Generate a policy for data retention policy.

**Data Retention Policy**

**1. Purpose and Scope**

This Data Retention Policy establishes guidelines for the systematic review, retention, and disposal of documents and records maintained by [Organization Name]. This policy applies to all employees, contractors, and third parties who create, receive, maintain, or dispose of records on behalf of the organization.

**2. Policy Statement**

[Organization Name] is committed to maintaining accurate records while ensuring compliance with legal, regulatory, and business requirements. This policy balances the need to retain information for operational, legal, and historical purposes with the obligation to protect privacy and manage storage costs effectively.

**3. Definitions**

**Record**: Any recorded information, regardless of physical form or characteristics, created or received in the conduct of business activities.

**Retention Period**: The length of time records must be maintained before they are eligible for disposal.

**Legal Hold**: A directive to preserve all forms of relevant information when litigation is reasonably anticipated.

**Personal Data**: Any information relating to an identified or identifiable natural person.

**Disposition**: The final action taken with records, including destruction, transfer, or permanent retention.

**4. Data Classification and Retention Schedules**

**4.1 Financial Records**

* **Tax Returns and Supporting Documents**: 7 years after filing
* **Audit Reports**: 7 years
* **General Ledgers and Journals**: 7 years
* **Invoices and Receipts**: 7 years
* **Payroll Records**: 7 years
* **Banking Records**: 7 years
* **Insurance Policies**: 7 years after expiration

**4.2 Human Resources Records**

* **Employee Personnel Files**: 7 years after termination
* **Employment Applications (Hired)**: Duration of employment + 3 years
* **Employment Applications (Not Hired)**: 2 years
* **Performance Reviews**: 5 years after employee separation
* **Training Records**: Duration of employment + 3 years
* **Workers' Compensation Claims**: 5 years after case closure
* **Employee Medical Records**: 30 years

**4.3 Legal and Compliance Records**

* **Contracts**: 7 years after expiration or termination
* **Legal Correspondence**: 7 years
* **Compliance Reports**: 7 years
* **Incident Reports**: 7 years
* **Board Meeting Minutes**: Permanent
* **Corporate Charter and Bylaws**: Permanent

**4.4 Customer and Client Data**

* **Customer Records (Active)**: Duration of relationship + 7 years
* **Customer Records (Inactive)**: 7 years after last interaction
* **Customer Communications**: 3 years
* **Marketing Lists**: Review annually, purge inactive records after 3 years
* **Website Analytics**: 2 years
* **Customer Support Tickets**: 3 years

**4.5 Information Technology Records**

* **System Backups**: 90 days (daily), 12 months (monthly)
* **Security Logs**: 1 year
* **Email Archives**: 7 years for business-related emails
* **Software Licenses**: 7 years after expiration
* **IT Asset Records**: 7 years after disposal
* **Network Configuration**: Current version + 2 previous versions

**4.6 Operational Records**

* **Project Documentation**: 5 years after project completion
* **Vendor Records**: 7 years after contract termination
* **Property Records**: Permanent while owned + 7 years after disposal
* **Environmental Records**: 30 years
* **Safety Records**: 30 years

**5. Legal Holds and Litigation**

When litigation, investigation, or audit is reasonably anticipated, all relevant records must be preserved regardless of their scheduled retention period. The Legal Department will issue legal hold notices specifying:

* Scope of preserved materials
* Custodians responsible for preservation
* Duration of the hold
* Instructions for compliance

Records subject to legal hold cannot be destroyed until the hold is formally lifted in writing.

**6. Data Disposal Procedures**

**6.1 Secure Destruction Methods**

* **Paper Records**: Cross-cut shredding or professional destruction service
* **Electronic Media**: Secure wiping software or physical destruction
* **Confidential Information**: Certificate of destruction required

**6.2 Disposal Authorization**

All record destruction must be approved by:

* Department manager for routine disposals
* Legal Department for records involving litigation or regulatory matters
* Data Protection Officer for personal data

**6.3 Documentation**

Maintain records of destruction including:

* Description of destroyed records
* Date of destruction
* Method of destruction
* Authorization signatures
* Certificate of destruction (if applicable)

**7. Privacy and Data Protection**

**7.1 Personal Data Retention**

Personal data will be retained only as long as necessary for the purposes for which it was collected, subject to:

* Legal requirements
* Legitimate business interests
* Individual consent (where applicable)

**7.2 Data Subject Rights**

Individuals have the right to:

* Request access to their personal data
* Request correction of inaccurate data
* Request deletion of data (subject to legal requirements)
* Object to processing in certain circumstances

**8. Responsibilities**

**8.1 Data Protection Officer**

* Oversee policy implementation and compliance
* Provide guidance on retention requirements
* Coordinate with legal counsel on holds and disposals
* Monitor regulatory changes affecting retention

**8.2 Department Managers**

* Ensure compliance within their departments
* Identify records for retention or disposal
* Train staff on retention procedures
* Authorize routine record disposal

**8.3 IT Department**

* Implement technical controls for retention
* Manage backup and archival systems
* Ensure secure disposal of electronic media
* Maintain system logs as required

**8.4 All Employees**

* Follow retention guidelines for their records
* Consult supervisors when uncertain about retention
* Report potential compliance issues
* Participate in retention training

**9. Monitoring and Compliance**

**9.1 Regular Reviews**

* Annual review of retention schedules
* Quarterly compliance audits
* Semi-annual disposal activities
* Regular training updates

**9.2 Non-Compliance**

Violations of this policy may result in:

* Disciplinary action up to and including termination
* Legal liability for the organization
* Regulatory penalties
* Loss of legal protections

**10. Training and Awareness**

All employees will receive training on:

* Data retention requirements
* Proper record handling procedures
* Legal hold obligations
* Privacy protection requirements

Training will be provided:

* During new employee orientation
* Annually for all staff
* When policy changes occur
* As needed for specific roles

**11. Policy Review and Updates**

This policy will be reviewed annually and updated as needed to reflect:

* Changes in applicable laws and regulations
* Business operational changes
* Technology updates
* Best practice developments

**12. Related Policies**

This policy should be read in conjunction with:

* Information Security Policy
* Privacy Policy
* Document Management Policy
* Email and Communications Policy
* Records Management Policy

**13. Contact Information**

For questions about this policy, contact:

* Data Protection Officer: [email/phone]
* Legal Department: [email/phone]
* IT Helpdesk: [email/phone]

**Policy Effective Date**: [Date]  
**Last Reviewed**: [Date]  
**Next Review Date**: [Date]  
**Policy Owner**: [Title/Department]  
**Approved By**: [Name, Title]