University of Duhok
Directorate of Information Technology (DOIT)

POLICY NAME:
Information Management and Data Security

Policy No.: UOD-POL-DOIT-021

ISSUING OFFICE: DOIT, UPLO
VERSION NO.: 01
VERSION DATE: July 1st, 2025
ORIGINAL DATE ISSUED: 10/07/2024

uplo.uod.ac
uplo.office@uod.ac

Policy Name: Information Management and Data Security

POLICY PURPOSE

The purpose of this policy is to safeguard the information assets and technology systems of the University of Duhok (UoD) from unauthorised access, modification, loss, or disclosure. It aims to ensure the confidentiality, integrity, and availability of data by complying with university policies, and relevant regulatory standards.
The university provides digital infrastructure that includes a variety of institutional electronic systems, computing services, networks, databases, management systems, and other resources (referred to as “UoD resources" generally). These resources are designed to help academic community members succeed in their academic endeavours. UoD ensures a safe and secure IT operating environment for all university community members.

RESPONSIBLE OFFICE

Directorate of IT (DOIT), The Vice President for Scientific Affairs, and the President of the University.

RESPONSIBLE EXECUTIVE

Vice President for Academic Affairs.

POLICY HISTORY

- Date of Permanent Approval: July 1st, 2025
- Date of Amendments:

APPLICABLE TO:

This policy applies to academics, staff, students, official university affiliates, and any other individuals who use the University electronic information resources or who use private

electronic information resources to conduct the University work. It encompasses all units within the university's campuses or under its administrative oversight, including the University Policy Office (UPLO) and the Directorate of IT (DOIT).

POLICY STATEMENT

Individual access rights should not be transferred, rented, shared, or otherwise made available to third parties. Access to restricted information resources is limited to those with the necessary university authorization only.
Users are responsible for any activities that occur while using information resources that have been assigned to them, and they must utilise these resources in the manner intended. Employees are encouraged to use University resources to do University work. Apart from approved access rights, University information records may only be disclosed in response to a court order or as required by law.

DEFINITIONS:

- **Information Assets:** Data, records, and other content that is stored, transmitted, or utilized through university-managed systems, including research data, student records, administrative information, academic staff details, staff information, and financial data.

- **UoD's Systems:** Information management at the University of Duhok (UoD) follows a structured approach to organizing, securing, and maintaining data throughout its lifecycle. The IT Directorate oversees critical digital systems, including **the ERP system, eUMS, university website, QA, eLearning (Moodle), Google Workspace, UoD Portal, Kurdistan Ministry of Finance System (KMFS), CCTV Data Management, Data Center, among others.**

  To ensure data security, UoD employs advanced technological solutions and strict policies to protect sensitive information from unauthorized access, breaches, or

loss. Clear access controls, well-documented processes, and continuous monitoring help maintain the integrity, confidentiality, and availability of essential university data. Additionally, comprehensive awareness programs educate staff and students on their roles in securing university information.

- **Third parties:** Any individual or organisation/party who doesn't have access rights and approval from the university senior leadership.

DATA CLASSIFICATION

Data classification involves categorising data into specific groups based on its sensitivity, importance, and the level of protection it requires. The goal is to ensure that the data is appropriately managed and protected. Common classifications include:

- **Confidential:** Restricted access, Sensitive data that could cause harm if disclosed to unauthorised entities, Such as Personal Information, Financial Information, Academic and Institutional Data, and Government and Legal Documents.
- **Internal Use Only:** Data used within the University that is not meant for public consumption. Such as Organizational and Administrative Data, Human Resources (HR) Data, Academic and Research Data, and others.
- **Public:** Information intended for public access, including general university information and non-sensitive academic content. Such as Public research papers, general university announcements, publicly accessible websites, and others.
- **Restricted Data**: Highly sensitive information that requires the highest level of protection, such as University and Academic Data, IT and System Data, HR and Staff Data, Operational and Strategic Data, and others.

RESPONSIBILITIES OF THE UNIVERSITY

As the University's electronic information resources are owned and managed by the KRG public sector, the University is responsible for monitoring and ensuring their proper use. While a culture of trust is promoted, the University may monitor systems for misuse. It is responsible for auditing all ICT systems and information assets to ensure compliance with policies. The University ensures the confidentiality and privacy of communications and data; however, in the event of a court order or authorized university administrative request, it reserves the right to inspect data in accordance with regional laws and regulations.

