions to explain the importance of the policy and how to comply with it.	• Don't Overlook Training: Skip Training: Avoid assuming that employees will understand the policy without formal training.
• Enforce Clear Desk Practices: End of Day Checks: Ensure employees clear their desks of all documents, notes, and removable media before leaving.	• Don't Ignore Non-Compliance: Ignore Violations: Don't overlook violations of the policy; address them promptly and consistently.
• Monitor Compliance: Regular Audits: Conduct regular checks to ensure employees are following the policy.	• Don't Allow Exceptions: Inconsistent Enforcement: Avoid allowing exceptions to the policy, as this can lead to confusion and non-compliance.
• Provide Necessary Tools: Shredders: Place shredders in convenient locations for the secure disposal of sensitive documents	• Don't Forget About Digital Security: Neglect Digital Data: Don't focus solely on physical documents and ignore the security of digital data.

17.5 Point of Contact

CISO/ Designated Authority

18. Incident Management Policy

18.1 Objective

To establish response procedures that ensure the quick, orderly and effective handling of IT & Cyber related security incidents / threats in APTRANSCO.

18.2 Scope

This policy addresses the definition and documentation of IT & Cyber security incident management procedures for such systems and services in APTRANSCO.

18.3 Policy

18.3.1 Incident Management Practice Standard

18.3.1.1 IT Team shall be identified for handling the IT & Cyber security incidents within APTRANSCO.

18.3.1.2 IT Team shall have pre-defined roles and responsibilities for incident management, which can take priority over normal duties.

18.3.1.3 Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, and interference in communication etc. is suspected or confirmed, the appropriate Incident Management procedure as stated below must be followed:

18.3.1.3.1 IT Team should be notified of such security incident through a mail or a call, and henceforth IT Team would be responsible for analyzing, initiating the appropriate incident management action including restoration, as per established guidelines.

18.3.1.4 The CISO will be determining the physical and electronic evidence to be gathered as part of the Incident Investigation.

18.3.1.5 The appropriate technical resources from the IT Team are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

18.3.1.6 The CISO will determine if a widespread communication is required, the content of the communication, and how best to distribute the communication.

18.3.1.7 The appropriate technical resources from the IT Team are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

18.3.1.8 The CISO will be initiating, completing, and documenting the incident investigation with assistance from the IT Team.

18.3.1.9 If an incident is detected by any employee, the concerned employee must Immediately bring it to the notice of the IT security team. The concerned team will complete the Incident Response checklist and additionally inform to CISO depending on the nature and criticality of incident.

18.3.1.10 If it is determined that the incident is real, the details of the incident are recorded in the Incident log book.

18.3.1.11 The CISO will report the incident to the higher authorities of the organization and coordinating with the crisis management team, as required.

18.3.2 **Implementation Principle**

18.3.2.1 Roles and Responsibilities:

18.3.2.1.1 Roles and Responsibilities should be delegated to appropriately trained personnel.

18.3.2.1.2 Roles and responsibilities of personnel delegated to carry out this policy should be clearly defined in order to ensure co-operative functioning.

18.3.2.1.3 Establishing security incident management framework.

18.3.2.1.4 Developing and reviewing the processes, framework, policy and procedures for incident management.

18.3.2.1.5 Identifying, documenting and maintaining rules for collection, retention and presentation of information security incident evidences.

18.3.2.1.6 Managing the response to an incident and ensuring that all procedures are correctly followed.

18.3.2.1.7 Reviewing incidents to determine what lessons can be learnt and what process improvement may be required.

18.3.2.1.8 Reporting to Management any serious incidents that may require a critical decision

18.3.2.1.9 A Cyber Security Incident that causes a critical situation that would negatively affect the organization's profitability, reputation or ability to operate, will be categorized as a Cyber Crisis and it would be dealt with as per the Cyber Crisis Management Plan (CCMP) of APTRANSCO.

18.3.2.2 Resources

18.3.2.2.1 Sufficient funds, resources and organizational support are provided to ensure the effective implementation of this policy.

18.3.3 **Analysis of Security Incident**

18.3.3.1 The incidents/weaknesses are collated and analyzed to detect trends. This analysis report indicates the following:

18.3.3.1.1 Number of Incident Logged.

18.3.3.1.2 No. of incidents closed

18.3.3.1.3 Actual time to resolve

18.3.3.1.4 Corrective action taken

18.3.3.1.5 Root Cause Analysis

18.3.3.1.6 Lessons learnt

18.3.3.1.7 Any monetary/ reputation/ client losses incurred

18.3.3.1.8 Preventive actions to be initiated

18.3.3.1.9 How it will impact on APTRANSCO activities.

18.3.4 **Managing Critical Incidents**

The comprehensive Management of Incidents will comprise 4 stages. Each stage has a number of issues and strategies that are relevant to successful outcomes. The 4 stages are:

1. Preparation and Prevention
2. Critical Incident Response Management
3. Post-Incident Management
4. Review

18.3.4.1 **Stage 1:** Preparation and Prevention

Preparation and Prevention may occur either before any outward disturbances are apparent or When disturbances occur but have not yet resulted in a critical incident or after a critical incident occurs, to prevent repetition, the main activities are preparation and education by –

a). General Education

b). Information

c). Training

d). Discussion

18.3.4.2 **Stage 2:** Critical Incident Response Management

18.3.4.2.1 A response to the critical incident needs to be planned and a rapid and effective intervention needs to be implemented. An accurate assessment of the person/situation needs to be made. This is critical otherwise inadequate action may be taken. A number of factors need to be considered.

a). Type of incident

b). Levels of risk and Probable Severity

c). Levels of Urgency

d). Implications of the incident

18.3.4.2.2 Assessment is usually ongoing until the situation is dealt with/resolved.

a). Accountability hierarchy in relation to assessment of level of risk and urgency should be clarified

b). Carrying out of intervention plan.

c). Contacting outside service emergency protocols need to be developed with minimum time delay.

d). Containing, waiting for services to arrive.

e). If incident is ongoing (e.g. stalker or threats), continual assessment, planning and intervention needs to take place.

18.3.4.3 **Stage 3:** Post Incident Management

18.3.4.3.1 A plan of recommended interventions will need to be made practicable, and may include any of the following:

a). An assessment of the degree of trauma and the affected persons

b). Defusing of involved persons within 8 hours of incident.

c). Psychological debriefing of employee and staff: 1-3 days after the incident (except legal processes contra-indicate)

d). Involvement of outside consultants in critical incident management and debriefing.

e). Counseling/ treatment/ group sessions for affected persons

f). Training groups in stress management and coping strategies

g). Provision of Information about community mental health services

h). Contribution to media releases

18.3.4.4 Stage 4: **Review of each Incident Management Process**

A system of reviewing action taken at specific critical incidents should be developed and carried out by the IT Team. This may include debriefing of the IT Team and assisting staff.

