Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: May 2025
Review: April 2028

Data Handling, Access, and Storage - Policy & Procedures

1.0 Purpose

1.1 This policy provides clear guidelines for how AUIB manages and stores data. It aims to protect the confidentiality, integrity, and availability of data from creation until it's no longer needed.

2.0 Scope

2.1 This policy applies to anyone who may access, handle, view, or store data within AUIB's infrastructure; this includes students, faculty, staff, and any third-party service providers.

2.2 The objectives of this policy are to ensure the protection, integrity, and efficient management of data within AUIB. Data security is a priority, with measures in place to protect sensitive information from unauthorized access or disclosure. AUIB maintains data integrity by validating the accuracy, consistency, and reliability of stored data through processes such as error correction and version control. Data accessibility is also emphasized, ensuring that authorized users can easily retrieve information, typically through effective indexing.

2.3 To optimize storage, AUIB implements guidelines for removing duplicates, compressing data, and archiving efficiently, which contributes to cost reduction. The policy supports scalability and flexibility by adopting technologies that accommodate growing data volumes and evolving institutional needs. In addition, AUIB complies with industry standards for data retention and disposal, specifying how long data should be kept and how it should be securely discarded.

2.4 Standardization is promoted across departments through the use of common formats and naming conventions, enhancing collaboration and data sharing. All practices are aligned with industry standards, security best practices, and compliance requirements. This policy applies to anyone who may access, handle, view, or store data within AUIB’s infrastructure, including students, faculty, staff, and third-party service providers.

3.0 Definitions

3.1 Access controls - security measures that regulate who can access data and which access level they have, based on authentication, authorization, and privilege management.

3.2 Audit trails - a record of activities and events related to data storage, providing a chronological trail of who accessed the data and when.

3.3 Availability - the accessibility and readiness of data for authorized users when needed, ensuring it is reliably and promptly accessible.

3.4 Backup - making copies of the data to protect it against loss, corruption, or accidental deletion.

3.5 Compliance - adherence to legal, regulatory, and industry standards pertaining to data storage, privacy, security, and other relevant areas.

3.6 Confidential data - information that is considered sensitive and should be protected from unauthorized access or disclosure, to maintain its confidentiality.

3.7 Data classification - data must be classified based on its sensitivity and importance, making sure it gets the right level of protection and preservation.

3.8 Data deduplication - the process of identifying and eliminating duplicate copies of data to optimize storage space and reduce storage costs.

3.9 Data format conversion - data transformation from one format to another to secure compatibility and/or to meet specific storage requirements.

3.10 Data disposal - deleting data while making sure it cannot be recovered when it is no longer needed.

3.11 Data lifecycle - the stages that data goes through from creation/ acquisition to disposal, including creation, storage, retrieval, modification, archival, and disposal.

3.12 Data migration - transferring data from one storage system, repository, or format to another one, typically to upgrade systems.

3.13 Data ownership - the identification of individuals or entities responsible for the data, including its accuracy, security, and compliance with applicable policies and regulations.

3.14 Data privacy - the protection of personal and sensitive information from unauthorized access, use, or disclosure in accordance with privacy laws and regulations.

3.15 Data retention - the period for which data should be stored and retained, based on legal, regulatory, or business requirements.

3.16 Data storage - storing data in a structured manner for future retrieval and use.

3.17 Data validation - ensuring the accuracy, completeness, and consistency of data through validation and verification procedures.

3.18 Encryption - converting data into an unreadable format using cryptographic techniques to protect it from unauthorized access.

3.19 Integrity - the accuracy, consistency, and reliability of data throughout its lifecycle, ensuring it remains unaltered and complete.

4.0 Policy

4.1 A culture of responsibility for handling data is promoted by clearly identifying roles and providing necessary training.

4.2 The entire lifecycle of data, from creation to disposal, is managed with appropriate controls and safeguards.

4.3 Open communication among team members is encouraged to ensure effective data management.

4.4 Regular improvements to data storage methods, aligned with new technology and auditing practices, are prioritized.

4.5 Data security, privacy, and confidentiality are maintained through strong security measures, compliance with privacy policies, and strict access controls.

