African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 4, Issue 3, 2025
Page No: 583-590
Website: https://aaasjournals.com/index.php/ajapas/index
ISI 2025: 1.126 **SJIFactor 2024: 6.752** **معامل التأثير العربي: 1.62**

Data Lifecycle as a Foundation for Building an Enterprise Information Security Policy

Musbah Abobaker Musbah *
Department of Information Systems, Faculty of Information Technology,
Aljufra University, Waddan, Libya

دورة حياة البيانات كأساس لبناء سياسة أمن معلومات مؤسسية

مصباح أبوبكر مصباح *
قسم نظم المعلومات، كلية التقنية المعلومات، جامعة الجفرة، ودان، ليبيا

*Corresponding author: musbah.musbah@ju.edu.ly

Received: July 25, 2025	Accepted: September 10, 2025	Published: September 21, 2025

Abstract:

In today's digital landscape, data security is a fundamental concern for organizations, requiring policies that extend beyond traditional technical measures. This study proposes a comprehensive information security framework based on the organizational data lifecycle, ensuring protection throughout the entire data lifecycle, from creation to destruction. By integrating key security principles—confidentiality, integrity, and availability—into each phase, the framework mitigates risks such as unauthorized access, data loss, and regulatory non-compliance. The research employs an analytical approach, drawing on international standards such as ISO/IEC 27001 [1] and NIST SP 800-53 [2], as well as benchmarking tools and case studies. Findings highlight the importance of lifecycle-driven security policies, institutional governance, and adaptive strategies to counter emerging cyber threats. The study offers practical recommendations for policy implementation, contributing to more robust and resilient organizational security practices.

Keywords: Information Security, Data Lifecycle, Policy Framework, Iso/Iec 27001, Nist Sp 800-53, Data Governance.

الملخص

في ظل المشهد الرقمي الحالي، تُعدّ أمن البيانات مسألة جوهرية بالنسبة للمؤسسات، مما يتطلب سياسات تتجاوز التدابير التقنية التقليدية. تقترح هذه الدراسة إطارًا شاملاً لأمن المعلومات يستند إلى دورة حياة البيانات التنظيمية، لضمان الحماية طوال دورة حياة البيانات، من الإنشاء إلى الإتلاف. ومن خلال دمج المبادئ الأساسية للأمن—السرية، والسلامة، والتوافر—في كل مرحلة، يساهم هذا الإطار في التخفيف من المخاطر مثل الوصول غير المصرح به، وفقدان البيانات، وعدم الامتثال التنظيمي. تعتمد الدراسة على منهج تحليلي، مستندةً إلى المعايير الدولية مثل ISO/IEC 27001[1] و NIST SP 800-53 [2]، بالإضافة إلى أدوات القياس المرجعي ودراسات الحالة. وتُبرز النتائج أهمية السياسات الأمنية المستندة إلى دورة الحياة، والحوكمة المؤسسية، والاستراتيجيات التكيفية لمواجهة التهديدات السيبرانية الناشئة. وتقدم الدراسة توصيات عملية لتنفيذ السياسات، مما يسهم في تعزيز ممارسات الأمن المؤسسي وجعلها أكثر قوة ومرونة.

الكلمات المفتاحية: أمن المعلومات، دورة حياة البيانات، إطار السياسات، ISO/IEC 27001، NIST SP 800-53، حوكمة البيانات.

Introduction

Data represents the most sensitive and strategic resource in the modern digital business environment. While data enables organizations to make knowledge-based decisions, it also exposes them to increasing risks due to the rapid development of cyber-attacks and intrusion techniques. Given this reality, there is an urgent need for institutional information security policies that extend beyond technical aspects to a precise understanding of the data lifecycle within an organization. Each phase of data—from creation to destruction—entails specific security risks and challenges that require tailored controls and procedures.

This study aims to develop a systematic framework for building a comprehensive information security policy based on the organizational data lifecycle. The goal is to create a policy that is more integrated and realistic, capable of mitigating security threats such as tampering, leaks, data loss, or privacy violations. The study employs an analytical approach combined with benchmarking tools and case studies, supported by a strong theoretical framework drawn from international standards such as ISO/IEC 27001 [1] and NIST SP 800-53 [2], as well as a review of leading literature in the field. Through this approach, the study seeks to bridge the gap between theoretical principles of information security and actual practices within institutions by proposing a dynamic and effective security policy model rooted in the data lifecycle as a strategic axis.

