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

Data Retention and Deletion 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".
Fill the retention table with the periods your business and statutory obligations require, then assign an owner to each data category before circulating this policy.
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

The Company collects, generates and stores large volumes of data across its operations: employee records, financial and tax records, customer and vendor information, system and security logs, and product or service data. Holding data for longer than necessary increases legal exposure, storage cost and breach impact, while deleting data too early can breach statutory record-keeping duties or destroy evidence.

This Policy establishes how long each category of data is retained, when and how it is securely deleted, how legal holds suspend deletion, and who is accountable for each step. It is designed to keep the Company compliant with the Digital Personal Data Protection Act, 2023 (DPDP Act), the Companies Act, 2013, the Income Tax Act, 1961, the Goods and Services Tax laws, labour and employment statutes, and the CERT-In Directions, 2022, while supporting the Company's information security objectives mapped to SOC 2 and ISO 27001 controls.

2. Scope

This Policy applies to:

- All data in any format (electronic, paper, audio, video) created, received, processed or stored by or on behalf of the Company.
- All employees, contractors, consultants, interns, and third-party processors who handle Company data.
- All systems and locations where data resides: production databases, file servers, SaaS applications, email, endpoints, mobile devices, removable media, physical files, and cloud or on-premise backups.

This Policy covers both personal data (as defined under the DPDP Act) and non-personal business records. Where a contract, statute, or regulator mandates a longer or shorter period than stated here, that requirement prevails and the difference must be recorded by the **Data Protection Officer**.

3. Definitions

- Personal Data: any data about an individual who is identifiable by or in relation to such data (a Data Principal under the DPDP Act).
- Retention Period: the maximum period for which a data category is kept active before deletion or archival.
- Archival: moving data out of active systems into a restricted, lower-access store for the remainder of its retention period.
- Secure Deletion: rendering data permanently unrecoverable using approved methods (see Section 8).
- Legal Hold: a directive to suspend deletion of specified data because it is relevant to actual or anticipated litigation, investigation, audit, or regulatory proceeding.
- Data Owner: the function head accountable for a category of data and its retention.
- Processor: a third party that processes personal data on behalf of the Company under contract.

4. Guiding Principles

- Purpose limitation: data is retained only for the purpose for which it was collected, or as required by law.
- Storage limitation: under the DPDP Act, personal data must be erased once the specified purpose is no longer served and retention is not required by law. Default to the shortest defensible period.
- Documented schedule: every data category has a defined retention period (Section 7); ad hoc indefinite retention is not permitted.
- Defensible deletion: deletion follows a documented, repeatable process and is logged.
- Security by design: retention and deletion controls map to SOC 2 / ISO 27001 controls and are reviewed annually.
- Legal hold overrides everything: data under hold is never deleted until the hold is released, regardless of schedule.

5. Roles and Responsibilities

Role	Responsibility
Data Protection Officer / DPO	Owns this Policy, maintains the retention schedule, approves exceptions, oversees DPDP compliance
Head of IT / Information Security	Implements deletion tooling, manages backups, certifies secure destruction of media and systems

Data Owners (function heads: **HR, Finance, Sales, Engineering**)	Classify their data, confirm retention periods, trigger deletion or archival on schedule
Legal / Company Secretary	Issues and releases legal holds, advises on statutory retention, manages regulator interactions
Employees and contractors	Follow this Policy, do not retain copies outside approved systems, report data they no longer need
Processors / vendors	Delete or return Company data per contract on termination and per documented retention terms

6. Data Classification

To apply the right retention period, data is classified by category and sensitivity. Each Data Owner classifies their data into the categories in Section 7 and tags sensitive personal data (financial, health, biometric, government identifiers) for stricter handling. Classification is reviewed at least **annually** and whenever a new system or data flow is introduced.

7. Retention Schedule

Retention periods below combine statutory minimums with the Company's standard practice. Periods marked editable are defaults the Company may extend or shorten within legal limits. The clock starts on the trigger event noted (for example, end of financial year, or employee exit), after which data is deleted or moved to restricted archival.

