Generate a secure policy for data retention policy. Ensure security best practices.

**Data Retention Policy**

**1. Purpose and Scope**

This Data Retention Policy establishes guidelines for the systematic retention, archival, and secure disposal of organizational data to ensure compliance with legal requirements, regulatory obligations, and business needs while minimizing security risks and storage costs.

**Scope:** This policy applies to all employees, contractors, vendors, and third parties who handle organizational data across all systems, platforms, and storage mediums.

**2. Policy Statement**

The organization is committed to maintaining data only as long as necessary for legitimate business purposes, legal compliance, or regulatory requirements. Data must be securely disposed of when retention periods expire to minimize security exposure and privacy risks.

**3. Data Classification and Retention Schedules**

**3.1 Personal Data (PII/PHI)**

* **Retention Period:** Maximum 7 years or as required by applicable privacy laws
* **Review Frequency:** Annual
* **Disposal Method:** Secure deletion with cryptographic erasure
* **Special Considerations:** Subject to data subject rights (GDPR, CCPA)

**3.2 Financial Records**

* **Retention Period:** 7 years minimum (varies by jurisdiction)
* **Review Frequency:** Annual
* **Disposal Method:** Secure shredding (physical) or cryptographic erasure (digital)
* **Legal Basis:** Tax regulations, SOX compliance

**3.3 Employee Records**

* **Active Employees:** Duration of employment + 7 years
* **Former Employees:** 7 years post-termination
* **Payroll Records:** 7 years
* **Benefits Records:** As required by plan documents or 7 years minimum

**3.4 Customer Data**

* **Active Customers:** Duration of relationship + 3 years
* **Former Customers:** 5 years post-relationship termination
* **Transaction Records:** 7 years
* **Marketing Data:** 3 years or until consent withdrawal

**3.5 Business Communications**

* **Email:** 3 years (general business), 7 years (financial/legal)
* **Instant Messages:** 1 year
* **Meeting Records:** 3 years
* **Contracts:** Duration of contract + 7 years

**3.6 Technical Data**

* **System Logs:** 1 year (operational), 3 years (security logs)
* **Backup Data:** 90 days (operational), 1 year (archival)
* **Monitoring Data:** 6 months
* **Audit Trails:** 7 years

**3.7 Legal Hold Data**

* **Retention Period:** Until legal hold is lifted + 90 days
* **Review Frequency:** Quarterly
* **Authorization Required:** Legal department approval for disposal

**4. Security Requirements**

**4.1 Data Protection During Retention**

* All retained data must be encrypted at rest using AES-256 or equivalent
* Access controls must follow principle of least privilege
* Regular access reviews required quarterly
* Data integrity monitoring and checksums required for long-term storage

**4.2 Secure Storage Requirements**

* Physical media must be stored in secure, climate-controlled environments
* Cloud storage must meet SOC 2 Type II or equivalent certifications
* Geographic restrictions may apply based on data classification
* Redundant storage required for critical business data

**4.3 Data Disposal Security Standards**

* **Digital Data:** Minimum 3-pass overwrite or cryptographic erasure
* **SSDs/Flash Storage:** Cryptographic erasure or physical destruction
* **Physical Media:** Cross-cut shredding or incineration by certified vendor
* **Cloud Data:** Verified deletion with provider confirmation
* **Certificate of Destruction:** Required for all disposal activities

**5. Implementation Procedures**

**5.1 Data Inventory and Mapping**

* Maintain comprehensive data inventory with classification tags
* Document data flows and processing activities
* Identify data controllers and processors
* Map retention requirements to specific data sets

**5.2 Automated Retention Management**

* Implement automated retention scheduling where technically feasible
* Configure system alerts for upcoming retention deadlines
* Establish approval workflows for retention extensions
* Monitor compliance through regular reporting

**5.3 Legal Hold Procedures**

* Immediate suspension of normal retention schedules when legal hold issued
* Notification to all relevant data custodians within 24 hours
* Preservation of all potentially relevant data in separate secure storage
* Documentation of all hold-related activities

**6. Roles and Responsibilities**

**6.1 Data Protection Officer (DPO)**

* Overall policy oversight and compliance monitoring
* Annual policy review and updates
* Liaison with legal and regulatory bodies
* Exception approval authority

**6.2 IT Security Team**

* Technical implementation of retention controls
* Secure disposal execution and verification
* Security monitoring of retained data
* Incident response for retention-related security events

**6.3 Legal Department**

* Legal hold management and coordination
* Regulatory requirement interpretation
* Litigation support and discovery management
* Policy compliance advice

**6.4 Data Custodians**

* Day-to-day retention schedule adherence
* Data quality and accuracy maintenance
* Access request processing
* Incident reporting to appropriate teams

**6.5 Business Unit Managers**

* Business justification for retention requirements
* Resource allocation for compliance activities
* Staff training and awareness programs
* Exception request initiation

**7. Compliance and Monitoring**

**7.1 Regular Audits**

* Annual comprehensive retention compliance audit
* Quarterly spot checks of high-risk data categories
* Monthly automated compliance reporting
* Immediate investigation of policy violations

**7.2 Metrics and KPIs**

* Percentage of data disposed within required timeframes
* Number of successful automated disposal processes
* Volume of data under legal hold
* Cost savings from proper data lifecycle management

**7.3 Training Requirements**

* Annual mandatory training for all staff
* Specialized training for data custodians and IT personnel
* New employee onboarding includes retention policy training
* Regular updates when policy changes occur

**8. Exceptions and Appeals**

**8.1 Exception Process**

* Written business justification required
* Risk assessment and mitigation plan
* Approval by DPO and relevant business unit manager
* Documentation in central exception registry
* Regular review of approved exceptions

**8.2 Emergency Procedures**

* Expedited disposal process for security incidents
* Emergency legal hold procedures
* Breach notification requirements
* Crisis communication protocols

**9. International Considerations**

**9.1 Multi-Jurisdictional Compliance**

* Compliance with local data protection laws in all operating jurisdictions
* Cross-border data transfer restrictions
* Conflicting law resolution procedures
* Regular monitoring of changing international requirements

**9.2 Data Localization Requirements**

* Documentation of data residency requirements
* Technical controls to ensure compliance
* Regular validation of data location
* Vendor management for international providers

**10. Policy Governance**

**10.1 Review and Updates**

* Annual policy review and approval by executive leadership
* Quarterly assessment of regulatory changes
* Immediate updates for significant legal or business changes
* Version control and change documentation

**10.2 Communication**

* Policy publication in employee handbook and intranet
* Regular awareness campaigns and communications
* Integration with onboarding and training programs
* Feedback mechanisms for policy improvement

**11. Enforcement and Sanctions**

**11.1 Policy Violations**

* Progressive disciplinary action for non-compliance
* Immediate action for willful violations
* Corrective action plans for systemic issues
* Regular compliance monitoring and reporting

**11.2 Vendor and Third-Party Requirements**

* Contractual retention requirements for all vendors
* Regular vendor compliance assessments
* Right to audit vendor retention practices
* Termination rights for non-compliance

**Policy Version:** 1.0  
**Effective Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 1 Year]  
**Approved By:** [Chief Information Security Officer, Data Protection Officer, Legal Counsel]  
**Document Classification:** Internal Use Only