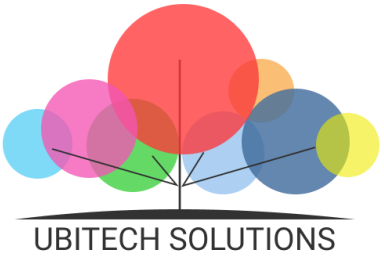


# Ubitech

## Backup & Restore Policy

**Version 1.0**

## PURPOSE

This policy aims to define the rules for taking data backups and testing the restoration.

## SCOPE

The policy covers backups of all types of data and information within the Ubitech Solutions Pvt. Ltd. (herein referred to as Organization).

## DEFINITION

Following is an explanation of various terms used within this document :

- Backup: A copy of file, data, or information made in case the original is lost or damaged.
- Backup Server: A backup server enables the backup of data, files, applications, and/or databases on a specialized in-house or remote server. It combines hardware and software technologies that provide backup storage and retrieval services to connected computers, servers, or related devices.
- Incremental Backup: An incremental backup is one in which successive copies of the data contain only the portion that has changed since the previous backup copy was made.
- Differential Backup: A data backup method that copies all files that have changed since the performance of the last full backup.
- Recovery Test: A backup recovery test ensures that the backup and recovery plan will work after a real emergency.

## RESPONSIBILITIES

The primary ownership of implementing this policy is with the IT and DevOps Team and the ISG.

## POLICY

1. All backups shall be executed automatically, based on frequency and timing, when they will have minimal impact on the systems being backed up.
2. All backups shall be available at two different systems in two locations if one is unavailable when data recovery is needed.

3. All backup data shall be encrypted where required by legislation, regulation, or customer requirements/ contractual obligations.
4. Cloud Implementation
    a. All backup copies of data shall reside at a different physical location (Region/Zone) than the source data.
    b. All backup copies of data shall reside on redundant media at the alternate location.

## Data Backups and Frequency

1. Data in all the in-scope systems should be backed up regularly as per the defined frequency, at least within 24 24-hour

## Backup Restorations Testing

1. Records of restoration testing shall be maintained at least once a year.
2. In case of any error or failure while restoration testing, the incident management process should be followed.

## Backup Monitoring

1. All systems servicing a backup function will be monitored regularly, at least quarterly, to ensure successful backup operations.
2. Dashboards should readily provide the status of backup operations, allowing the appropriate IT personnel to manage the backup system proactively.
3. IT teams shall monitor the success/failure of the scheduled backup jobs and take corrective actions in case a backup fails.

# Version Details

| Version | Version Date | Description of changes | Created By | Approved By | Published By |
|---|---|---|---|---|---|
| Version 1.0 | Aug 26 2025 | Initial Release | Aditya Goyal | Parth Bhansali | Aditya Goyal |