Data Lifecycle Management Policy

> **Source File:** generated-documents\dmbok\data-lifecycle-management-policy.md
> **Generated:** 30/07/2025 at 06:57:35
> **Generated by:** Requirements Gathering Agent - PDF Converter

Data Lifecycle Management Policy

Generated by adpa-enterprise-framework-automation v3.2.0
Category: dmbok
Generated: 2025-07-17T18:06:24.762Z
Description: Comprehensive policy for managing data throughout its lifecycle from creation to archival and disposal.

Certainly! Here's a professional Data Lifecycle Management (DLM) Policy template tailored to the **ADPA - Advanced Document Processing & Automation Framework** project, aligning with enterprise frameworks (BABOK, PMBOK, DMBOK) and referencing best practices for scalable, compliant, and secure data management.

Data Lifecycle Management (DLM) Policy

Project: ADPA – Advanced Document Processing & Automation Framework

---

1. Introduction

1.1 Purpose

This policy establishes standardized requirements and controls for managing data throughout its lifecycle within the ADPA project. It ensures data is created, maintained, shared, archived, and disposed of in compliance with regulatory, contractual, and organizational requirements, including but not limited to GDPR, SOX, PCI DSS, and DMBOK best practices.

1.2 Scope

This policy applies to all ADPA data assets—structured and unstructured, regardless of storage location (cloud, on-premises, third-party platforms like SharePoint/Confluence, or within the ADPA system itself). It covers all users, including employees, contractors, and third parties with data access.

---

2. Data Lifecycle Phases

2.1 Data Creation and Collection

- All data must be created or collected using approved methods.
- Mandatory metadata capture at creation (e.g., owner, classification, source).
- Data quality checks must be embedded at point of entry.
- Compliance with relevant standards (e.g., DMBOK 2.0, PMBOK).

2.2 Data Storage and Maintenance

- Data must be stored in approved, secured repositories (with encryption at rest).

- Storage systems must support versioning, audit trails, and automated backup.
- Retention schedules must be documented and enforced per data classification.
- Data quality monitoring (accuracy, completeness, consistency) is mandatory.

2.3 Data Usage and Sharing

- Access must be controlled using least-privilege principles and RBAC.
- Data sharing (internal/external) requires documented agreements and approvals.
- Usage is logged and monitored; all activity must be auditable.
- Data must not be used for purposes outside of its intended scope without re-authorization.

2.4 Data Archival

- Data eligible for archival must meet criteria (age, regulatory, or project closure).
- Archival storage must ensure integrity, security, and retrievability.
- Access to archived data must be strictly controlled and monitored.

2.5 Data Disposal

- Data disposal must use secure, irreversible methods (e.g., cryptographic wipe, DOD-compliant deletion).
- Disposal actions must be documented and, where required, independently verified.
- Retention of disposal records per compliance requirements (e.g., 7 years for SOX).

---

3. Roles and Responsibilities

3.1 Data Owners

- Assign data classification and approve access.
- Define retention and archival periods.
- Ensure compliance with policy and regulatory requirements.

3.2 Data Stewards

- Implement data governance and quality controls.
- Monitor, report, and remediate data quality issues.
- Maintain data dictionaries, lineage, and documentation.

3.3 IT Operations

- Provide and maintain secure storage and backup infrastructure.
- Enforce access controls and monitor for policy violations.
- Execute data archival and disposal as directed.

3.4 Business Users

- Handle data in accordance with this policy and training.
- Report suspected data quality or security issues.
- Participate in data governance activities as required.

---

4. Implementation Guidelines

4.1 Data Classification

- All data must be classified (e.g., Public, Internal, Confidential, Restricted) per the data classification scheme.
- Classification must be reviewed periodically and updated as necessary.
- Data must be labeled/marked appropriately in all systems.

4.2 Data Quality Management

- Data quality metrics (accuracy, timeliness, completeness, consistency, validity) must be defined and monitored.
- Automated and manual quality checks must be implemented.
- Issues must be logged, tracked, and resolved per workflow.

4.3 Security and Privacy

- All data must be protected using appropriate technical (encryption, access controls) and organizational (policies, training) controls.
- Compliance with privacy (GDPR, CCPA, etc.) and security (ISO 27001, NIST) standards is mandatory.
- Data masking/anonymization must be used for non-production environments and analytics.

4.4 Compliance and Auditing

- Maintain a compliance matrix mapping data to regulatory requirements.
- Regular audits (internal and external) must be scheduled and findings tracked to closure.
- Audit logs must be immutable and retained per policy.

---

5. Review and Update

5.1 Policy Review

- This policy must be reviewed at least annually, or upon significant changes to regulations, business processes, or system architecture.
- Reviews must be documented, and updates approved by data governance leadership.

5.2 Change Management

- Policy changes follow the ADPA change management process.
- Version history and change rationales must be maintained.

- Stakeholders must be notified and trained on significant changes.

5.3 Metrics and Reporting

- Key metrics (e.g., data quality scores, retention compliance, incident rates) must be tracked and reported to governance bodies.
- Dashboards and reports must be available to support continuous improvement.
- Benchmark against industry standards and best practices.

---

6. References

- [DMBOK 2.0 – Data Management Body of Knowledge]
- [PMBOK 7th Edition]
- [GDPR, SOX, PCI DSS, ISO 27001]
- ADPA Documentation (GitHub Wiki)

Contact:
For questions or exceptions, contact the Data Governance Lead or ADPA Project Owner.

This policy is subject to periodic review and improvement in alignment with evolving business, legal, and technological requirements.