# Data Decommissioning Plan

Project Name: [Insert Project Name]

Date: [Insert Date]

Version: [Insert Version Number]

**1. Introduction**

This Data Decommissioning Plan details the steps for securely decommissioning data in the [Insert Project Name]. It outlines the procedures for data disposal, anonymization, or archiving, ensuring compliance with data governance policies and protecting against unauthorized access or breaches.

**2. Purpose and Scope**

**2.1 Purpose**

The purpose of this plan is to:

* Outline the steps for securely decommissioning data that is no longer needed in the [Insert Project Name].
* Ensure that all decommissioned data is properly disposed of, anonymized, or archived in accordance with governance policies.
* Mitigate risks associated with data decommissioning, such as unauthorized access, data breaches, or non-compliance with regulatory requirements.

**2.2 Scope**

This plan applies to all datasets used in the [Insert Project Name] that have reached the end of their lifecycle. It covers structured, unstructured, and semi-structured data stored in internal and external systems.

**3. Decommissioning Criteria**

**3.1 Criteria for Decommissioning**

Data will be decommissioned when it meets one or more of the following criteria:

* End of Retention Period: The data has exceeded its retention period as defined in the Data Retention and Archiving Policy.
* Business Usefulness: The data is no longer required for operational, analytical, or historical purposes.
* Regulatory Requirements: The data must be decommissioned in compliance with specific regulatory or legal mandates.

**3.2 Exemptions**

Data subject to the following exemptions will not be decommissioned:

* Legal Holds: Data involved in ongoing litigation or regulatory investigations will be retained until the hold is lifted.
* Critical Data: Data required for disaster recovery or business continuity will not be decommissioned until it is no longer needed.

**4. Data Disposal**

**4.1 Disposal Process**

Data that is no longer needed and does not meet archival criteria will be securely disposed of. The disposal process includes:

* Secure Deletion Tools: Data will be erased using [Insert Deletion Tool/Method], ensuring that it is irrecoverable and meets industry standards (e.g., NIST SP 800-88 guidelines for data destruction).
* Verification of Deletion: A verification process will be conducted using [Insert Verification Method] to ensure that the data has been successfully and permanently deleted.
* Audit Logging: All data disposal activities will be logged in the audit system for compliance verification.

**4.2 Physical Media Disposal**

If data is stored on physical media (e.g., hard drives, tapes), the following steps will be taken to securely dispose of the media:

* Destruction Methods: Physical media will be destroyed using [Insert Method, e.g., shredding, degaussing] to ensure that data cannot be recovered.
* Certificate of Destruction: A certificate of destruction will be obtained from the disposal vendor to verify that the media has been destroyed according to industry standards.

**5. Data Anonymization**

**5.1 Anonymization Process**

In cases where the data must be retained for analytical or historical purposes, but personally identifiable information (PII) or sensitive data must be protected, the data will be anonymized using the following steps:

* Anonymization Techniques: Data will be anonymized using [Insert Anonymization Techniques, e.g., k-anonymity, differential privacy] to ensure that individuals cannot be re-identified.
* Pseudonymization: If anonymization is not possible, pseudonymization techniques will be applied, where identifiers are replaced with unique keys that are stored separately.
* Anonymization Validation: After anonymization, the data will be reviewed to confirm that it meets regulatory standards (e.g., GDPR) and that no re-identification is possible.

**6. Data Archiving**

**6.1 Archival of Data**

Data that is no longer actively used but must be retained for legal or historical reasons will be archived according to the following procedures:

* Archiving Method: Data will be moved to an archival system, such as [Insert Archival Tool], where it will be securely stored and protected.
* Encryption and Access Control: Archived data will be encrypted using [Insert Encryption Standard, e.g., AES-256] and access will be restricted to authorized personnel only.
* Audit Trails: All actions involving archived data, including retrievals, will be logged for compliance purposes.

**7. Decommissioning Risk Management**

**7.1 Risk Identification**

The following risks have been identified in the data decommissioning process:

* Unauthorized Access: Risk of unauthorized access to data during the decommissioning process.
* Data Breach: Risk of data breach due to improper deletion or disposal.
* Non-Compliance: Risk of non-compliance with data protection laws and regulations.

**7.2 Risk Mitigation Strategies**

* Encryption: All sensitive data will be encrypted before decommissioning to protect it from unauthorized access.
* Secure Disposal: Use certified vendors and secure methods for physical and electronic data disposal to prevent breaches.
* Compliance Monitoring: Regular audits will be conducted to ensure that decommissioning activities comply with legal and regulatory requirements.

**8. Documentation and Reporting**

**8.1 Audit Logs**

All data decommissioning activities will be documented in detailed audit logs, including:

* Decommissioning Date: The date when the data was decommissioned.
* Decommissioning Method: The method used for decommissioning (e.g., deletion, anonymization, archiving).
* Personnel Involved: The individuals responsible for performing and verifying the decommissioning process.

**8.2 Reporting**

Decommissioning reports will be generated on a [Insert Frequency] basis and submitted to [Insert Approver Name] for review. These reports will include a summary of all data decommissioned during the reporting period, any issues encountered, and the steps taken to mitigate risks.

**9. Document Control**

* Document Owner: [Insert Name, Role]
* Approval Date: [Insert Date]
* Next Review Date: [Insert Date]
* Version History:
  + Version [Insert Version Number] - Initial Document - [Insert Date] - Approved by [Insert Name]