18.3.4.4.1 Checklist to be followed - Preparation

a). Were controls applicable to the specific incident working properly?

b). What conditions allowed the incident to occur?

c). Could more education of users or administrators have prevented the incident?

d). Were all of the people necessary to respond to the incident familiar with the incident response plan?

e). Were any actions that required management approval clear to participants throughout the incident?

18.3.4.4.2 Detection

a). How soon after the incident started did the APTRANSCO detect it?

b). Could different or better logging/process have enabled APTRANSCO to detect the incident sooner?

c). Does the APTRANSCO even know exactly when the incident started?

d). How smooth was the process of invoking the incident response plan?

e). Were appropriate individuals outside of the incident response team notified?

f). How well did the APTRANSCO follow the plan?

g). Were the appropriate people available when the response team was called?

h). Should there have been communication to inside and outside parties at this time; and if so, was it done?

i). Did all communication flow from the appropriate source?

18.3.4.4.3 Containment

a). How well was the incident contained?

b). Do the available staff have sufficient skills to do an effective job of containment?

c). If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people?

d). Are there changes that could be made to the environment that would have made containment easier or faster?

e). Did technical staff document all of their activities?

18.3.4.4.4 Eradication and Recovery

a). Was the recovery complete? Was any data permanently lost?

b). If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?

c). Were the technical processes used during these phases smooth?

d). Was staff available with the necessary background and skills?

18.4 Do's and Don'ts of Incident Management Policy

DO'S	DON'TS
• Establish Clear Procedures: Define Incident Categories: Clearly classify different types of incidents (e.g., security breaches, system failures).	• Don't Neglect Documentation: Document All Incidents: Ensure that all incidents are thoroughly documented, including actions taken and outcomes
• Implement a Reporting System: Use a Centralized System: Implement a centralized system for logging and tracking incidents.	• Don't Rely on a Single Point of Contact: Avoid Single Points of Failure: Ensure there are multiple points of contact for incident reporting and response.
• Conduct Risk Assessments: Identify Potential Threats: Regularly assess potential threats and vulnerabilities	• Don't Skip Training: Regular Training: Don't neglect regular training and updates for employees and the incident response team.
• Develop an Incident Response Plan: Create Response Plans: Develop specific response plans for different types of incidents.	• Don't Neglect Legal and Regulatory Requirements: Ensure Compliance: Don't ignore legal and regulatory requirements related to incident management.

18.5 Point of Contact

CISO/Designated Authority

19 Asset Management Policy

19.1 Objective

This document describes the Asset Management and Asset Purchase Policy for IT and OT assets of APTRANSCO.

19.2 Scope

The policy covers the IT and OT assets of hardware, software and data of APTRANSCO. The scope of this policy includes purchase and procurement of any IT and OT asset for any APTRANSCO employee or other Wing.

19.3 Policy

19.3.1 **Responsibility for Assets**

19.3.1.1 **Identification and Inventory of assets**

19.3.1.1.1 The first step should be the identification of all assets and record relevant information about them, like their location, Usage, Asset value, criticality etc. The assets of APTRANSCO includes:

a). Information: Databases, Contracts and agreements, Manuals, Policies, Procedures and Plans, Backups, source codes etc.

b). Software: System software, Application software, Development tools, Utilities etc.

c). Hardware: Computing and Network hardware, communication services etc.

d). Personnel: People and their location, Roles/Designation, qualifications and skills.

e). Services: The services the organization acquires either in-house or outsourced.

19.3.1.2 **Ownership and Responsible Use of assets**

Assigning ownership entails responsibility. Every asset should have a designated owner. All employees should be made aware of the Information Security Acceptable Usage Policy which should be accessible to them for reference

19.3.2 **Asset Classification**

19.3.2.1 **Classification guidelines**

19.3.2.1.1 The basis of the Asset classification should be its value, criticality (CIA) and legal requirements for APTRANSCO.

19.3.2.1.2 Criticality of an Asset can be classified taking into account the confidentiality value, availability value and integrity value of the information contained/processed by the Asset.

19.3.2.1.3 Classification for APTRANSCO Asset's is given below:

Classification Level	Definition	Examples
RESTRICTED (LEVEL IV)	This classification applies to the most sensitive Asset, which is intended strictly for use within APTRANSCO. Its unauthorized access could seriously and adversely impact APTRANSCO, its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion.	Merger and acquisition plans, planning for existing litigation, trade secrets, customer data, and information security data, Strategy Documents. NAT(Network Address Translation) and routing details.
CONFIDENTIAL (LEVEL III)	This classification applies to less sensitive Assets, which are intended for use within APTRANSCO. Its unauthorized access could adversely impact APTRANSCO, its stockholders, business partners, employees, and/or customers. Information that some people would consider to be private is included in this classification.	Employee performance evaluations , internal audit reports, Procedures, Short-term marketing plans, analyses of competitive products / services and intellectual capital of APTRANSCO which comprises the collective experience, knowledge, skill and information of APTRANSCO and its people.
INTERNAL (LEVEL II)	This classification applies to Assets, which are Generally accessible to APTRANSCO employees. The access to such Information/asset may be through a unique authentication or may be accessible through the privileges of being an APTRANSCO employee. While its unauthorized Access/ disclosure is against policy, it is not expected to seriously or adversely impact APTRANSCO employees / customer's stockholders & business partners.	APTRANSCO telephone Directory, training materials, and policy manuals and other office information through Intranet. .
PUBLIC (LEVEL I)	This classification applies to information, which has been explicitly approved by APTRANSCO's management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	Service brochures, advertisements, job opening announcements, and press releases etc.

19.3.2.2 Information labeling and handling

19.3.2.2.1 All the information should be labeled according to the information classification scheme.

19.3.2.2.2 Rules shall also be made for the handling of information. The handling means their processing, storage and destruction.

19.3.2.3 **IT administrator's scope of work**

To ensure that all the users IT and OT assets are labeled / tagged as per the given policy. "No IT and OT assets are left un-tagged."

19.3.3 **New device commission guidelines**

19.3.3.1 The information Systems being deployed must be configured in accordance with corresponding guidelines:

19.3.3.1.1 The information security requirements of the asset to be purchased / developed must be established and evaluated before the capex expenditure/approval.

19.3.3.1.2 The information System shall be updated with authorized patches/ service packs before deployment.

19.3.3.1.3 The information System shall be configured and tested for various loads to verify the robustness and correctness of the configuration.

19.3.3.1.4 The information System shall be declared deployed on the production environment after passing UAT, wherever required.

19.3.4 **IT Assets Audit**

19.3.4.1 CISO assigns Team members from IT TEAM Wing for the inventory audits.

19.3.4.2 Team members refer to the Inventory Register and cross check the entry.

19.3.4.3 The system is checked for the hardware information that includes ID, make, model, configuration and service tag number, serial number, IP address, host name, user and department information, software installed.

