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

**1. Purpose**

The purpose of this policy is to define the procedures for retaining and securely disposing of data in compliance with legal, regulatory, and business requirements.

**2. Scope**

This policy applies to all data collected, processed, and stored by the organization, including electronic and physical records.

**3. Data Classification**

* **Sensitive Data**: Includes personal identifiable information (PII), financial records, health information, and any other data protected by law.
* **Business Data**: Includes operational data, business records, and other information critical to business operations.
* **Non-Sensitive Data**: Includes public information and data that does not require special protection.

**4. Retention Periods**

* **Sensitive Data**: Retain only as long as necessary to fulfill the purpose for which it was collected, and in accordance with legal and regulatory requirements.
* **Business Data**: Retain for a period that aligns with business needs and legal requirements.
* **Non-Sensitive Data**: Retain as needed for operational purposes.

**5. Data Storage and Security**

* **Encryption**: All sensitive data must be encrypted both at rest and in transit.
* **Access Controls**: Implement strict access controls to ensure that only authorized personnel can access sensitive data.
* **Regular Audits**: Conduct regular audits to ensure compliance with this policy and to identify any potential security risks.

**6. Data Disposal**

* **Secure Deletion**: Use secure deletion methods to ensure that data cannot be recovered once it is no longer needed.
* **Physical Records**: Shred or otherwise destroy physical records in a secure manner.
* **Documentation**: Maintain records of data disposal activities for audit purposes.

**7. Compliance**

* **Legal and Regulatory Requirements**: Ensure that all data retention and disposal activities comply with applicable laws and regulations.
* **Internal Policies**: Adhere to internal policies and procedures related to data management and security.

**8. Roles and Responsibilities**

* **Data Owners**: Responsible for defining data retention periods and ensuring compliance with this policy.
* **IT Department**: Responsible for implementing technical controls to secure data and ensure proper disposal.
* **Employees**: Responsible for adhering to this policy and reporting any potential violations.

**9. Review and Updates**

* **Regular Reviews**: Conduct regular reviews of this policy to ensure it remains up-to-date with changing legal, regulatory, and business requirements.
* **Updates**: Make updates to this policy as needed and communicate changes to all relevant stakeholders.

**10. Training and Awareness**

* **Training Programs**: Implement training programs to educate employees on the importance of data retention and security best practices.
* **Awareness Campaigns**: Conduct awareness campaigns to reinforce the importance of adhering to this policy.

**11. Incident Response**

* **Reporting**: Establish procedures for reporting potential violations of this policy.
* **Investigation**: Conduct thorough investigations of any reported incidents and take appropriate action.