Research Issues

The core issue addressed by this research is the lack of an integrated information security policy that aligns with the organizational data lifecycle. This gap results in fragmented protection efforts and exposes institutions to various security threats that emerge across different data phases. A deeper understanding of the complexities involved reveals several interrelated challenges:

1. Weak Integration Between Lifecycle Stages and Security Requirements: Most existing security policies focus primarily on data storage, neglecting critical phases such as creation, usage, archiving, and destruction. This narrow focus creates vulnerabilities at unprotected stages.
2. Inflexible and Centralized Security Policies: Traditional policies often adopt a one-size-fits-all approach, failing to accommodate the diversity and distribution of data across systems and departments, especially in hybrid and cloud environments.
3. Lack of Monitoring and Tracking Mechanisms: Institutions typically lack internal tools or processes to monitor the flow and status of data across its lifecycle. This absence hinders the effective application of phase-specific controls.
4. Institutional Disconnect Between Business Functions and Security Units: Security measures are often developed in isolation from business operations, leading to conflicts between usability and protection, and weakening organizational resilience.
5. Absence of Clear Data Governance Standards: Without defined responsibilities, roles, and policies for data ownership and stewardship, enforcing security becomes inconsistent and reactive.
6. Escalating Threat Landscape Targeting Lifecycle Gaps: Modern cyber threats increasingly exploit transitional phases of data, such as during transmission or temporary storage. Static security models fail to adapt to these dynamic risks.

This research thus aims to address these challenges by constructing a flexible and lifecycle-aware security framework that synchronizes policy enforcement with the actual flow of institutional data.

Literature Review

In recent academic and professional discourse, the data lifecycle has gained prominence as a foundational concept for developing security frameworks. Several key contributions highlight the necessity of integrating protection strategies at each phase of data handling.

1. Integrated Models of Lifecycle-Based Security

- Musbah (2024) proposed a four-dimensional model involving data classification, role definition, IT infrastructure requirements, and alignment of business goals with protection strategies. Drawing on ISO/IEC 17799 and ITIL, the model supports adaptive application across various institutional structures.
- Zhang et al. (2022) designed a privacy protection framework that utilizes access control, encryption, monitoring, and secure disposal. Their phased approach enables proactive security management and ensures regulatory compliance.

2. Data Classification as a Foundational Step

- Tankard (2023) emphasized that effective data classification enables automation in applying access control and data loss prevention (DLP) strategies. This approach enhances auditability and supports legal compliance, especially under GDPR and HIPAA.
- Tipton & Krause (2007) further reinforced the role of classification in facilitating risk-based security decisions, suggesting that without categorization, security policies lack precision and enforceability.

3. Cloud Computing and Lifecycle Security

- Chaoui et al. (2023) argued that securing cloud environments requires comprehensive policies that transcend data-at-rest protection. Their proposed framework supports end-to-end data lifecycle management in volatile and distributed infrastructures.
- von Solms & van Niekerk (2013) introduced a broader cyber-security lens, advocating for "security by design" across the lifecycle, especially in environments susceptible to advanced persistent threats (APTs).
- Whitman & Mattord (2022) emphasized the interplay between governance and security effectiveness. Their research points out that lifecycle policies must be dynamic, context-aware, and guided by executive support.
- NIST (2018) and ISO/IEC 27001 (2022) frameworks offer essential guidance for aligning lifecycle policies with best practices. These standards call for continuous monitoring, incident response, and policy revision mechanisms.

Summary of Literature Findings

The reviewed literature converges on the view that embedding security controls into every phase of the data lifecycle fosters a more resilient, compliant, and strategically aligned security posture. The lifecycle approach not only mitigates technical risks but also bridges organizational silos, enabling holistic information governance. This study builds on these insights to develop a practical, standards-aligned model tailored for modern institutional contexts.

Research Objective

- **General Objective**

To develop a scientific and applied framework for an institutional information security policy based on different phases of the data lifecycle.

- **Specific Objectives**
  - Analyze the comprehensive concept of the data lifecycle.
  - Associate each lifecycle stage with its specific security requirements.
  - Examine deficiencies in traditional security policies.
  - Assess international models and standards for applicability.

- **Applied Objectives**
  - Design an integrated information security policy model.
  - Propose institutional procedures for activating security policies.
  - Test the proposed framework through a case study.
  - Provide practical, applicable recommendations.

Theoretical Framework

The theoretical framework of this study integrates four foundational concepts—data lifecycle, information security, data governance, and risk management—to establish a comprehensive basis for developing a security policy rooted in the dynamic progression of institutional data. These components are interconnected and essential for creating an effective, responsive, and standards-aligned information security policy.

