[COMPANY NAME]
[Add your company logo / letterhead and registered address here]

Backup Policy

HOW TO USE THIS TEMPLATE
This template is mostly complete and pre-filled with standard Indian practice. You should not have to fill many blanks.
Text in blue is a default that companies commonly change. Skim the blue text and edit only what differs for you.
Add your company name and letterhead once, in the header above. The body refers to "the Company".
Tune the frequency, retention and RTO/RPO values per system tier; mission-critical systems usually need shorter RPOs than the defaults below.
Have it reviewed by a qualified HR or legal professional before you adopt it, and delete this box.
Provided by CFOmatrix (cfomatrix.in). General template, not legal advice.

Policy owner	**[Human Resources / IT / Compliance]**
Effective date	**[DD MMM YYYY]**
Version	1.0
Approved by	**[Name, Title]**

1. Purpose

This Policy establishes the requirements for backing up the Company's data, systems and applications so that information can be reliably restored after accidental deletion, corruption, hardware failure, ransomware, cyber incidents or disasters. It defines what is backed up, how often, how long copies are retained, where they are stored, how they are protected, and how restores are tested.

The Policy supports the Company's obligations to safeguard data, including personal data processed under the Digital Personal Data Protection Act, 2023 (DPDP Act), and aligns backup controls with recognised security frameworks such as SOC 2 and ISO/IEC 27001 (Annex A controls for information backup and business continuity).

2. Scope

This Policy applies to:

- All Company data classified as Confidential, Restricted or Internal, in any format (databases, files, application data, email, source code, configuration).
- All Company-owned or operated systems, servers, endpoints, virtual machines, containers, SaaS applications and cloud workloads.
- All employees, contractors, consultants and third-party service providers (including managed service providers and processors) who create, manage or operate Company data and systems.
- On-premises infrastructure, co-located infrastructure and cloud infrastructure (**AWS / Azure / GCP**).

Personal devices used under any Bring Your Own Device arrangement are out of scope for centralised backup; users must store Company data only in approved, backed-up systems.

3. Definitions

- Backup: A copy of data taken at a point in time that can be used to restore the original after loss or corruption.
- Full Backup: A complete copy of the entire dataset or system.
- Incremental Backup: A copy of only the data that changed since the last backup of any type.
- Differential Backup: A copy of all data that changed since the last full backup.
- RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time (how far back the last good backup must be).
- RTO (Recovery Time Objective): The maximum acceptable time to restore a system to service after a failure.
- Offsite Copy: A backup copy held in a physically or logically separate location from the primary data.
- 3-2-1 Rule: Keep at least 3 copies of data, on 2 different media types, with 1 copy offsite.

4. Backup Strategy and Data Classification

The Company follows the 3-2-1-1 backup principle: at least three copies of data, on two different media or platforms, with at least one copy offsite, and at least one copy immutable or air-gapped to protect against ransomware.

Backup requirements are tiered by system criticality. Each system must be assigned a tier by the system owner.

Tier	System Type	Backup Frequency	RPO	RTO
Tier 1 (Mission critical)	Production databases, core applications, payments, identity	**Continuous / hourly**	**1 hour**	**4 hours**
Tier 2 (Business critical)	Internal apps, shared file stores, email, code repositories	**Daily**	**24 hours**	**24 hours**
Tier 3 (Standard)	Departmental files, endpoints, dev/test environments	**Weekly**	**1 week**	**3 business days**

5. Backup Frequency and Schedule

Unless a system's tier in Section 4 requires otherwise, the standard backup schedule is:

- Incremental backups: **daily**, typically run during the off-peak window of **01:00 to 05:00 IST**.

- Full backups: **weekly**, typically on **Sunday**.
- Monthly archival backup: **the first full backup of each calendar month** is retained as a monthly archive.
- Database transaction log backups (Tier 1): every **15 minutes** to support point-in-time recovery.
- SaaS application data (for example email, CRM, ticketing): backed up **daily** via the provider's export or a third-party SaaS backup tool, because provider native retention is not a substitute for the Company's own backup.

Backup jobs must complete within their defined window. Jobs that overrun, fail or are skipped must be flagged for review the next business day.

6. Retention

Backups are retained only as long as needed for recovery, legal, regulatory and contractual reasons, consistent with the data minimisation and storage limitation principles of the DPDP Act.

Backup Type	Retention Period	Notes
Daily incremental	**30 days**	rolling
Weekly full	**12 weeks**	rolling
Monthly archive	**12 months**	first full backup of the month
Annual / year-end archive	**7 years**	where required for tax, audit or statutory records
Database transaction logs	**14 days**	point-in-time recovery window

Where backups contain personal data, retention must not exceed the retention period defined for that data in the Company's Data Retention and Data Protection policies. When a record reaches end of retention, backups containing it are rotated out and overwritten or securely destroyed. Backups under a legal hold must not be deleted until the hold is lifted, even if the standard retention has expired.