19.3.4.4 In case of any discrepancy, CISO or his designated Support member is informed and the discrepancy is resolved.

19.3.4.5 This check is done yearly.

19.3.5 **IT Asset Purchase Policy**

As per IT Policy / DOP

19.4 Do's and Don'ts Asset Management Policy

DO'S	DON'TS
• Develop Clear Asset Management Procedures: Clearly outline processes for acquiring, tracking, maintaining, and disposing of assets.	• Don't Ignore Asset Documentation: Incomplete Records: Avoid keeping incomplete or outdated records of assets.

- Maintain an Accurate Asset Inventory: Utilize software tools to keep a detailed and up-to-date inventory of all assets.
- Classify Assets: Classify assets by type, such as hardware, software, and physical equipment.
- Secure Digital Assets: Use Encryption: Encrypt sensitive data stored on digital assets.
- Don't Dispose of Assets Improperly: Improper Disposal: Don't dispose of assets without securely erasing sensitive data.
- Don't Allow Unauthorized Access: Unrestricted Access: Don't allow unrestricted access to assets, especially sensitive digital assets.
- Don't Allow Asset Misuse: Don't allow employees to use company assets for personal purposes without authorization.

19.5 Point Of Contact

CISO/Designated Authority

20 Capacity Management Policy

20.1 Objective

"Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner." As the usage of IT Services change and functionality evolves, the amount of processing power, memory etc. also changes. If it is possible to understand the demands being made currently, and how they will change over time, this approach proposes that planning for IT Service growth becomes easier and less reactive.

20.2 Scope

20.2.1 The Capacity management policy intended to optimize performance and efficiency is concerned with following areas:

20.2.1.1 Monitoring the performance and throughput or load on a server,

20.2.1.2 Performance analysis of measurement data, including analysis of the impact of new releases on capacity

20.2.1.3 Performance tuning activities to ensure the most efficient use of existing infrastructure

20.2.1.4 Understanding the demands on the Service and future plans for workload growth (or shrinkage)

20.2.1.5 Influences on demand for computing resources

20.2.1.6 Capacity planning – developing a plan for the Service

20.2.1.7 Capacity management interacts with the discipline of Performance Engineering, both during the requirements and design activities of building a system, and when using performance monitoring as an input for managing capacity of deployed systems.

20.2.1.8 If new resources or technology are to be introduced in the System, evaluation and testing is performed on the test environment before introducing into live environment.

20.3 Policy Details

20.3.1 Capacity Management Activity:

20.3.1.1 The capacity management evaluation will be done by the IT team on annual basis and will submit their individual report to the CISO.

20.4 Do's and Don'ts of Capacity Management Policy

DO'S	DON'TS
• **Define Clear Objectives:** Set Goals: Clearly define the objectives of the capacity management policy, such as optimizing resource use, minimizing downtime, and planning for future growth.	• **Don't Neglect Monitoring:** Ignore Real-Time Data: Don't neglect real-time monitoring of resource usage; it's crucial for identifying immediate issues.
• Implement Capacity Planning: Forecast Demand: Use historical data and market trends to forecast future demand.	• Don't Underestimate Future Demand: Short-Term Focus: Don't focus solely on current capacity needs; plan for future growth and demand.
• Optimize Resource Utilization: Balance Loads: Distribute workloads evenly across available resources to prevent bottlenecks.	• Don't Rely Solely on Manual Processes: Manual Tracking: Avoid relying only on manual tracking of capacity data; use automated tools for accuracy and efficiency.
• Implement Capacity Management Tools: Use Specialized Software: Utilize capacity management tools to track and analyze resource usage.	• Don't Overlook Staff Training: Untrained Staff: Don't neglect training staff on capacity management tools and processes.

20.5 Point of Contact

CISO /Designated Authority

21 Data Classification Policy

21.1 Objective

To ensure that integrity, confidentiality and ownership of IT information is maintained, a data classification scheme needs to be designed for APTRANSCO. The level of security to be afforded to the information of APTRANSCO will depend directly on the classification of the data. All employees, especially those who may come into contact with "sensitive" information are expected to familiarize themselves with this data classification scheme and to consistently use it in their business activities. "Sensitive" information is either "confidential" or "restricted" information.

21.2 Scope

This section addresses policies and procedures related to the classification of data processed, generated, handled, transmitted, received and shared by all employees of APTRANSCO and the people dealing with APTRANSCO. This Policy applies to all APTRANSCO employees dealing with all APTRANSCO's IT related Digital data.

21.3 Summary of procedures

21.3.1 Consistent protection for the information

21.3.2 Preconditions/ rules for data classification

21.3.3 Data classification matrix

21.3.4 Minimum baseline security controls (MBSC)

21.3.5 Consistent classification labels

21.3.6 Review of classified data and associated security measures

21.3.7 Declassification / Downgrading

21.4 Executive owner

The respective data owners are responsible for execution of the policy on data classification. The top management and CISO should consistently review APTRANSCO compliance to data classification policies and procedures.

21.5 Procedures

21.5.1 Need to Know

One of the fundamental principles of IT & Cyber security is the "need to know." This principle holds that information should be disclosed only to those people who have a legitimate business need for the information. The data classification scheme has been designed to support the "need to know" policy so that information will be protected from unauthorized disclosure, use, modification and deletion.

21.5.2 Consistent Protection

The digital information of APTRANSCO must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology was used to handle it and what purpose it serves. Although this data classification scheme provides overall guidance to achieve consistent information protection, employees need to apply and extend these concepts to fit the needs of day-to-day operations.

21.5.3 Rules for Asset Classification

All assets at APTRANSCO are to be maintained in an inventory with nominated owners and classification. The classification is to be determined on the basis of criticality, value and legality impacts on the asset.

21.5.4 **Rules for Data Classification**

All information possessed by or used by a particular Department/branch Office/regional office/franchisee office/business within APTRANSCO must have a designated information owner. The information owners will be responsible for assigning/maintaining appropriate data classifications as defined in Asset Management Policy.

21.5.4.1 Files/ e-mails created by individuals will be owned and classified by them.

21.5.4.2 The data classification process must be completed for existing data and must be undertaken for any new application development project at the time of designing the new application.

21.5.4.3 Information stored in several media formats (either hard copy or electronic) will have the same level of classification.

21.5.5 **Cumulative Classification**

The data classification levels represent cumulative information sensitivity. As the levels of sensitivity increase, the access and modification controls become more rigorous and comprehensive. For example, confidential information is a restricted subset of internal information and requires additional security controls.

21.5.6 **Security Control Matrix Guidelines.**

The requirements in the following table outline the minimum baseline security control (MBSC) mechanisms that must be used for each information classification.