- Data Lifecycle: This concept outlines the sequential phases through which data passes—from creation to storage, usage, archiving, and destruction. Each phase involves distinct processes, stakeholders, and security considerations. Understanding these phases allows organizations to tailor protection mechanisms specific to each point in the lifecycle. For instance, during data creation, classification and validation are essential, whereas secure deletion is critical during the destruction phase.
- Information Security: At its core, information security encompasses the principles of confidentiality, integrity, and availability (CIA). These principles must be applied across all lifecycle phases to ensure that data is protected against unauthorized access, tampering, or loss. Effective information security is not static but evolves alongside data as it transitions between phases and contexts.
- Data Governance: Governance refers to the structures, policies, and roles responsible for overseeing data management and protection. It involves assigning ownership, defining accountability, and establishing policies that guide secure data usage and compliance. Governance ensures that data security is not limited to technical solutions but includes procedural and administrative controls as well.
- Risk Management: This element focuses on identifying, evaluating, and mitigating risks associated with data throughout its lifecycle. Each phase presents unique vulnerabilities—such as interception during transmission or residual data after deletion—that must be anticipated and addressed proactively. Risk management frameworks allow organizations to prioritize resources and responses based on threat likelihood and impact.

Collectively, these theoretical pillars form the foundation of a lifecycle-oriented security policy. They provide a structured lens through which institutions can analyze existing gaps, design targeted controls, and foster a culture of security and accountability across all levels.

Research Methodology

- Type of Research: Descriptive analytical study with an applied approach.
- Methods: Content analysis, benchmarking, case studies, and interviews.
- Analysis: Linking lifecycle stages with security controls, identifying vulnerabilities, and building a comprehensive model.

Data Lifecycle Analysis and Its Link to Security Policies

The data lifecycle consists of several distinct phases, each requiring specialized security measures to ensure confidentiality, integrity, and availability. The alignment of security policies with these phases enhances institutional resilience and regulatory compliance. Below is an expanded overview of each phase and the corresponding security considerations:

- Creation Phase: This phase involves the initial generation or acquisition of data. Security at this stage focuses on data classification, source authentication, and integrity verification. Institutions must define metadata standards and tagging mechanisms to ensure that sensitive data is identified and labeled correctly from the start. Policies should also include validation steps to ensure the authenticity and reliability of the sources generating the data. This proactive labeling plays a critical role in automating downstream security protocols such as encryption and access controls.
- Storage Phase: Once data is created, it must be stored securely. Storage security involves the use of encryption (both at rest and in transit), implementation of access control mechanisms, and configuration of redundancy through secure backup systems. Data must be stored in accordance with regulatory standards like GDPR or HIPAA, and storage locations should be evaluated periodically to detect potential vulnerabilities. This phase also encompasses database hardening and use of storage firewalls to protect against unauthorized access.
- Usage Phase: During this phase, data is accessed, shared, and modified. Security policies must govern acceptable use, role-based access, logging of activities, and protection during data transmission. Institutions should deploy intrusion detection systems and enforce policies related to secure collaboration, particularly when dealing with third parties. Endpoint security and data masking techniques are also relevant in this phase, especially when sensitive data is used in non-production environments.
- Archiving Phase: Data that is no longer actively used must be archived properly to maintain long-term integrity and accessibility. Policies here should define clear retention schedules based on legal, regulatory, and organizational requirements. Archived data must be stored in formats that ensure readability over time and protected against unauthorized access or alteration. Additionally, regular reviews of archived data should be conducted to determine if retention is still justified or if secure deletion is warranted.
- Destruction Phase: Eventually, data must be disposed of in a manner that guarantees it cannot be recovered or misused. Secure destruction policies include cryptographic erasure, physical destruction of media, and detailed documentation of the process. Institutions should also define criteria for data deletion eligibility, ensuring that all copies—including those on backup or shadow systems—are permanently and verifiably destroyed.

Together, these lifecycle-specific policies contribute to a robust governance framework that ensures data is managed securely from inception to disposal. A well-structured lifecycle policy not only addresses technical controls but also clarifies roles and responsibilities across departments, reducing ambiguity and enhancing accountability.

Proposed Model for Organizational Information Security Policy Based on the Data Lifecycle

Traditional information security policies often emphasize infrastructure protection without adequately addressing the data itself—the asset that is most frequently targeted. The modern digital environment necessitates a shift toward data-centric security strategies. This section proposes a comprehensive policy model that embeds specific security controls and procedures at each stage of the data lifecycle, ensuring continuous and contextual protection.

