UNIVERSITY OF BAHRAIN

Data, Information and Document Classification Policy

Authority / Owner of Policy: Director General of Administrative Services

Effective: October 19, 2025

Table of Contents

POLICY INFORMATION

Title:	Data, Information and Document Classification Policy
Policy Description:	This policy is a comprehensive regulatory framework for the protection of data, information and documents at the University of Bahrain by classifying them into four levels (Highly Classified, Classified, Restricted/Limited, Public) and linking each level to appropriate protection controls, in a way that ensures effective protection of all academic, administrative, financial and research data, information and documents at the University.
Policy Scope:	☐ Academic ☐ Administrative ☐ Research ☐ Student ☒ general
Policy Status	☒ New policy ☐ Revision of existing policy
Approval Authority:	University of Bahrain Council
Authority/ Owner of Policy:	Director General of Administrative Services
Approval Date:	19 October 2025
Effective Date:	19 October 2025
Approval Date of Last Revision:	19 October 2025
Date of Next Revision:	October 2030
University Council Decision No.:	557/1/2025
Document No.:	UOB-GDAS-PO-007
Related Documents:	Law No. (30) of 2018 issuing the Personal Data Protection Law, Law No. (16) of 2014 on the Protection of State Information and Documents, Law No. (60) of 2014 on Information Technology Crimes and Information Security Policies observed at the University

Policy Stakeholders

☐ President

☐ Vice Presidents

☐ Legal Advisor

☐ Deans

☐ Directors

☐ Faculty members

☐ Students

☐ Admin Staff

☒ All University Affiliates

1 Definitions

In implementing the provisions of this policy, the following words and phrases shall have the meanings assigned to them below, unless the context requires otherwise:

University:	University of Bahrain.
Data, Information, and Documents:	All data, information, and documents, whether textual, paper, or electronic, produced or circulated by the University through its systems, applications, and technologies.
Classification:	The process of evaluating data, information, and documents according to their sensitivity and significance, and then assigning an appropriate level of protection to ensure their confidentiality, integrity, and availability.
Classification Level:	The defined level of sensitivity and significance of data, information, and documents within the University.
Labeling:	The process of placing a clear physical or electronic marker on issued or stored documents or information, indicating their classification level and facilitating the identification of requirements for handling them.
Data, Information, and Document Owner:	The administrative or academic body (college, deanship, department, center, or other organizational units) that creates data, information, and documents and bears primary responsibility for

	their accuracy, quality, classification, and the implementation of their protection controls.
Data, Information, and Document User:	Any individual affiliated with the University or dealing with it who is granted access to data, information, and documents and the power to use them within the limits required by their job duties or responsibilities.

2 Policy Purpose

This policy aims to protect data, information, and documents, ensure their confidentiality, protect them from unauthorized access, and comply with applicable laws and policies in the country.

3 Policy Scope

This policy applies to all data, information, and documents stored, processed, or circulated at the University, whether paper or electronic, including data exchanged with third parties such as suppliers, contractors, or external partners. The appendices accompanying this policy shall be considered an integral part thereof and have the same binding force.

4 Policy Statement

4.1 Classification Levels

Data, information, and documents at the University are classified into one of the following four levels, based on an assessment of the impact of unauthorized disclosure, as detailed in Appendix (1) to this policy:

4.1.1 Level 1: Highly Classified

Data, information, and documents are classified at this level if unauthorized disclosure would cause serious harm to national security or the higher interests of the State or the

University. Access to this level is restricted to individuals specifically authorized by the University President.

4.1.2 Level 2: Classified

Data, information, and documents are classified at this level if unauthorized disclosure would harm the interests of the University or the State, or constitute a serious violation of individual privacy. Access to this level is restricted to authorized personnel whose work nature require it, based on the authority granted by their job role.

4.1.3 Level 3: Restricted/Limited

Data, information, and documents intended for internal use only within the University are classified at this level. This is the default level for most data, information, and documents not classified for public release. Access to this information is permitted for all members of the University affiliates unless the owner of the data, information, and documents imposes additional restrictions.

4.1.4 Level Four: Public

This level includes data, information, and documents that have been approved for public release and are available to everyone without restrictions.

