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

Here's a sample **Data Retention Policy** that aligns with data security best practices and can be adapted for most organizations:

**Data Retention Policy**

**1. Purpose**  
This Data Retention Policy outlines the procedures and guidelines for retaining, storing, and securely disposing of data to ensure compliance with legal, regulatory, and operational requirements while protecting sensitive information from unauthorized access or disclosure.

**2. Scope**  
This policy applies to all employees, contractors, and third-party service providers who handle data for [Organization Name], including electronic and paper records.

**3. Data Classification**  
Data will be categorized into the following types:

* **Confidential:** Personally Identifiable Information (PII), financial data, health records, etc.
* **Internal:** Business process documents, internal communications.
* **Public:** Marketing materials, press releases, etc.

**4. Retention Periods**

| **Data Type** | **Retention Period** | **Disposal Method** |
| --- | --- | --- |
| Financial records | 7 years | Shredding/encrypted deletion |
| Employee records | 7 years post-employment | Secure destruction |
| Customer data (PII) | 5 years after last activity | Anonymization/deletion |
| Emails | 3 years | Secure deletion |
| Logs (Security/Audit) | 1 year | Secure deletion |

**5. Secure Storage and Access**

* Data must be stored using encrypted systems.
* Access controls must enforce the principle of least privilege.
* All systems must utilize multi-factor authentication (MFA).

**6. Data Disposal**

* Electronic data must be deleted using secure wiping tools compliant with DoD 5220.22-M or NIST SP 800-88 standards.
* Paper records must be shredded using cross-cut shredders or incinerated.

**7. Compliance and Monitoring**

* Regular audits will be conducted to ensure compliance.
* Violations of this policy may result in disciplinary action up to and including termination.

**8. Policy Review**  
This policy shall be reviewed annually or upon significant changes to applicable regulations or business processes.

**9. Roles and Responsibilities**

* **Data Owners:** Ensure compliance with retention schedules.
* **IT Department:** Implement technical safeguards and secure disposal mechanisms.
* **Compliance Officer:** Monitor adherence and audit readiness.

**10. Exceptions**  
Any exceptions to this policy must be documented and approved by the Compliance Officer.