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

**Data Retention Policy**

Effective Date: May 30, 2025

Last Reviewed: May 30, 2025

1. Introduction and Purpose

This Data Retention Policy outlines the guidelines and procedures for managing and retaining data within [Your Company Name]. The primary purpose of this policy is to ensure that data is retained for the appropriate duration to meet legal, regulatory, business, and operational requirements, while also minimizing risks and costs associated with unnecessary data storage. This policy is designed to incorporate security best practices to protect data throughout its lifecycle.

2. Scope

This policy applies to all data created, received, processed, stored, or transmitted by [Your Company Name], regardless of its format (e.g., electronic, paper) or location (e.g., company servers, cloud storage, employee devices, physical archives). This includes, but is not limited to:

* Customer data
* Employee data
* Financial records
* Intellectual property
* Operational data
* Communication records (e.g., emails, instant messages)
* System logs

3. Roles and Responsibilities

* Data Protection Officer (DPO) / Legal Counsel: Responsible for overseeing compliance with this policy, advising on legal and regulatory retention requirements, and approving retention schedules.
* IT Department: Responsible for implementing and maintaining the technical infrastructure and procedures for data retention, secure storage, and secure disposal. This includes managing backups, archiving systems, and data destruction processes.
* Data Owners/Custodians: Heads of departments or designated individuals responsible for classifying data within their respective areas, ensuring adherence to retention schedules, and authorizing data disposal in consultation with the DPO/Legal Counsel.
* All Employees and Contractors: Responsible for understanding and complying with this policy in their daily handling of company data.

4. Data Classification

Data must be classified based on its sensitivity, criticality, and applicable legal or regulatory requirements. The classification level will help determine the appropriate retention period and security controls. A separate Data Classification Policy should provide detailed categories, but generally, classifications may include:

* Confidential: Highly sensitive data requiring the strictest access controls and security measures (e.g., Personally Identifiable Information (PII), financial account details, trade secrets).
* Restricted: Data that is sensitive and intended for internal use only, requiring strong security measures (e.g., internal business plans, employee records).
* Internal: Data generally available to employees but not for public disclosure (e.g., internal communications, operational procedures).
* Public: Data that is approved for public dissemination.

5. Retention Schedules

Retention schedules define the minimum and maximum time periods for which different types of data must be retained. These schedules must be based on:

* Legal and Regulatory Requirements: Compliance with relevant laws and regulations (e.g., GDPR, CCPA, HIPAA, SOX, industry-specific regulations).
* Business Needs: Operational requirements, historical reference, and potential litigation.
* Financial and Audit Requirements: Tax laws, accounting standards, and audit trails.

A detailed Data Retention Schedule will be maintained as a separate document, appended to this policy, and reviewed regularly by the DPO/Legal Counsel and relevant Data Owners. This schedule will specify:

* Data Category/Type
* Data Classification
* Retention Period (start and end triggers)
* Legal/Regulatory Citation (if applicable)
* Storage Location/Medium
* Disposal Method

6. Data Storage and Security During Retention

All retained data must be stored securely to protect its confidentiality, integrity, and availability. Security measures include:

* Access Controls: Implementing role-based access controls (RBAC) and the principle of least privilege to ensure that only authorized personnel can access data relevant to their roles. Multi-factor authentication (MFA) should be enforced for access to sensitive data.
* Encryption: Encrypting sensitive data both at rest (stored on servers, databases, backups) and in transit (when transmitted over networks). Strong, industry-standard encryption algorithms must be used.
* Physical Security: Implementing appropriate physical security measures for servers, storage media, and physical records to prevent unauthorized access, theft, or damage.
* Logical Security: Utilizing firewalls, intrusion detection/prevention systems (IDS/IPS), anti-malware software, and regular security patching to protect electronic data.
* Data Masking and Anonymization: Where appropriate, sensitive data in non-production environments (e.g., testing, development) should be masked or anonymized.
* Regular Audits and Monitoring: Conducting regular security audits and monitoring access logs to detect and respond to suspicious activity.
* Backup and Disaster Recovery: Maintaining regular, secure backups of critical data and having a tested disaster recovery plan in place to ensure data can be restored in case of loss or corruption. Backup data is subject to the same retention and security requirements as primary data.

7. Data Disposal

Once the retention period for specific data has expired, and there are no superseding legal holds or business requirements for its continued retention, the data must be securely and permanently disposed of.

* Secure Deletion: Electronic data must be disposed of using methods that render it unrecoverable, such as cryptographic erasure, degaussing, or physical destruction of storage media. Simple deletion (e.g., moving to a recycle bin) is not sufficient for sensitive data.
* Physical Document Destruction: Paper records must be destroyed by shredding (cross-cut), pulping, or incineration to ensure they cannot be reconstructed.
* Third-Party Disposal: If third-party vendors are used for data disposal, they must be vetted for their security practices and provide a certificate of destruction.
* Documentation: A record of data disposal, including the date, data category, method of disposal, and authorization, must be maintained.

8. Legal Holds

In the event of litigation, investigation, or audit, a "legal hold" may be issued. A legal hold suspends the normal data retention and disposal procedures for specific data relevant to the matter. Data subject to a legal hold must be preserved until the hold is officially lifted by the DPO/Legal Counsel. No employee may destroy data subject to a legal hold.

9. Policy Review and Updates

This Data Retention Policy and the associated Data Retention Schedule will be reviewed at least annually, or as needed, to reflect changes in legal, regulatory, or business requirements. Updates will be approved by the DPO/Legal Counsel and communicated to all relevant personnel.

10. Training and Awareness

All employees and relevant contractors will receive training on this Data Retention Policy and their responsibilities for data handling, retention, and disposal. Regular awareness campaigns will reinforce the importance of this policy.

11. Compliance and Enforcement

* Compliance with this policy is mandatory for all employees and contractors.
* Violations of this policy may result in disciplinary action, up to and including termination of employment1 or contract, and may also lead to legal or regulatory penalties for [Your Company Name].
* Any suspected or actual breaches of this policy or data security incidents must be reported immediately to the IT Department or the DPO.

12. Exceptions

Any exceptions to this policy must be documented, justified, and approved in writing by the DPO/Legal Counsel and the relevant Data Owner. Exceptions should be reviewed periodically.

Appendices:

* Appendix A: Data Retention Schedule (to be maintained as a separate, living document)

Approval:

[Name and Title of Approving Authority, e.g., CEO, CIO, DPO]

Date