4.2 Classification Criteria

Data, information, and documents are classified according to criteria designed to ensure their confidentiality, integrity, and availability, based on the following:

1- Impact Assessment: Classification is based on the impact of unauthorized disclosure on the University's public interest, its smooth operation, or the interests or privacy of its members or stakeholders, to determine whether the information warrants being classified under a specific level of confidentiality.

2- Factors Affecting Classification: The classification level is also determined according to the nature and content of the data, information, and documents, their source, the beneficiary, and relevant legal and regulatory requirements.

4.3 Security Requirements by Classification

The following security requirements are adopted by the University to protect data, information, and documents:

1- General Requirements: Relevant departments within the University are committed to implementing basic controls for protecting data, information, and documents. This includes virus prevention, activating firewall systems, implementing periodic security updates, and performing regular backups to ensure business continuity.

2- Requirements Specific to Highly Sensitive Data, Information, and Documents (Highly Classified and Classified): In addition to the general requirements stipulated above, relevant departments are committed to encrypting data, information, and documents during storage and transmission, imposing strict and logical access controls at the system and application levels, storing hard copies in secure, locked cabinets within secure locations, recording and monitoring all access attempts and reviewing them periodically, and using specialized systems and technologies to prevent data, information, and document leaks in all forms.

3- Labeling: Data, information, and documents classified according to their classification level must be clearly labeled and marked using approved physical or electronic means within the University. Labeling standards and formats are detailed in Appendix (2) to this Policy.

4.4 Lifecycle Management

The University is committed to managing the lifecycle of data, information, and documents from creation to destruction, in accordance with the following guidelines:

1- Classification upon Creation: The owner of the data, information, and documents is responsible for classifying newly created or received data to determine its sensitivity level and apply appropriate security controls according to established policies.

2- Periodic Review: Classifications are reviewed by the document owner when significant changes occur in the nature or use of the data, information, and documents to ensure the continued suitability of the classification level.

3- Secure Destruction: Classified data, information, and documents are securely destroyed, whether paper -using approved destruction methods- or electronic -using final erasure technologies-, in a manner that ensures they cannot be recovered or reused.

5 Roles and Responsibilities

Entity	Responsibility
University President:	Adopting this Policy by the University Council, oversee its implementation, and providing the necessary resources to protect data, information, and documents.
Information Technology and Digital Education Department:	Implementing the necessary technical controls to protect data, information, and documents, managing access privileges, monitoring networks and systems, and providing technical support.
Data, Information, and Document Owner:	Classifying data, information, and documents under their responsibility, defining access requirements, granting permissions, and conducting periodic reviews of the classification and permissions.
Data, Information, and Document User:	Adhering to the provisions of this Policy, handling data, information, and documents according to their classification level, protecting their passwords, and immediately reporting any incident affecting the security of data, information, and documents.
Internal Audit Office:	Monitoring compliance with the provisions of this Policy by conducting periodic reviews of the mechanisms for classifying, protecting, and safeguarding data, information, and documents, and submitting periodic reports on the review results and recommendations to the University President.
University Training Entities:	Organizing periodic training and awareness programs targeting all its affiliates, including faculty, administrators, and students, to raise awareness of the importance of classifying data, information, and documents and the controls for protecting them, and to clarify the procedures to be followed for handling them according to the approved classification level, ensuring full compliance with the provisions of this Policy.

6 Policy Procedures

1. **Classification Procedures**: The owner of data, information, and documents is obligated to evaluate new or received data, information, and documents, determine the appropriate classification level, assign specific labels, document the decision in an official record, and inform relevant users of the requirements for handling the data.
2. **Access Granting Procedures**: Requests for access to data, information, and documents are submitted according to the procedures approved by the relevant authority. The owner of the data, information, and documents reviews these requests for approval or rejection based on actual need. The Information Technology and Digital Education Department is responsible for implementing the granted access permissions on the University's approved electronic systems, documenting all transactions in official records, and signing a non-disclosure agreement with third parties.
3. **Periodic Review Procedures**: The owner of data, information, and documents reviews the granted access permissions periodically, and these permissions are revoked as soon as they are no longer needed. Also, the classification of data, information, and documents is reviewed when there are material changes in their nature or uses, in accordance with legal changes. The results shall then be documented, and the necessary corrective actions are taken.
4. **Breach Reporting Procedures**: Users or owners of data, information, and documents must immediately report any breach or suspected breach to the Information Technology and Digital Education Department through official channels within 24 hours of discovery. The data, information, and document owner is responsible for overseeing the documentation of all breaches or violations, including identifying their causes, consequences, and corrective actions, in coordination with the Information Technology Department. If the incident entails legal obligations requiring notification of the relevant legal authorities under applicable laws, senior management shall take the necessary actions within the prescribed timeframes.
5. **Incident Response Procedures**: Upon receiving a report, the Information Technology and Digital Education Department assumes responsibility for the initial response to security incidents related to data, information, and documents. This includes taking immediate measures to contain the incident and mitigate its direct effects. When necessary, a specialized team from the department will be formed to conduct a detailed investigation of the incident, identify its causes and effects, and propose the necessary corrective actions. A detailed report of the investigation's