4.6 Compliance with industry standards and regulatory requirements is mandatory, with regular audits to ensure adherence.

4.7 Data classification and retention are based on sensitivity and regulatory requirements, with secure disposal methods in place.

4.8 Backup procedures ensure data availability and recoverability, with regular testing to verify integrity.

4.9 Storage infrastructure is designed to be scalable and optimized for performance, with continuous monitoring and resource management.

5.0 Procedures

5.1 IT leadership/management sets the strategic direction and goals for storage management within the organization; establishes and communicates the IT Storage Standard policy to all relevant stakeholders; allocates resources for the implementation and maintenance of storage infrastructure.

5.2 Data management/archiving team classifies and categorizes data based on its value and retention requirements; develops and enforces data retention policies and procedures; monitors and manages data backups and restoration processes.

5.3 Security administrator establishes and enforces security controls for data stored within the storage systems; monitors storage systems for security breaches, unauthorized access, or data loss; develops and maintains encryption mechanisms for sensitive or confidential data.

5.4 Backup/recovery team designs and implements backup/recovery strategies for data stored within the storage systems; develops backup schedules and ensure regular backups are performed according to policies; monitors backup processes and verify the integrity of backup data.

5.5 The compliance and legal team collaborate with other teams to ensure storage policies comply with data protection regulations and industry-specific requirements; monitors and assesses changes in data protection and retention regulations; conducts regular audits and assessments to validate compliance with storage standards.

5.6 End users/application owners manage data and storage usage efficiently, following defined practices; collaborate with storage admin to address storage-related issues, optimize storage usage; comply with data retention and archiving guidelines for proper management and storage of data.

Storage Capacity Planning

5.7 The IT leadership/management plans and allocates sufficient storage resources to accommodate projected data growth.

5.8 The IT leadership/management monitors storage utilization regularly to identify potential capacity constraints and take proactive measures to address them.

Storage Provisioning

5.9 The IT leadership/management determines storage requirements for different applications, users, and systems.

5.10 The IT leadership/management allocates and provides storage resources based on defined criteria, such as performance, availability, and data classification.

Data Classification and Categorization

5.11 The data management/archiving team classifies data based on its sensitivity, criticality, and regulatory requirements.

5.12 The data management/archiving team applies appropriate storage policies, access controls, and backup strategies based on data classification and categorization.

Data Backup and Recovery

5.13 The backup/recovery team develops a backup strategy that aligns with data retention and business continuity objectives.

5.14 The backup/recovery team backs up data according to defined backup schedules, considering the importance of data.

5.15 The backup/recovery team verifies the integrity of backup data through regular testing and validation.

5.16 The backup/recovery team implements procedures for data restoration in the event of data loss or system failures.

Data Archiving and Retention

5.17 The data management/archiving team defines data retention policies based on regulatory and business requirements.

5.18 The data management/archiving team identifies data that needs to be archived for long-term storage and retrieval.

5.19 The data management/archiving team monitors data retention and archival processes, ensuring compliance with defined policies.

Storage Security and Access Controls

5.20 The security administrator implements access controls and permissions to ensure authorized access to stored data.

5.21 The Security administrator regularly reviews and updates access controls to align with changes in user roles, responsibilities, and data classification.

Storage Performance Monitoring and Optimization

5.22 The IT leadership/management continuously monitors storage performance metrics, including I/O throughput, latency, and response times.

5.23 The IT leadership/management identifies and addresses storage performance bottlenecks or capacity constraints.

Compliance and Audit

5.24 The compliance and legal team regularly reviews and assesses storage practices to ensure compliance with regulatory and industry standards.

5.25 The compliance and legal team conducts internal audits to verify adherence to storage policies and security controls.

5.26 The Compliance and legal team documents audit findings, address any identified gaps or non-compliance issues, and implement corrective actions.

Related Policies and Documents

Data Privacy Policy
Information Security Policy