7.1 HR and Employee Data

Data Type	Retention Period	Trigger / Notes
Recruitment records of unsuccessful candidates	**6 months** from decision	Delete unless consent taken to retain for future roles
Employee personnel file (contracts, appraisals)	**5 years** after exit	Supports limitation period for employment claims
Payroll and salary records	**8 years** after the relevant year	Aligns with statutory wage and tax records
PF, ESI, gratuity and nomination records	**Permanently / 8 years** after exit	Gratuity nomination and PF records support lifetime claims
Attendance and leave records	**3 years**	Per State Shops and Establishments Act practice
POSH complaint and inquiry records	**5 years** after closure	Confidential; access restricted to Internal Committee
Disciplinary and grievance records	**5 years** after closure	Retain longer if litigation likely
Background verification reports	**2 years** after exit	Sensitive personal data, restrict access

7.2 Finance, Tax and Statutory Data

Data Type	Retention Period	Trigger / Notes
Books of account and financial statements	8 years	Companies Act, 2013 requires minimum 8 financial years
Income tax records and returns	6 to 8 years	Income Tax Act; up to 10 years where reassessment for undisclosed foreign income applies
GST records, invoices and returns	6 years	From the due date of the annual return for the year
TDS / TCS records	**8 years**	Align with income tax record practice
Statutory registers, board and general meeting minutes	Permanently	Companies Act, 2013 (permanent records)
Bank statements and reconciliations	**8 years**	Match books of account
Vendor and procurement contracts	**Contract term plus 7 years**	Supports limitation period under the Limitation Act, 1963
Expense claims and supporting documents	**8 years**	Match tax records

7.3 Customer, Vendor and Marketing Data

Data Type	Retention Period	Trigger / Notes
Active customer account and KYC data	Duration of relationship plus **8 years**	Tax and contractual evidence
Inactive / closed customer accounts	**3 years** after last activity	Then delete personal data unless statute requires longer
Customer support tickets and chat transcripts	**3 years**	May contain personal data; minimise
Marketing consent and preference records	**3 years** after consent withdrawal	Retain proof of consent under DPDP Act
Marketing prospect / lead data	**2 years** from last engagement	Delete if no consent or interaction
Vendor master and payment data	**8 years** after relationship ends	Tax and audit evidence

7.4 IT, Security and System Logs

Data Type	Retention Period	Trigger / Notes
Application and access logs	**1 year**	Supports investigations and audit
Security and SIEM logs	**180 days hot, 1 year cold**	Meet SOC 2 / ISO 27001 monitoring needs
CERT-In mandated logs (ICT system logs)	180 days	CERT-In Directions, 2022 require logs enabled and maintained for 180 days within India
Email and collaboration data	**3 years**	Subject to legal hold
CCTV footage	**30 to 90 days**	Longer only if incident under review

System backups	**35 days** rolling	See Section 9
Audit trail of deletions and holds	**3 years**	Evidence of compliance

8. Secure Deletion Methods

When a retention period expires (and no legal hold applies), data is deleted using a method appropriate to the medium. The objective is permanent, irreversible destruction.

- Electronic data in databases and applications: hard delete (not soft delete / flag), then purge from indexes, caches and exports. Where systems only soft-delete, schedule periodic purge jobs.
- Files and storage: cryptographic erasure (destroy the encryption keys) or multi-pass overwrite of the storage area.
- Cloud storage / SaaS: use the provider's permanent delete function and confirm removal from versioning and recycle bins; obtain a deletion attestation where contractually available.
- Endpoints and removable media: full-disk wipe to a recognised standard (for example NIST SP 800-88 purge) before reuse; physically destroy (shred / degauss) media that is end-of-life or faulty.
- Paper records: cross-cut shredding or secure destruction by an approved vendor with a destruction certificate.
- Mobile devices: remote wipe and factory reset before redeployment or disposal.

Every destruction of a system, drive or batch of records must be logged in the **deletion register** with date, data category, method, and the person who certified it. Media destruction by vendors requires a certificate of destruction retained for **3 years**.