Security Objective	**Information Classification**			
	Public	**Internal**	**Confidential**	**Restricted**
Identification and Authentication	None	User IDs	Strong Authentication (pins, token, certificate, smart cards)	Strong Authentication, Passwords
Authorization and Access Control	Access Control for Modification	Authorization for granting access by business department head, access control as per functions, or directory level access control	Fine-grained access control - by document and directories	Access control and authorization at the field level
Confidentiality	None	Encryption over public communications facilities (Internet, dial-up)	Encrypted communications (all), and encrypted files on storage media	Encrypted communications and encrypted files on storage media
Integrity	Access / change control	Minimal audit trail (e.g., document history), data integrity checks	Encryption, detailed audit trail (e.g., system level file history), “maker-checker”	Field-level change history

Non-repudiation	Access / change control	Minimal audit trail (e.g. document history)	Detailed audit trail (e.g., system level file history), digital signatures	Field-level change history, digital signatures
Auditing	Modification, events, alarms	User activities, access denials, alarms	User activities, file changes, access denials, alarms	All events, alarms
Availability	Virus scanning, backup/restore	Virus scanning, backup/restore	Virus scanning, strong change control over system configuration, backup/restore	Virus scanning, strong change control over system configuration, backup/restore

Table No.2

For example, for achieving the objective of Identification and Authentication, no security mechanism would be required for public data. While User IDs and passwords would suffice for internal data, stronger authentication techniques such as pins, tokens, biometrics, smart cards etc. may be required for Confidential and Restricted data.

Note: While reading the above table, it must be kept in mind that the security mechanisms to be applied at a level are additional to those indicated at the previous level. It may also be noted that the above matrix is merely suggestive of the kind of controls / mechanisms that may be applied for a particular classification. Controls suggested for confidential data, may therefore, also be applied for restricted data and so on.

21.5.7 **Consistent Classification Labels**

All information whether restricted, confidential, internal or public must be labelled accordingly; from the time it is created until the time it is destroyed or re-labelled. Such markings must appear on all manifestations of the information. For public information, the date when the owner declared the information public, must also be indicated. The LAN and Desktop Security Administrator will have list of all Data classifications and Ownership.

21.5.8 **Review of classified data**

A regular audit of the classified data and applied security controls should be conducted.

21.5.9 **Declassification / Downgrading**

The designated information owner may, at any time, declassify or downgrade information. To achieve this, the concern must change the classification label appearing on the original document and inform CISO and all known recipients / users.

21.5.9.1 If known, the date on which restricted or confidential information will no longer be sensitive (declassified) must be indicated on all sensitive information of APTRANSCO.

21.5.9.2 The designated information owner may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.

21.5.9.3 To determine whether sensitive information may be declassified or downgraded, at least once a year, information owners must review the sensitivity classifications assigned to information for which they are responsible.

21.6 Do's and Don'ts of Data Classification Policy

DO'S	DON'TS
• Involve Key Stakeholders: Collaborate: Work with key stakeholders from various departments to ensure the policy meets the organization's need	• Don't Neglect Employee Training: Assume Knowledge: Don't assume that employees know how to classify data without proper training.
• Develop Comprehensive Guidelines: Detail Procedures: Provide detailed guidelines for classifying data, including specific criteria and steps.	• Don't Ignore User Feedback: Disregard Input: Don't ignore feedback from employees who are using the classification system daily.
• Ensure Consistent Application: Standardize Processes: Establish standardized processes for classifying and handling data.	• Don't Overlook Data Classification Tools: Manual Processes: Avoid relying solely on manual processes for data classification.
• Protect Sensitive Data: Implement Security Measures: Apply appropriate security measures (e.g., encryption, access controls) based on the data classification level.	• Don't Underestimate the Importance of Security: Weak Controls: Don't apply weak security controls to sensitive data.

21.7 Point of Contact

CISO/Designated Authority

22 Removable Media Disposal Policy

22.1 Objective

Organizational data is information that supports the mission of APTRANSCO. It is a vital asset and is owned by the APTRANSCO. APTRANSCO's IT related digital data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth APTRANSCO's standards with regard to the disposal of removable media.

22.2 Scope

To establish policy for the safeguarding of restricted and sensitive IT related digital data relating to customer, client and APTRANSCO personnel that is created, received, maintained or transmitted by the APTRANSCO. This policy is intended to ensure that Media containing business information shall be destroyed before disposing them.

22.3 Policy

22.3.1 **Media Disposal**

22.3.1.1 Information and data held in paper or hard copy which contain sensitive Information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, or incineration

22.3.1.2 All IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

22.3.1.3 Where an overwrite procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed.

22.3.1.4 For the avoidance of doubt, removable digital media including but not limited to CDs, DVDs, USB drives, where the default is that they contain sensitive data, shall, if not successfully overwritten, be physically destroyed to the extent that all data contained in the media are irretrievable.

22.3.1.5 All IT equipment awaiting disposal must be stored and handled securely.

22.3.1.6 Where the overwriting procedure and/or physical destruction of IT equipment are carried out on behalf of the APTRANSCO by a third party, there shall be a contract with that third party which appropriately evidences that party's obligations to keep that data confidential.

22.3.1.7 In any case where IT equipment is to be passed on by the APTRANSCO for re-use, those employees involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed.

22.3.1.8 All disposals of sensitive media shall be recorded for audit trails.

22.4 Do's and Don'ts of Removable Media Disposal Policy

DO'S	DON'TS
• Implement Secure Disposal Methods: Physical Destruction: Use methods like shredding, crushing, or incinerating to physically destroy the media.	• Don't Dispose of Media Carelessly: Improper Disposal: Avoid disposing of removable media in regular trash bins where it can be easily accessed.

- Classify Data on Media:
  Data Classification: Classify data stored on removable media to determine the appropriate level of security required for disposal.
- Use Certified Vendors:
  Certified Disposal Services: Partner with certified vendors who specialize in secure media disposal.
- Use Encryption:
  Encrypt Data: Encrypt data on removable media to add an extra layer of security in case of loss or theft before disposal.
- Don't Ignore Data Wiping:
  Incomplete Erasure: Don't assume data is completely erased without using certified data wiping tools.
- Don't Skip Employee Training:
  Untrained Staff: Don't assume employees understand the proper disposal procedures without adequate training.
  Don't Forget to Document Disposals:
  No Records: Avoid disposing of media without keeping a detailed record of the disposal.

22.5 Point of Contact :

CISO /Designated Authority

Section –II

IT & Cyber Security Policy for End Users

1. Anti-Virus

1.1. Ensure that Anti-Virus client is loaded & scheduled on the desktop or other devices prior to connecting to LAN.

1.2. Ensure Virus updates are loaded on standalone desktop / Laptop / other devices before putting on use.

1.3. Virus infected computers must be removed from the network until they are verified as virus free by IT TEAM Official/Coordinator.

1.4. Never download files from unknown or suspicious sources.

1.5. Any desktop, showing symptoms of a virus, unusual behavior or flashing un-meaningful messages shall be immediately removed from the network and matter shall be reported to the Helpdesk, IT TEAM Wing.

1.6. Usage of USB drives should be restricted through suitable blocking option. However, if it is required to be used, Permission from competent authority should be obtained prior to unblocking/enabling of the USB ports. The USB drives shall be scanned for any viruses/malware etc.