- Key Model Principles
  - Lifecycle-Driven Security Policy: The core of the model is a security strategy designed around the data lifecycle. Instead of applying generic controls, the policy is decomposed into discrete stages—creation, storage, usage, archiving, and destruction—with tailored protections for each. This approach ensures proactive mitigation of vulnerabilities as data progresses through its lifecycle.
  - Comprehensive and Specialized: The policy framework is detailed and precise, providing context-specific protocols and responsibilities for each stage. By integrating both technical and administrative safeguards, the model goes beyond surface-level compliance to provide meaningful, operational security.

- Flexibility and Adaptability: Recognizing the evolving nature of threats, the model is designed to be dynamic. It allows for regular updates based on technological advancements, emerging threat intelligence, and organizational changes. This adaptability is crucial for maintaining long-term effectiveness in dynamic environments such as hybrid and multi-cloud infrastructures.
- Alignment with International Standards: The policy is anchored in globally recognized standards like ISO/IEC 27001, NIST SP 800-53, and GDPR. These standards provide a validated framework that ensures legal compliance, enhances audit readiness, and aligns institutional practices with global best practices.

- Security Policies by Data Lifecycle Stage
- Creation Phase: Policies in this phase address data classification, validation of sources, and initial integrity checks. Data should be labeled based on sensitivity and regulatory requirements from the moment it is created. In addition, organizations must document data ownership, determine access permissions, and enforce secure generation protocols to prevent insertion of malicious or unauthorized content.
- Storage Phase: Security controls for stored data include encryption (AES-256 or equivalent), granular access control models (e.g., RBAC or ABAC), and automated backup systems with off-site redundancy. Data storage systems should be subject to vulnerability scanning and patch management. This stage also includes monitoring for anomalies and unauthorized access, often using tools like SIEM (Security Information and Event Management).
- Usage Phase: Data use policies govern how data is accessed, edited, and shared. Multifactor authentication, continuous monitoring, and secure communication protocols (e.g., TLS 1.3) should be enforced. This phase includes the use of data anonymization and pseudonymization where applicable, particularly for personally identifiable information (PII). Organizations should also maintain detailed audit logs to ensure accountability.
- Archiving Phase: Data that is infrequently accessed should be moved to secure archive systems with long-term readability. Policies must define legal and operational retention periods and include mechanisms for periodic validation of archived data integrity. Encryption at rest and metadata tagging are essential to ensure compliance and retrieval efficiency. Archived data should be isolated from active systems to reduce attack surfaces.
- Destruction Phase: The final stage involves secure deletion or physical destruction. Data destruction must follow documented procedures, using industry best practices like DoD 5220.22-M or NIST 800-88 guidelines. All copies of the data, including those in backups or logs, must be erased or destroyed to prevent recovery. Audit trails should be maintained to document the destruction process for compliance verification.

This proposed model facilitates a holistic and resilient security posture that prioritizes the data itself throughout its lifecycle. It promotes coordinated action among technical teams, compliance officers, and business units, ensuring that data protection is embedded into every organizational process rather than being treated as a standalone function. In doing so, institutions can better anticipate risks, comply with regulations, and maintain trust with stakeholders.

CASE STUDY: Survey-Based Assessment of Data Lifecycle Security Practices.

1. General Structure of the Data

- Number of responses: Approximately 50.
- Job categories: Include faculty members, registrars, deans, department heads, and administrative staff.
- Departments: Distributed across administration, academic departments, and examination offices.
- Survey questions: Cover the stages of the data lifecycle—creation, storage, usage, archiving, deletion, and governance.

2. Quantitative Results

A numeric scale (0 to 2) was used to measure the presence or implementation of security practices at each stage of the data lifecycle and the table 1 shows the approximate averages used at each stage.

Table 1: the approximate averages.

Data Lifecycle Stage	Average Score	General Comment
Creation	1.2	Weak systems for secure data creation.
Storage	1.0	Lack of advanced technologies or robust storage policies.
Usage	0.9	Limited training on secure data usage.
Archiving	0.0	Almost no clear archiving policies or tools.
Deletion	0.0	No defined mechanisms for secure deletion or documentation.
Governance	0.0	Near-total absence of institutional data governance.

These results suggest that institutional focus is limited to creation and storage, while critical stages like archiving, deletion, and governance are largely neglected. The relation between Average Implementation of Security Policies and Data Lifecycle Stages show plow in the figure (1) .

