

Data Retention and Disposal Policy

Purpose

Holding data longer than it is needed increases risk: more information to secure, more to search in litigation, more to disclose in a breach. Holding data for less time than is required breaches law, regulation, or contract. This policy establishes Your Organization's retention schedules by data type, and the secure disposal requirements that apply when retention ends.

Scope

This policy applies to all Your Organization data — electronic and physical — regardless of where it is stored (primary systems, backups, archives, endpoint copies, email, collaboration tools, paper files, removable media). It applies to every workforce member, contractor, and third party that handles Your Organization data.

Principles

- **Retain only as long as necessary.** Retention matches the legitimate business, legal, regulatory, and contractual need — no longer.
- **Dispose of data securely.** When retention ends, data is deleted, destroyed, or anonymized so it cannot be reconstructed.
- **Suspend deletion under legal hold.** When a legal hold is in place, deletion pauses for the data in scope until the hold is released, regardless of the normal schedule.
- **Same schedule across copies.** The retention clock applies to all copies of a given record — primary, replicas, and backups — as far as reasonably practical.

Retention schedule

The schedule below is a default; specific regulations (GDPR, HIPAA, SOX, industry-specific rules) or customer contracts may require longer or shorter retention, in which case the stricter obligation governs.

Data type	Default retention	Authoritative obligation
Customer account records	7 years after account closure	Contract, tax
Customer content (tenant-scoped)	Per customer contract; default 30 days after account closure	Contract
Payment card data (PCI DSS)	Only as long as required for authorization and settlement; never store CVV post-auth	PCI DSS
Protected Health Information (PHI)	6 years minimum (HIPAA) or longer where state law requires	HIPAA

Data type	Default retention	Authoritative obligation
Personal data of EU residents	Until the purpose for processing ends, or earlier on valid erasure request	GDPR
Employee records	7 years after termination	HR, tax, employment law
Financial records (general ledger, invoices, tax)	7 years	Tax, SOX
Security logs (authentication, access, DLP)	1 year online; 2 years archived	SOC 2, incident support
Application logs (non-security)	90 days online; 1 year archived	Operational
Backups	90 days rolling; longer for legal-hold scope	Operational
Email and chat	3 years; legal-hold overrides	Contract, litigation support
Incident records	7 years after closure	Audit, litigation support
Vendor contracts and assessments	Term + 7 years	Audit, litigation support
Marketing and sales leads	2 years from last contact; earlier on opt-out	Privacy

Legal hold

When litigation, regulatory inquiry, or internal investigation is reasonably anticipated, Legal issues a written legal-hold notice identifying the custodians and the data in scope. Receiving a hold notice suspends the retention schedule for the identified data. Deletion may not resume until Legal issues a written release.

Deletion and destruction

- **Electronic data.** Deletion uses methods appropriate to the storage medium: cryptographic erasure (encrypted-at-rest systems), secure overwrite or secure erase commands for local media, and tenant-isolated key destruction where cloud providers support it. Backups roll off per the backup schedule.
- **Paper.** Paper records containing Confidential or Restricted information are cross-cut shredded or destroyed by an approved, certified disposal vendor. Certificates of destruction are retained for bulk disposal of Restricted records.
- **Removable media and retired hardware.** Storage media is wiped per NIST SP 800-88 guidance, with a record of who wiped, when, and the verification evidence.

Responsibilities

- **Data Owners.** Know the retention obligations for the data they own; validate that retention controls function; authorize deletion or retention extensions.

- **IT and Infrastructure.** Implement the retention controls — scheduled deletion jobs, backup lifecycle policies, archive tiering — and evidence their execution.
- **Legal.** Issues and releases legal holds; advises on regulatory and contractual retention obligations.
- **Workforce members.** Do not retain copies of Confidential or Restricted data beyond the retention period; do not retain data on personal devices.

Scope exceptions

Exceptions (longer or shorter retention than this policy prescribes) must be submitted in writing, identify the authoritative basis, and be approved by Legal and the CISO.

Review cadence

This policy is reviewed annually by Legal, the Data Protection Officer (or delegate), and the security team, or sooner on material change to Your Organization's regulatory or contractual obligations.

Effective date: [the date this policy takes effect]