1.7. Pirated or gifted copies of software shall not be used as these may contain virus and even facilitate intrusions into the system.

1.8. Computer games are prohibited to run on the computer. These could be the main carriers of Computer viruses and an unsuspecting easy medium for an intruder to break into the computer.

1.9. Any mail from unknown source shall not be opened as it might be malicious mail.

1.10. Usage of internet connectivity through dialup or other internet providers is not permitted within APTRANSCO's network to avoid virus activities.

1.11. Do not load disks/flash drives of unknown origin & incoming disks/flash drives shall be scanned for viruses before they are read

1.12. Do not uninstall (remove) or disable the official anti-virus program on your computer, nor install a program of your choice.

➢ **Do's and Don'ts of Anti-Virus Policy**

DO'S	DON'TS
• Install and Regularly Update Anti-Virus Software: Approved Software: Use only the organization-approved anti-virus software.	• Don't Disable Anti-Virus Software: Continuous Protection: Never disable your anti-virus software, even temporarily.
• Perform Regular Scans: Scheduled Scans: Set your anti-virus software to perform regular, scheduled scans.	• Don't Ignore Alerts: Immediate Action: Don't ignore alerts or notifications from your anti-virus software.
• Enable Real-Time Protection: Active Monitoring: Ensure real-time protection is enabled to continuously monitor your system for threats.	• Don't Use Unapproved Software: Third-Party Software: Avoid using unapproved third-party anti-virus or security software.
• Backup Important Data: Regular Backups: Regularly back up important data to a secure location.	• Don't Overlook Software Updates: Postponing Updates: Don't postpone software updates, as they often include critical security patches.

2. Password Management

2.1. Password shall be complex & may comprise of alphabets in upper case as well as in lower case, numbers, special characters etc. Use strong password should be minimum 8 characters long containing alphabet (Upper & Lower case), numeral and special characters. e.g:Task@25109$%

2.2. Few Guidelines for creating password:

2.2.1 Password must be at least eight alphanumeric characters long.

2.2.2 Password shall not be a dictionary word in any language, slang, dialect, jargon etc.

2.2.3 Passwords shall not be based on personal information, names of family etc.

2.3. If an account or password is suspected to have been compromised, it must be reported to Helpdesk, IT TEAM Wing and change all passwords.

2.4. All Power-on passwords must be changed at least once every quarter.

2.5. Don’t enter wrong password more than 3 times.

2.6. For password reset contact IT In charge/ADMIN

2.7. As user is wholly responsible for activities against his/her user-ids, sharing of passwords with others is not recommended as per good security practice.

2.8. Avoid keeping a paper record of passwords. User should not divulge passwords to other users. Authorized users are responsible for the security of their passwords.

2.9. All user-level passwords (e.g., network, application-level password, intranet personal dashboard, etc.) must be changed at least every three months. The recommended change interval is every 45 days.

2.10. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

2.11. Password must not be shared at any point of time, if such request is made it must be denied and requestor must be informed to speak to IT TEAM Wing.

2.12. Passwords used to sign on to the various Internet sites may be intercepted anywhere along the network. Hence Users shall consider using a different password on the Internet from that used for signing on to their systems for various applications. Users shall safeguard passwords and not leave them in predictable places, like desk/drawers

2.13. Separate password shall be used for various APTRANSCO accounts. For example, select one password for the Intranet Personal Account and a separate password for Network login.

2.14. APTRANSCO passwords shall not be shared with anyone. All passwords are to be treated as sensitive & confidential. Password must not be revealed to ANYONE over the phone.

2.15. Regular password must not be revealed in an E-Mail message or any other form of electronic communication.

2.16. Password must not be told to the juniors for the sake of comfort.

2.17. Password must not be talked about/discussed in front of others.

2.18. Password on questionnaires or security forms must not be revealed.

2.19. Password shall not be shared with family members or co-workers

2.20. The "Remember Password" feature of applications shall not be used. Do not include passwords in any automated log-on process, e.g., stored in a macro or function key or “remember password”.

2.21. Passwords shall not be written down or stored in a file on any computer system without encryption

2.22. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User password resets shall be performed when requested by the individual/IT coordinator.

- **Do’s and Don’ts of Password Policy**

DO’S	DON’TS
• Implement Multi-Factor Authentication (MFA): Use MFA to provide an additional layer of security beyond just passwords.	• Don’t Use Default Passwords: Never use default passwords; always change them to strong, unique passwords during the initial setup.
• Regularly Update Passwords: Enforce regular password changes, such as every 60-90 days, to reduce the risk of compromised credentials.	• Don’t Reuse Passwords: Avoid reusing passwords across different accounts and systems to prevent a single breach from compromising multiple accounts.
• Use Password Managers: Encourage the use of reputable password managers to store and manage passwords securely.	• Don’t Store Passwords in Plain Text: Never store passwords in plain text; always use encryption and hashing mechanisms.
• Educate Users: Provide training on creating strong passwords and the importance of password security.	• Don’t Share Passwords: Prohibit the sharing of passwords among users to maintain accountability and security.

.

3. Internet Access and Usage

3.1. Browse Internet for Official purpose only. Browsing shall be done for gathering information in the interest of the Organization only.

3.2. While not working on Internet, close the browser.

3.3. Participation as a representative of APTRANSCO in Internet discussion groups’ chat rooms, or other public electronic forums or access inappropriate content like gambling sites etc. is prohibited.

3.4. Passing over of Confidential or Restricted information over the Internet without prior management approval and reasonable security measures (such as encryption or other appropriate method) in place is strongly prohibited.

3.5. Internet shall not be used for personal business purposes or for exchanging confidential /sensitive information.

3.6. Any Software (executable files), audio-video files, games, third party tools etc. shall not be downloaded installed or executed on the system without consulting Cyber Security Nodal Officer. Downloading copyright protected material from the Internet is prohibited.

3.7. Social networking sites such as Face book, YouTube, Orkut etc. shall not be accessed.

3.8. It is unauthorized to Download or view any obscene material or pornographic contents.

3.9. Attempting to gain or gaining unauthorized access to any computer System of APTRANSCO or any other organization's infrastructure is unauthorized.

3.10. Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the APTRANSCO's network without APTRANSCO'S IT team's approval.

3.11. Users are not permitted to alter network hardware in any way.

3.12. Cookies and running of active content, such as, ActiveX, JSP, PHP etc. should be allowed from the trusted sites only.

- **Do's and Don'ts of Internet Access and Usage Policy**

DO'S	DON'TS
• Understand and Follow the Policy: Familiarize yourself with the Internet Access and Usage Policy and adhere to its guidelines.	• Do Not Share Your Passwords: Never share your passwords with anyone. Each user should have a unique login.
• Use Strong Passwords: Create complex passwords and change them regularly. Use a mix of letters, numbers, and special characters.	• Avoid Unapproved Software: Do not install or use software that has not been approved by the IT department.
• Secure Your Devices: Ensure that your devices are protected with up-to-date antivirus software and firewalls.	• Do Not Access Inappropriate Content: Avoid accessing websites that are inappropriate, illegal, or not work-related.