7. Offsite and Cloud Copies

- At least one backup copy must be stored offsite from the primary data location, in a geographically separate region or availability zone.
- Cloud backups must use a separate account, subscription or storage bucket from production, with independent access controls, so that a compromise of production credentials does not also destroy the backups.
- At least one copy must be immutable (for example object lock / write-once-read-many) or air-gapped, retained for at least **30 days**, to defend against ransomware and malicious deletion.
- For data subject to localisation or contractual residency requirements, offsite and cloud copies must remain within **India** unless a documented exception is approved.

- Physical backup media (tapes or drives), where used, must be transported and stored securely in a locked, access-controlled, environmentally suitable location.

8. Encryption and Security

- All backups must be encrypted in transit using TLS **1.2 or higher**.
- All backups must be encrypted at rest using **AES-256**.
- Encryption keys must be managed in an approved key management service, stored separately from the backup data, and rotated at least **annually**. Loss of keys means loss of the backups, so key custody and recovery must be documented.
- Access to backup systems, storage and restore functions is restricted on a least-privilege, need-to-know basis and protected by multi-factor authentication.
- All access to and actions on backups (creation, restore, deletion, configuration change) must be logged, and logs retained for at least **1 year**.
- Backup credentials and service accounts must not be shared and must be rotated when an administrator with access leaves the Company.

9. Restore Testing and Validation

Backups are only useful if they restore. The Company therefore validates backups on two levels:

- Automated verification: every backup job is checked for completion, integrity (checksums) and that the data is readable, with failures alerted automatically.
- Restore testing: a sample restore is performed at least **quarterly** for Tier 1 and Tier 2 systems, and at least **annually** for Tier 3, to confirm that data can actually be recovered within the defined RTO and RPO.

A full disaster recovery restore exercise covering critical systems is conducted at least **once a year**. Each restore test must be documented with the date, system tested, backup used, restore time achieved versus RTO target, data loss versus RPO target, issues found and corrective actions. Failed restore tests are treated as incidents and remediated promptly.

10. Roles and Responsibilities

Role	Responsibility
IT / Infrastructure Manager	Owns this Policy, the backup architecture, schedules and overall compliance
Backup Administrator	Configures, runs and monitors backup jobs; investigates failures; performs restore tests
System / Data Owners	Classify systems into tiers, define RTO/RPO, confirm what must be backed up
Information Security / CISO	Sets encryption, access and immutability standards; reviews logs; handles backup-related incidents
Data Protection Officer / **privacy@company.com**	Ensures backup retention and handling comply with the DPDP Act

Employees and contractors	Store Company data only in approved, backed-up systems; report data loss promptly

11. Monitoring, Reporting and Alerting

- Backup job status is monitored daily through the backup tool's dashboard and automated alerts.
- Failed, missed or partial backups generate an alert to the **Backup Administrator** and must be resolved or escalated within **1 business day**.
- A backup health report (success rate, storage usage, failures, restore test results) is reviewed **monthly** by IT management. The target backup success rate is at least **99** percent.
- Storage capacity is monitored, and growth is forecast so backups never fail for lack of space.

12. Incident Response and Breach Notification

If a backup is lost, corrupted, exposed or destroyed, or if a restore fails when needed, the event is treated as a security incident and handled under the Company's Incident Response Policy.

- Cyber incidents falling within the CERT-In Directions, 2022 (for example unauthorised access, ransomware, data breach) must be reported to CERT-In within 6 hours of detection.
- Where a backup containing personal data is breached, the Company will notify the Data Protection Board of India and affected data principals as required under the DPDP Act, without undue delay.
- Backups are a primary recovery tool against ransomware: immutable and air-gapped copies must be verified clean before any restore into production.

13. Exceptions

Any deviation from this Policy (for example shorter retention, no offsite copy, unencrypted legacy system) must be documented, risk-assessed, approved in writing by the **IT Manager** and **CISO**, assigned an owner and an expiry date, and reviewed at each Policy review.

14. Enforcement

Compliance with this Policy is mandatory. Failure to comply, including disabling backups, bypassing encryption or neglecting restore testing, may result in disciplinary action up to and including termination, and where applicable, legal action. Third parties who fail to comply may have their contracts reviewed or terminated.

15. Review and Governance

This Policy is owned by the **IT / Infrastructure Manager** and approved by **Management / the Board**. It is reviewed at least **annually**, or sooner following a major incident, a significant change

in infrastructure, or a change in law. The effective date of this version is **DD-MM-YYYY** and the next scheduled review is **DD-MM-YYYY**.