9. Backups and Deletion

Backups create a tension with deletion: data deleted from production may still exist in backups. The Company manages this as follows:

- Backups are retained on a rolling cycle of **35 days**; older backups are overwritten or expired automatically.
- When personal data is deleted from production (including on a Data Principal erasure request), it is not separately purged from each backup. Instead, the data remains only within the backup retention window and is permanently overwritten as that window passes. Restored backups must be re-processed to re-apply pending deletions before the restored data is used.
- Disaster-recovery and archival backups intended for long-term retention follow the relevant retention period in Section 7, not the rolling cycle.
- Backup media is encrypted at rest, access-controlled, and stored **within India** where data localisation or sectoral rules require it.

- The **Head of IT** documents the backup-to-deletion reconciliation process and tests it at least **annually**.

10. Legal Hold

A legal hold suspends the routine deletion of specified data when it is relevant to actual or reasonably anticipated litigation, regulatory investigation, audit, government request, or internal inquiry.

- Only **Legal / Company Secretary** may issue or release a legal hold, in writing.
- A hold notice identifies the custodians, the data categories and systems affected, and the matter. It overrides any scheduled deletion for that data.
- On receiving a hold, custodians and the **Head of IT** must immediately stop deletion (including disabling auto-purge and extending backups) for the in-scope data and preserve it intact.
- Holds are tracked in a **legal hold register** with issue date, scope, and status.
- When the matter closes, **Legal** releases the hold in writing, after which normal retention and deletion resume. Data already past its retention period at release is queued for prompt deletion.

11. Data Principal Rights and Erasure Requests

Under the DPDP Act, a Data Principal may request correction or erasure of their personal data. On a verified request:

- The **DPO** acknowledges the request and verifies identity within **7 days**.
- Personal data is erased unless retention is required by law (for example, tax or statutory records) or for an ongoing legal hold; in that case the Company retains only the legally required minimum and informs the Data Principal of the basis.
- Erasure is completed within **30 days** of a valid request, and the data ages out of backups per Section 9.
- The action is logged in the **deletion register**.

Requests are submitted to **privacy@company.com** or the grievance contact published in the Company's privacy notice.

12. Processors and Third Parties

Where a processor or vendor stores Company data:

- The contract must specify retention periods, secure deletion obligations, and a duty to delete or return all Company data on termination.
- Processors must confirm deletion in writing (deletion attestation) within **30 days** of contract end or on instruction.

- The Company maintains an inventory of processors, the data they hold, and their retention terms, reviewed at least **annually**.

13. Breach and Incident Considerations

Retention reduces breach exposure, but incidents still occur. Note the reporting timelines that interact with this Policy:

- Cyber incidents falling within the CERT-In Directions, 2022 must be reported to CERT-In within 6 hours of becoming aware.
- A personal data breach under the DPDP Act must be notified to the Data Protection Board of India and to affected Data Principals (the DPDP Rules detailing form and timeline are being finalised and this Policy will be updated when they take effect).
- Logs and records relevant to an incident are placed under legal hold and are not deleted while the incident or any consequent proceeding is open.

14. Non-Compliance and Enforcement

Failure to follow this Policy, including unauthorised retention, premature deletion, or deletion of data under legal hold, may result in disciplinary action up to and including termination, and may expose individuals and the Company to liability under the DPDP Act, the Companies Act, and other laws. Deleting data to obstruct an investigation or proceeding is treated as serious misconduct. Vendors that breach their deletion obligations may face contract termination and recovery of resulting losses.

15. Review and Governance

This Policy is owned by the **Data Protection Officer** and reviewed at least **annually**, and sooner when the DPDP Rules are notified, when statutory retention periods change, or after a significant incident or audit finding. The retention schedule in Section 7 is validated by each Data Owner during the review. Changes are approved by **the Management / Board** and communicated to all staff. Records of reviews and approvals are retained for **3 years**.

This Policy is effective from **DD/MM/YYYY** and supersedes any prior data retention practice.