4. E-Mail Usage- User Guideline

4.1. Use official APTRANSCO e-mails only for official correspondence, i.e the mail account provided / approved by the competent authorities shall be used for official communication.

4.2. User shall not attempt any unauthorized use of E-mail services.

4.3. Proper signatures should be used, i.e., Account Holder's full name, designation, company name (in CAPS), telephone numbers, Fax Number and Company Web Site.

4.4. If mass mailing is required in the Corporation's interest, take prior approval from the competent authority, concerned HOD's or HOD of IT wing and forward the request to Helpdesk, IT Team Wing.

4.5. All files must be scanned for viruses using antivirus program to ensure file being sent is clean of any malicious code.

4.6. Effective password protection shall be used on attachments, while communicating sensitive information via E-Mail.

4.7. If you receive any objectionable E-Mail from any employee, report the matter to Helpdesk, IT Team.

4.8. Empty the Inbox, Sent Item & Deleted Item folders regularly. Store important mails into a separate folder on the local PC, if required.

4.9. APTRANSCO's E-Mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, religious beliefs and practice, political beliefs, or national origin, Chain letters or joke E-Mail etc. Employees who receive any emails with this content from any APTRANSCO employee should report the matter to their supervisor immediately.

4.10. **Inappropriate use of the e-mail service will include, but is not limited to:**

4.11.1.1 Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

4.11.1.2 Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

4.11.1.3 Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officer's user ids or using a false identity.

4.11.1.4 Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

4.11.1.5 Creation and exchange of information in violation of any laws, including copyright laws.

4.11.1.6 Wil-full transmission of an e-mail containing a computer virus.

4.11.1.7 Misrepresentation of the identity of the sender of an email.

4.11.1.8 Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.

4.11.1.9 Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

4.11.1.10 Correspondence through official E-Mail address for personal business is strictly prohibited.

4.12 Confidential information shall not be sent in clear text using E-Mail.

4.13 Delete spam and suspicious emails; don't open, forward or reply to them. There is no thumb rule for judging such mails but some clues are helpful, like attachments not expected or not addressed directly to you, attachments with suspicious or unknown file extensions, e.g. ".exe", ".vbs", ".bin", ". Com", ".pif", ".zzx", ".zip" etc., wrong or odd file name, web links to access attachment, unusual topic lines etc.

4.14 The employees shall not try to access the email services other than official email service provided by the APTRANSCO.

4.14.1 The employees must exercise due care in retention and deletion of emails.

4.14.2 APTRANSCO employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. APTRANSCO may monitor messages without prior notice.

- **Do's and Don'ts of E-mail Usage -User Guideline Policy**

DO'S	DON'TS
• Maintain Confidentiality: Use encryption or secure methods for sending sensitive or confidential information.	• Do Not Use official Email for Personal Business: Avoid using your work email for personal communications to maintain professionalism and security.
• Log Out of Shared Devices: Always log out of your official email account when using shared or public devices to prevent unauthorized access.	• Do Not Open Suspicious Emails: Refrain from opening emails or attachments from unknown or suspicious sources to prevent phishing attacks and malware.
• Use Professional Language: Maintain a professional tone and language in all business-related emails	• Do Not Send Large Attachments Without Notice: Avoid sending large attachments without warning the recipient, as they may cause email delivery issues.
• Follow Company Email Formatting: Adhere to any company-specific email templates, signatures, and formatting guidelines.	• Do Not Share Email Credentials: Never share your email password with anyone, even trusted colleagues.

5 Desktop Policy:

5.1 Administrative passwords for desktop shall remain with concern IT Team..

5.2 Hardware configuration of Desktop after first time installation should not be changed and any requirements from users to upgrade hardware configuration must be routed to the IT TEAM subject to approval from concerned HOD of IT wing.

5.3 Allowing remote access of the desktop to an external agency will require authorization by concerned HOD's and also HOD of IT wing . on case-to-case basis.

5.4 Temporary Internet files and Cookies shall be deleted periodically.

5.5 Cleanup the Hard-Disk on regular basis using Disk Cleanup utility of the Operating system for smooth functioning of the computer.

5.6 Save files/data in drive other than root drive (generally [C:]) of Hard Disk of the Computer for smooth functioning & proper recovery of data/files in case of corruption of Operating System.

5.7 Shut Down the Computer in systematic manner.

5.8 System properties and privileges must not be changed.

5.9 Desktop / Laptop should not be left in open mode (use Ctrl+Alt+Del or Win+L to lock).

5.10 CDs/Pen Drive or any other removable storage media to run on the computer system shall not be used, and for exceptional cases specific approval of CISO/IT team is required.

5.11 Avoid Computer Shut Down by switching off the UPS directly; this may corrupt the Operating System.

5.12 Before leaving seat, please ensure that desktop is locked (use Ctrl+Alt+Del or Win+L to lock).

5.13 After an idle time of 10 minutes, desktop shall be automatically switched to "Screen Saver" mode as designed by Helpdesk, IT TEAM and terminal locked.

5.14 Change the password of desktop immediately after being initially assigned the desktop, by the system Administrator.

5.15 Employees are prohibited from installing, removing or editing scripts, which affects system configuration.

5.16 The information on PCs, laptops, tablets and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or by logging-off when it is unattended.

5.17 Information sent by employees from APTRANSCO email address shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of APTRANSCO, unless information is in the course of business duties.

- **Do's and Don'ts of Desktop Policy**

DO'S	DON'TS
• Use Strong Passwords: Create complex passwords for your desktop login and change them regularly. Use a combination of letters, numbers, and special characters.	• Unauthorized Software: Prohibit the installation of unauthorized software on desktops to avoid security risks and potential conflicts with existing software.
• Lock Your Desktop When Not in Use: Always lock your screen when stepping away from your desk to prevent unauthorized access	• Unsecured Networks: Discourage employees from connecting to unsecured or public Wi-Fi networks, which can be vulnerable to attacks.
• Regularly Update Software: Keep your operating system, antivirus software, and other applications up to date to protect against vulnerabilities.	• Sharing Credentials: Advise against sharing login credentials or leaving desktops unlocked and unattended to prevent unauthorized access.
• Follow APTRANSCO Security Policies: Adhere to all APTRANSCO security guidelines, including using encryption for sensitive data and following data backup procedures.	• Ignoring Security Alerts: All employees to promptly respond to security alerts and report any suspicious activity.

6 Backup Policy:

6.1 Take back up of official data regularly in share folder.

6.2 Test these backups periodically.

6.3 Loss of data on Desktop/Laptop computers due to any reason, IT TEAM is not responsible to recover the data.

6.4 Backup media with official information shall not be carried out of office premises. If at all it has to be taken outside the office building, prior intimation / approval from competent authority i.e. concerned HOD's / HOD of IT Wing with the intimation to IT Wing - is mandatory.