findings and recommendations is then submitted to the Director General of Administrative Services for appropriate decision-making and to address any resulting obligations or subsequent measures.

6. **Secure Destruction of Data, Information, and Documents Procedures:** When the purpose for data retention has been fulfilled, or when the legal or regulatory retention period has expired, it must be disposed of using secure and approved destruction methods that ensure it cannot be recovered or reused. This includes:
   - For paper data: Destruction using security shredders or through an approved shredding service provider.
   - For digital/electronic data: Secure deletion using advanced data wiping software or physical destruction of the storage media if necessary.

7 Final Provisions

Violation of the provisions of this Policy shall be grounds for disciplinary or administrative accountability, as the case may be, in accordance with the regulations and rules applicable at the University, without prejudice to the legal liability established under the relevant laws.

8 Contact Information

To provide further assistance in implementing this policy, or any related questions can be directed to the office of the Director General of Administrative Services:

Email: dgas@uob.edu.bh

Contact #: 17438882

Annex No. (1)

Examples and Access Controls

Classification Level	Examples	Access Controls
Level 1: Highly Classified	• Data, information, and documents related to national security in which the University is involved. • Highly sensitive data pertaining to senior leadership figures. • Master passwords for critical infrastructure. • Emergency and cybersecurity plans.	Access is restricted to individuals named by the University President, data, information and documents are encrypted during storage and transfer, and paper copies are kept in locked safes.
Level 2: Classified	• Sensitive personal data, information, and documents of students and staff (health or biometric). • Detailed academic records. • Research findings and evaluations prior to publication. • Strategic contracts and agreements. • Detailed financial data and information prior to being open to the public. • Examinations.	Restricted access for authorized users based on the nature of their work, with permissions granted according to job roles, encryption of data, information and documents during transfer and storage, and adoption of strict sharing controls.
Level 3: Restricted/Limited	• Data, information, and documents intended for internal correspondence. • Minutes of closed meetings. • Initial drafts of policies. • Internal administrative reports. • Internal employee contact information.	Access is available to all members of the University unless the owner of the data, information, and documents imposes additional restrictions, with the application of limited sharing policies and basic protection controls

Classification Level	Examples	Access Controls
		(passwords and secure storage).
Level 4: Public	• Data, information, and documents intended for public dissemination, such as information published on the University's official website. • Press releases. • Academic calendar. • Published admission requirements. • Approved general policies and regulations. • Open data, including statistics.	Open access for everyone without restrictions, with a commitment to the formal accuracy of the published content.

Annex No. (2)

Data, Information, And Documents Labeling Standards

Classification Level	Physical Labeling (Paper Documents)	Digital Marking (Electronic Documents)	E-mail	Designated Color
Level 1: Highly Classified	Visible red stamp/label bearing the phrase "Highly Classified "	Insert the phrase "Highly Classified" in Header and Footer	The subject must begin with: "Highly Classified"	Red
Level 2: Classified	Yellow stamp/label bearing the phrase "Classified "	Insert the phrase "Classified" in Header and Footer	The subject must begin with: "Classified"	Yellow
Level 3: Restricted/Limited	Blue stamp/label bearing the phrase "Limited"	Insert the phrase "Limited" in Footer	The subject must begin with: "Limited"	Blue
Level 4: Public	No special labeling required	No special labeling required	No additional information is required in the subject.	Green

Executive Notes:

1. All University departments are required to affix seals or labels to paper documents immediately upon classification.

2. Classification text will be automatically added to electronic document management systems whenever possible.

3. For data, information, and document handling and storage, the sender shall be responsible for including the classification in the subject according to the message's sensitivity level.