



**TRANSMISSION CORPORATION OF NDHRAPRADESH LIMITED**

## **Backup and Restoration Policy**

## Confidentiality Statement

This Backup and restoration policy document is strictly private, confidential and it is only for use by the Internal. This document shall not be used, disclosed, copied, published, distributed or reproduced in whole or in part without the prior written consent of APTRANSCO.

## Document Control

Version	Date	Reviewed by	Approve by	Change Description
V1.0	10-09 -2024	CE/Telecom & IT/VS/Vijayawada		Initial Release

## Distribution

- Intranet Portal
- Email

**TABLE OF CONTENTS**

<b>1. Introduction</b>	<b>4</b>
<b>2. Intended Audience</b> .....	<b>4</b>
<b>3. Inputs</b> .....	<b>4</b>
<b>4. Roles and Responsibilities</b> .....	<b>5</b>
<b>5. Procedure Overview</b> .....	<b>5</b>
<b>6. Operational Requirement</b> .....	<b>6</b>
6.1 Data Back up .....	6
6.2 Backup Monitoring.....	6
6.3 Backup Log.....	7
<b>7. Backup Restoration &amp; Testing</b> .....	<b>7</b>
7.1 Recovery .....	8
7.2 Recovery clasification's .....	8
7.3 Restore request & Backup request.....	8
7.4 Testing Procedures .....	8

## 1. Introduction

Backup and recovery is the process of duplicating APTRANSCO Data (online & off line) and storing it in a secure place in case of data loss or damage and the same can be again used in Organisation operations.

There is a massive growth in the volume of data due to usage of Internet, email, and application software. Data is increasingly being recognized as one of the real assets of any organization and losing of data would cause severe damage to organization. Critical data loss will have a severe financial impact on any organization. Hence, data backup is considered a core business continuity/ security control, rather than just an operational procedure.

### **Purpose**

The purpose of a backup is to protect the organization against data loss and reconstruction of database in case of data corruption due to accidental data loss, data base corruption, Hardware failure and even natural disasters. This document provides a general outline and guide for ensuring adequate back-ups, restoration, and storage of digital data.

### **Scope**

This procedure pertains solely to digital electronic data stored on the Servers or Network enabled devices of APTRANSCO Power Station.

## 2. Intended Audience

This process is addressed to every person entrusted to access APTRANSCO premises and IT infrastructure and resources including, APTRANSCO employees, contractors, consultants, trainees, vendors, sub-contractors, visitors, and client representatives and out-sourced employees.

This process assumes that the reader has general knowledge about available IT infrastructure and is familiar with common computer terminology. It is assumed that the reader has enough knowledge to access and use the programs and tools discussed.

## 3. Inputs

This procedure applies to taking backup and recovery of the following:

- Domain Servers
- Data Server

#### 4. Roles and Responsibilities

Role	Responsibilities
HOD of IT Wing	<ul style="list-style-type: none"> <li>• Define and Implement the Data Backup process for Domain &amp; Data base Servers</li> </ul>
IT Application Division for Domain & Data base Servers	<ul style="list-style-type: none"> <li>• Setting up a backup schedule</li> <li>• Monitoring the backup environment</li> <li>• Troubleshooting backup problems</li> <li>• Taking appropriate corrective action if backup fails</li> <li>• Plan restoration testing on random samples of backup and maintain records of the test results.</li> <li>• Regular review of backup process and subject systems / data</li> <li>• Backup and recovery</li> <li>• Maintain record of Backup taken.</li> </ul>
IT Infra Division for Fire wall, Routers , Switches and other related devices etc.	<ul style="list-style-type: none"> <li>• Setting up a backup schedule</li> <li>• Monitoring the backup environment</li> <li>• Troubleshooting backup problems</li> <li>• Taking appropriate corrective action if backup fails</li> <li>• Plan restoration testing on random samples of backup and maintain records of the test results.</li> <li>• Regular review of backup process and subject systems / data</li> <li>• Backup and recovery</li> <li>• Maintain record of Backup taken.</li> </ul>

#### 5. Procedure Overview

The data backup is taken wherein the data is residing on servers, networks or similar devices. The type of backup varies with the application and volume of data to be backed up.