6.5 Before handing over the Old Hard Disk to IT TEAM, It may also be ensured by the end user that there is no useful /sensitive data available in Hard Disk and will not be claimed in future. The IT-Coordinator may assist the end user in securely deleting any sensitive data and if required taking the backup (as described at serial no. 1).

- **Do's and Don'ts of Backup Policy**

DO'S	DON'TS
• Regular Backups: Ensure that backups are performed regularly (e.g., daily, weekly) depending on the importance and frequency of data changes.	• Inconsistent Backups: Avoid irregular backup schedules, which can lead to data loss in the event of a system failure or data corruption
• Automated Processes: Implement automated backup processes to minimize the risk of human error and ensure consistency.	• Single Location Storage: Do not store all backups in a single location, as this creates a single point of failure.
• Multiple Backup Locations: Store backups in multiple locations, including off-site or cloud storage, to protect against physical damage or theft.	• Ignoring Alerts: Do not ignore backup failure alerts or error messages. Address issues promptly to ensure data is backed up correctly.
• Retention Policy: Establish a data retention policy that specifies how long backups will be kept before being deleted or overwritten	• Overlooking Critical Data: Do not forget to include all critical data in the backup plan, such as application data, user files, and system configurations.

7 Network

7.1 Personal Laptops / HDDs / Modems are not allowed on LAN without prior approval from competent authority i.e., concern HOD's / HOD of IT Wing

7.2 Patch Cord shall not be detached from the computer.

7.3 Security shall not be compromised and network communication shall not be disrupted.

7.4 APTRANSCO (IT Team) reserves the right to audit networks and systems on a periodic basis to ensure compliance with security policy.

7.5 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of APTRANSCO's network, and as such are subject to the same rules and regulations that apply to APTRANSCO owned equipment, i.e., their machines must be configured to comply with the Security Policies defined by the APTRANSCO.

7.6 To ensure security and avoid the spread of viruses, users should access the Internet through a computer attached to Organization's network only. Bypassing Organization's computer network security by accessing the Internet directly by modem, CDMA, GPRS or other means is strictly prohibited, If this is required for official reasons, then the permission must be sought explicitly from IT Team subject to approval from the concerned HOD's.

7.7 Port scanning or security scanning is expressly prohibited unless authorization from Network administrator is obtained.

7.8 Executing any form of network monitoring without prior intimation to CISO/HOD is prohibited.

7.9 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is not permitted, without permission of system administrator.

- **Do's and Don'ts of Network Policy**

DO'S	DON'TS
• Use Strong Passwords: Ensure all network accounts are protected with strong, unique passwords and change them regularly.	• Unsecured Connections: Avoid connecting to the network via unsecured or public Wi-Fi networks without using a VPN.
• Secure Devices: Keep all devices connected to the network secure by using antivirus software, firewalls, and ensuring they are regularly updated.	• Sharing Credentials: Do not share network login credentials with others or write them down in easily accessible places
• Regular Updates: Apply software patches and updates to all devices and applications connected to the network promptly	• Unauthorized Devices: Do not connect unauthorized or personal devices to the network without proper security measures and authorization.
• Encrypt Data: Use encryption for sensitive data, both in transit and at rest, to protect it from unauthorized access.	• Downloading Unverified Content: Avoid downloading or installing unverified or pirated software, which could introduce malware to the network

8 Information security Acceptable Usage- User Guideline.

8.1 General Use and Ownership

8.1.1 Information security recommends that any IT information that users consider sensitive or vulnerable be password protected.

8.1.2 While APTRANSCO'S network administration desires to provide a reasonable level of privacy, users shall be aware that the data they create on the corporate systems remains the property of APTRANSCO.

8.1.3 IT Information contained on portable computers such as Laptops, are especially vulnerable, special care shall be exercised to prevent unauthorized access to these machines to protect sensitive information. If restricted or confidential data is saved on the laptop after getting requisite approval from HOD of IT Wing

8.1.4 Internet/Intranet/Extranet-related systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

8.1.5 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords should be changed after 90 Days.

8.1.6 All hosts used by the employee that are connected to the 'APTRANSCO's Internet, whether owned by the employee or APTRANSCO', shall be continually executing approved virus-scanning software with a current virus database.

8.1.7 Under no circumstances is an employee of 'APTRANSCO' authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing 'APTRANSCO' owned IT resources.

8.2 Unacceptable Use

8.2.1 Ensure security of Information available on computing assets, with no exceptions:

8.2.2 Exporting any IT related technical information.

8.2.3 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

8.2.4 Revealing your account password to others or allowing use of your account by others.

8.2.5 Using APTRANSCO IT asset to actively engage in procuring or selling any product not pertaining to the corporation.

8.2.6 Making fraudulent offers of products, items, or services originating from any APTRANSCO account.

8.2.7 Effecting security breaches or disruptions of network communication. Security breaches includes, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

- **Do's and Don'ts of Information security Acceptable Usage- User Policy**

DO'S	DON'TS

- Understand the Policy:
  Read and understand the organization's AUP, and seek clarification if needed.
- Use Strong Passwords:
  Create strong, unique passwords for all accounts and change them regularly. Use multi-factor authentication (MFA) where possible.
- Secure Devices:
  Keep all devices secure by using antivirus software, firewalls, and keeping them updated with the latest patches.
- Report Incidents:
  Immediately report any suspected security incidents, breaches, or suspicious activities to the IT department.
- Unauthorized Access:
  Do not attempt to access systems, networks, or data that you are not authorized to use.
- Unapproved Software:
  Do not install or use unauthorized software on organizational devices or networks.
- Neglecting Updates:
  Do not ignore software updates and patches. Keep your devices and software up to date to protect against vulnerabilities.
- Downloading Unauthorized Content: Do not download or install unauthorized software, apps, or files that could contain malware or other security threats.

9 Handling of Sensitive Data

9.1 If and when sensitive information is required to be removed from the PC, before deleting the file, over-write the information with some useless or junk information immediately after the processing is over. Also, the same shall be removed from the recycle bin to prevent its access by restoration by an unauthorized user.

9.2 Maintenance or rectification of faults in the computer system shall be carried out under proper and close supervision of concerned user or IT official to ensure that no data file/program is copied and taken out by the maintenance engineer.

9.3 Unauthorized copying of copyrighted material including, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which APTRANSCO or the end user does not have an active license is strictly prohibited.

9.4 Old hard disk shall not be released even after it is replaced by a new one. Such hard disks shall be handed over to IT TEAM for further disposal.

9.5 The user interface for information contained on Internet/Intranet/Extranet-related systems shall be classified as confidential, internal or public. System administrator shall take all necessary steps to prevent unauthorized access to confidential information.

