Generate a policy for data retention policy.

# DATA RETENTION POLICY

## 1. Policy Purpose

To establish guidelines for retaining, securing, and disposing of organizational data to ensure:

- Compliance with legal/regulatory requirements

- Minimization of storage costs and privacy risks

- Availability of data for business needs

## 2. Scope

\*\*Applies to:\*\*

✅ All employees, contractors, and third parties

✅ All data formats (electronic, physical, backups)

✅ All systems and storage locations

## 3. Core Principles

| Principle | Description |

|-----------|-------------|

| \*\*Compliance\*\* | Adhere to GDPR, CCPA, HIPAA, SOX, etc. |

| \*\*Minimization\*\* | Retain only as long as necessary |

| \*\*Security\*\* | Protect based on sensitivity classification |

| \*\*Accountability\*\* | Document retention/disposal actions |

## 4. Data Classification & Retention

\*\*Default Retention:\*\* `[7 years]` unless otherwise specified

### Retention Schedule (Illustrative)

| Data Category | Owner | Retention Period | Legal Basis | Disposal Method |

|---------------|-------|------------------|-------------|-----------------|

| Employee Records | HR | Termination + 7 yrs | Labor Laws | Secure Shredding |

| Financial Records | Finance | Fiscal Year + 7 yrs | IRS/SOX | Secure Erasure |

| Customer Contracts | Legal | Expiry + 10 yrs | Contract Law | Shredding/Erasure |

| System Logs | IT | 90 days - 1 yr | Security | Secure Erasure |

| Backup Tapes | IT | 30-90 days | DR | Physical Destruction |

> \*Customize full schedule in Appendix A\*

## 5. Data Storage & Security

- Encrypt sensitive data at rest/in transit

- Restrict access via least-privilege principle

- Physically secure storage for documents/media

- Apply security controls per Data Classification Policy

## 6. Secure Disposal Procedures

\*\*Electronic Data:\*\*

- Certified erasure (NIST 800-88)

- Physical destruction of media

\*\*Physical Records:\*\*

- Cross-cut shredding

- Certified vendor destruction

\*\*Document:\*\* Date, method, data category, responsible party

## 7. Litigation Hold Process

- \*\*Trigger:\*\* Anticipated/active litigation, investigation

- \*\*Action:\*\* Immediate suspension of disposal

- \*\*Authority:\*\* Legal Department holds

- \*\*Duration:\*\* Until formal release

## 8. Roles & Responsibilities

| Role | Key Duties |

|------|------------|

| \*\*Senior Management\*\* | Policy approval, resource allocation |

| \*\*Data Owners\*\* | Classify data, define retention needs |

| \*\*Legal/Compliance\*\* | Regulatory guidance, hold management |

| \*\*IT Department\*\* | Technical implementation, disposal execution |

| \*\*All Personnel\*\* | Compliance, reporting holds |

## 9. Policy Governance

- \*\*Annual review\*\* by Legal/Compliance/IT

- Updates for legal/operational changes

- Mandatory training for data handlers

- Audits with corrective actions

## 10. Definitions

- \*\*Data Owner:\*\* Business head accountable for dataset lifecycle

- \*\*Litigation Hold:\*\* Legal suspension of disposal

- \*\*Secure Destruction:\*\* Irreversible data elimination

## 11. Contacts

- Policy Questions: `[Compliance Officer Email]`

- Legal Holds: `[General Counsel Email]`

- IT Implementation: `[IT Security Manager Email]`

\*\*Effective Date:\*\* `[Date]`

\*\*Last Reviewed:\*\* `[Date]`

---

\*\*APPENDIX A: FULL RETENTION SCHEDULE\*\*

\*Customize this table for your organization\*

| Data Category | Owner | Retention Trigger | Retention Period | Legal/Regulatory Basis | Disposal Method |

|---------------|-------|-------------------|------------------|------------------------|-----------------|

| `[e.g., Healthcare Records]` | `[Dept]` | `[Last Treatment Date]` | `[10 years]` | `[HIPAA]` | `[Secure Erasure]` |

| `[e.g., Tax Filings]` | `[Finance]` | `[Filing Date]` | `[Permanent]` | `[IRS]` | `[Secure Archiving]` |