The backup software is used to control the backup processes as per requirements. Logs are maintained to verify the amount of data backed up and the unsuccessful backup occurrences. The Backups are taken on regular basis and the frequency of the backup taken is different for data residing on different servers.

The backup schedule is summarized as below:

<b>Frequenc y</b>	<b>Backup Mode</b>	<b>Server/Data</b>	<b>Recording Method</b>	<b>Time</b>
Daily	Offline/Online	Individual Applications	External HDD/ Share folder	End of the day
Daily	Offline/Online	Data Server	External HDD/ Share folder	Weekend
Weekly / Quarterly	Offline/Online	Domain Server	External HDD/Share folder	Weekend

## 6.0 Operational Requirement

### 6.1 Data Back up

- i. A database backup records the complete state of the data in the Database at the time the backup operation completes.
- ii. A transaction log backup records the state of the transaction log at the time the backup operation starts.
- iii. Depending upon the requirements, one of the following ways to back up the database should be selected:
  - a) **Complete database backups:** Perform a full backup of the database, objects, system tables, and data.
  - b) **Differential backups:** Back up data that has changed since the last complete backup.
  - c) **Transaction log backups:** Back up all database modifications transaction logs.
  - d) **File and file group backups:** Back up database files and file groups rather than the entire database.

### 6.2 Backup Monitoring

IT Apps Division keeps monitoring the data backup operations and resolve all contentions. Every Backup failure is recorded, and analysis is performed on it with cause effect analysis.

### 6.3 Backup Log

Pertinent information related to back-ups is recorded in the backup log. In the event of a failure, is to be notified the failure to ensure comprehensive disaster recovery measures.

## 7. Backup Restoration & Testing

### 7.1 Recovery

A backup is only as good as the recovery it can provide. This may experience One or more of the following database integrity problems and will be required to Recover the lost data.

Invalid Data	This is the smallest, but most common database problem. It occurs when a finite number of invalid entries find their way into the data.
Corrupted Database Object	The next level of database problems includes situations in which a single or limited number of database objects have become corrupted or invalid.
Full Database Corruption	At this level, the scope of the problem is so significant that the database is no longer operational and a full database recovery must be performed.
Multiple Database Corruption	The largest levels of database problems occur when multiple databases within the enterprise have been corrupted and must be recovered as a set.

### 7.2 Recovery classification's:

Transaction Recovery	Transaction recovery, also known as data-level recovery, allows DBAs( Data base administrator) to precisely identify and correct the invalid data. The DBA should select and examine each of the changes that were applied to the database by using selection and filtering capabilities
Database Object Recovery	Database object recovery allows DBAs to identify and recover only the missing or damaged objects. DBA should use tools available for Object recovery contain built-in database intelligence to identify all of the objects making up the database from information captured when the backup was taken. This information

	can be then matched against the existing database environment. Missing or invalid objects can then be automatically recovered from the physical backup of the database, while valid objects remain unaffected.
Full Database Recovery	The DBA may need to recover entire database. This requires the database to be closed. During this time, users will not be able to access important business critical applications.
Multiple Database Recovery	The DBA should select tools that combine an enterprise-wide view of the organization with maximum database recovery capabilities. This enterprise-wide recovery management console allows consistent, reliable backup and recovery plans to be established and automated

### 7.3 Restore Request & Backup Request

Restoration is done on a request basis to recover lost or deleted data as per retention period specified. Requests to restore file must be authorized by HOD IT Wing. Restore request can be from either backup or archive media. The request contains the following information to retrieve the data.

- IP:
- File or Directory Name:
- Date file(s) were last modified, if available:
- If existing file(s) can be overwritten or not?
- Priority

### 7.4 Testing Procedures

**The request contains at least the following information to retrieve the data.**

- File or Directory Name:
- Date file(s) were last modified, if available:
- If existing file(s) can be overwritten or not?
- Quality of Backup:

#### ➤ Output

- Successful backup and restoration of data completed.
- Backup and restoration record is updated and maintained.