➢ **Do's and Don'ts of Handling of Sensitive Data Policy**

DO'S	**DON'TS**

- Educate Users:
  Provide regular training and educational materials to users on the importance of handling sensitive data securely and the specific policies and procedures they need to follow.
- Establish Clear Guidelines:
  Clearly outline what constitutes sensitive data within your organization and provide specific examples to help users understand what they need to protect
- Implement Access Controls:
  Limit access to sensitive data to only those employees who need it to perform their job functions. Use role-based access controls to ensure that users only have access to the data necessary for their roles.
- Encrypt Data:
  Require the encryption of sensitive data both in transit and at rest to protect it from unauthorized access or interception.
- Don't Share Credentials:
  Users should never share their login credentials, passwords, or access tokens with anyone else, even within the organization.
- Don't Use Unsecured Networks: Users should avoid accessing or transmitting sensitive data over unsecured or public Wi-Fi networks, as these can be easily intercepted by attackers.
- Don't Ignore Security Warnings: Users should never ignore security warnings or alerts from their systems or applications, as these could indicate a potential security threat or vulnerability.
- Don't Leave Devices Unattended: Users should never leave their devices unattended or unlocked, especially if they contain sensitive data. Locking devices when not in use can help prevent unauthorized access.

10 Data Retention, Storage & Disposal of Media, Records

10.1 Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

10.1.1 Access organizational/sensitive data only in their conduct of organization business and if they have the requisite authorization.

10.1.2 Request only the minimum necessary confidential/sensitive information necessary to perform organization business.

10.1.3 Respect the confidentiality and privacy of individuals whose records they may access.

10.1.4 Observe any ethical restrictions that apply to data to which they have access.

10.1.5 Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

10.1.6 The removable devices, like USB Drive, are to be formatted using low level formatting after its use for transfer of official data.

10.1.7 Data shall be completely erased using low level formatting by IT Team from the removable media, like USB/ External Hard Disk/ Pen Drive, before discarding it. CD/ DVD containing data shall be destroyed before disposal.

10.1.8 Sensitive or confidential documents, if stored on the device, should be encrypted if possible.

➢ **Do's and Don'ts of Data Retention, Storage & Disposal of Media, Records Policy**

DO'S	DON'TS
• Understand Retention Requirements: Educate users about the legal and regulatory requirements for retaining different types of data and records.	• Don't Keep Data Longer Than Necessary: Avoid retaining data longer than necessary for business or legal purposes.
• Secure Storage: Store data securely using encryption and access controls to prevent unauthorized access.	• Don't Store Sensitive Data Indefinitely: Avoid indefinite storage of sensitive data, as this increases the risk of unauthorized access and exposure over time.
• Monitor Storage Usage: Monitor storage usage and regularly review data to identify outdated or unnecessary information.	• Don't Use Insecure Storage Solutions: Avoid using insecure or unapproved storage solutions, such as personal cloud storage accounts or external hard drives, to store sensitive data.
• Dispose of Data Securely: When disposing of data or storage media, ensure it is securely erased or destroyed to prevent data recovery by unauthorized parties.	• Don't Forget About Physical Records: Ensure that physical records containing sensitive information are stored securely and disposed of properly when no longer needed.

11 Mobile Computing and Communication Policy

11.1 Do not discuss confidential issues on cell phone.

11.2 Do not open confidential documents in public.

11.3 Do not sit in a position which allows others to peek onto your display.

11.4 Always carry your device well secured and do not leave it unattended.

11.5 Carrying confidential data on portable device is not allowed without approval. If approval has been obtained from CISO for storage of restricted/confidential information, the said data must be protected by encryption.

11.6 Keep all connectivity options like Infrared, Bluetooth and Wireless switched off when not in use. Use invisible mode where possible.

11.7 All mobile devices must be password protected. Choose and implement a strong password – please refer to the Password Policy.

11.8 The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible.

11.9 If a mobile device is lost or stolen, promptly report the incident to the IT Team and Security Wing.

11.10 Sensitive or confidential documents, if stored on the device, should be encrypted if possible.

11.11 Sensitive and confidential information should be removed from the mobile device before it is returned, exchanged or disposed. Whenever possible all mobile devices should enable screen locking and screen timeout functions

11.12 Mobile devices when connected to Office LAN should be in separate VLAN with access to only whitelisted applications

11.13 Just as with static devices (e.g., desktop computers), user remain responsible to ensure that the information is backed-up and available as and when required.

11.14 Work from home users should not divulge and keep safe all the confidential information related to APTRANSCO from family members and outsiders.

- **Do's and Don'ts of Mobile Computing and Communication Policy**

DO'S	DON'TS
• Device Security: Enable device encryption to protect data stored on mobile devices.	• Unauthorized Device Usage: Do not use unauthorized or jail broken/rooted devices for work-related activities.
• App Permissions: Review and carefully consider the permissions requested by mobile apps before granting access to sensitive data or device features	• Insecure Data Sharing: Avoid sharing sensitive information, such as passwords or corporate data, through insecure channels like unencrypted emails or messaging apps
• Safe Browsing Practices: Exercise caution when accessing websites or clicking on links from emails or messages to avoid phishing attacks or malicious websites.	• Unsecured Networks: Avoid connecting to unsecured or unknown Wi-Fi networks, as they may be compromised or used for malicious purposes, putting sensitive data at risk.

12 Remote Access Policy

12.1 At no time shall any APTRANSCO employee provide their login or email password to anyone, not even to family members.

12.2 Organizations or individuals who wish to implement non-standard Remote Access solutions to the APTRANSCO production network shall obtain prior approval from Remote Access Services of APTRANSCO.

12.3 While using APTRANSCO owned computer to remotely connect to APTRANSCO's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

12.4 All hosts that are connected to APTRANSCO's internal networks via remote access technologies, must use the most up-to-date anti-virus software; this will include personal computers too.

- **Do's and Don'ts of Remote Access Policy**

DO'S	DON'TS
• Regular Updates and Patching: Keep operating systems, software applications, and security patches up-to-date on remote devices to address vulnerabilities and protect against malware and other security threats.	• Unsecured Public Networks: Avoid connecting to unsecured public Wi-Fi networks or using untrusted network connections for remote access, as they may expose sensitive data to interception or unauthorized access by attackers.
• Access Controls: Implement access controls and permissions to restrict remote access to authorized users only, based on their roles and responsibilities within the organization.	• Sharing Credentials: Do not share remote access credentials, such as usernames and passwords, with unauthorized individuals or use default or weak passwords that are easily guessable.
• Logging and Monitoring: Log remote access activities and monitor for suspicious or unauthorized access attempts to detect and respond to security incidents promptly.	• Ignoring Security Warnings: Take security warnings and alerts seriously and do not ignore them, as they may indicate potential security threats or vulnerabilities that need to be addressed promptly.
• Multi-Factor Authentication (MFA): Require multi-factor authentication (MFA) for remote access to add an extra layer of security beyond passwords, such as one-time passcodes or biometric authentication.	• Unapproved Software: Do not install unauthorized or unapproved software applications on remote devices used for accessing corporate networks or sensitive information, as they may introduce security risks or conflicts with existing security controls.

----- END ----