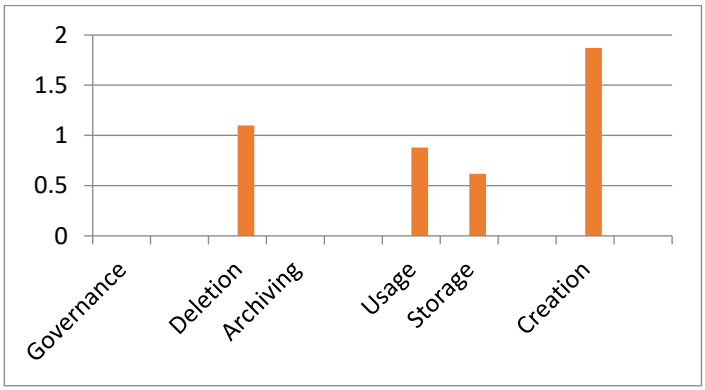

Figure 1: Average Implementation of Security Policies across the Data Lifecycle Stages

3. Qualitative Insights from Participant Comments

Common Challenges:

- Lack of clear data protection policies.
- Absence of training and awareness programs.
- Weak technical infrastructure and systems.
- Undefined roles and responsibilities.

Frequent Suggestions:

- Launch training and awareness initiatives.
- Develop unified systems with security protocols.
- Establish regulatory frameworks defining access and protection.
- Upgrade equipment and adopt modern technologies.

Results

The survey results strongly support the findings in the Word document study, which emphasizes:

- A significant gap between data lifecycle stages and applied security policies.
- Weak institutional governance and unclear accountability.
- The need for a flexible, integrated security model that spans all lifecycle stages.

The study proposes a model based on the data lifecycle, which aligns perfectly with the challenges revealed in the survey—especially the complete neglect of archiving and deletion stages.

Analytical Recommendations

1. Design tailored information security policies for each stage of the data lifecycle.
2. Implement regular training programs for all staff on data security.
3. Activate institutional governance through clear regulations and role definitions.
4. Adopt international standards like ISO/IEC 27001 and NIST SP 800-53 for compliance and quality.
5. Conduct periodic reviews of systems and policies to ensure updates and responsiveness to emerging threats.

References

[1] ISO/IEC 27001 (ISO, 2022): Information security, cybersecurity, and privacy protection — Information security management systems — Requirements.

[2] NIST Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.

[3] European Union General Data Protection Regulation (GDPR), 2018.

[4] Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

[5] von Solms, R., & van Niekerk, J. (2013). "From Information Security to Cyber Security." Computers & Security, 38, 97–102.

[6] Tipton, H. F., & Krause, M. (2007). Information Security Management Handbook (6th ed.). Auerbach Publications.

[7] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018.

[8] M. A. Musbah, "Information Security Management Requirements Model Through Data Life Cycle," *The International Journal of Engineering & Information Technology (IJEIT)*, vol. 6, no. 1, Jun. 2024.
[9] H. Zhang, S. Cheng, Q. Cai, and X. Jiang, "Privacy security protection based on data life cycle," in *Proc. 2022 World Automation Congress (WAC)*, Oct. 2022.
[10] C. Tankard, "Data classification – the foundation of information security" ,Network Security, vol. 2015, no. 5, pp. 8–11, May 2015.
[11] K. Chaoui, N. Kabachi, N. Harbi, and H. Badir, "Comprehensive Data Life Cycle Security in Cloud Computing: Current Mastery and Major Challenges," in New Technologies, Artificial Intelligence and Smart Data, Communications in Computer and Information Science (CCIS), vol. 1824, pp. 195–206, Nov. 2023.

Appendix 1: Questionnaire Questions.

Section One: General Information

1. Department/Division Name (Optional)
2. Job Title (----------)
3. Number of years of experience in the field of IT/Data: (---------)

Section Two: Assessment of Data Security Practices at Each Stage of the Lifecycle
Please select the most appropriate answer based on the reality of your institution:

Item	Question	Yes	No	Partially
1	Are data classified at the time of creation?	☐	☐	☐
2	Are data owners and their responsibilities defined?	☐	☐	☐
3	Are data encrypted during storage?	☐	☐	☐
4	Are there different access privileges to data?	☐	☐	☐
5	Are data operations logged and tracked (Logs)?	☐	☐	☐
6	Are there institutional procedures for archiving old data?	☐	☐	☐
7	Are archived data reviewed periodically?	☐	☐	☐
8	Is there a clear policy for securely deleting data?	☐	☐	☐
9	Are employees trained on secure data handling?	☐	☐	☐
10	Does the institution apply international standards such as ISO 27001?	☐	☐	☐

Section Three: Open-Ended Questions (Optional)

1. What are the main challenges you face in protecting data across its different stages?
2. What suggestions do you consider necessary to improve data security in your institution?