1. Information Management Responsibilities

The DOIT directorate is responsible for advising new and proposed systems according to QP-DOIT-01, implementing and maintaining information management systems that ensure the proper storage, classification, and security of university data. The systems mentioned above such as Data center, ERP, eUMS …etc

2. Access Management

Access management is the process of controlling and managing user access to UoD resources, such as UoD website, UoD portal, CCTV, and electronic financial systems. UoD systems access control matrix explains the individual role/responsibilities of each user within the institution's systems.
If any staff member changes their role or leaves the University, the IT Director must be informed to update access privileges immediately. The privileges must be revoked with an official letter.
Any staff member responsible for UoD systems or information that is restricted must sign the University confidentiality agreement.

3. Incident Response and Reporting

In the event of a data breach or suspected misuse of university information resources, users must immediately report the incident through the designated reporting channels. Incidents can be reported, via official phone numbers (whatsapp, viber groups), and email IT@uod.ac.

Employee Responsibilities

All employees of the University of Duhok are responsible for safeguarding job-related information and maintaining the confidentiality of sensitive data accessed during their duties. This responsibility to protect university information extends beyond active employment and continues after the conclusion of employment, including retirement. Employees must not disclose, share, or misuse any confidential information obtained during their employment. Failure to comply with these responsibilities will subject individuals to enforcement under Articles 327 and 437 of the Iraqi Penal Code No. 111 (1969).

USER RESPONSIBILITIES

1. Appropriate Use of Resources

Users of UoD systems are expected to use information assets responsibly, in accordance with the university's objectives. Access privileges should not be shared, and unauthorised attempts to gain access to restricted systems are strictly prohibited. Misuse of information resources may be subject to disciplinary action.

2. Data Protection & Compliance

- All users must respect the confidentiality of sensitive information, including student records, financial data, staff account information (academic and administrative),

personal identifiable information (PII), institutional emails, and intellectual property accounts.
- Unauthorised sharing, modification, or distribution of this information will result in serious consequences, including legal repercussions under data protection laws(Articles 327 and 437 of the Iraqi Penal Code No. 111 (1969) or updates will be referenced and enforced.)

3. Personal Use

- Limited personal use of university UoD systems is permitted, provided it does not interfere with operations, incur costs to the University, or violate UoD's policies.
- Use of resources for personal financial gain, political campaigning, or other unauthorised external activities is prohibited.

DATA SECURITY MEASURES

1. **Access Control:** All access to the university's information resources must be governed by a stringent access control **matrix** that requires user identification and authentication.
2. **Password Management:** It's recommended that all users regularly update their passwords following security guidelines. When a user departs from the university, their accounts and access must be promptly revoked. However, in certain cases such as those outlined in the **Alumni Engagement Policy**, or in other specific circumstances where continued access is deemed necessary limited account access may be granted for a defined period.
3. **Backup and Recovery:** Every system owner must maintain robust backup systems that ensure data recovery in case of system failures, breaches, or other incidents.
4. **Data Encryption**: Data must be encrypted at rest and in transit using SSL/TLS and other protocols.
5. **Network Security**: Up to date Firewalls, IDS/IPS, and network segmentation should be applied to secure traffic.
6. **Physical Security**: Restriction of physical access to servers and sensitive devices.

7. **Endpoint Security:** Install antivirus/anti-malware software, and Ensure all devices have updated software and patches.
8. **Risk Management:** Risk management involves identifying, assessing, and mitigating risks to ensure the integrity, confidentiality, and availability of data. It helps protect data from threats like unauthorised access, data breaches, and cyber-attacks.

Archiving of Records

To ensure the protection, accessibility, and proper management of administrative records, the following guidelines must be followed when archiving files:

- **Storage Methods**
  Administrative records must be securely archived using one or both of the following:
  - A secure cloud storage platform (with appropriate access controls and encryption)
  - A dedicated external storage device.
- **File Organization**
  - All files must be clearly **coded** (e.g., by department, document type, or reference number)
  - Each file should be **dated** to indicate when it was created or last modified
  - A consistent **folder structure** should be used for easy navigation and retrieval
- **Accessibility**

- Archived files must be organized in a way that makes them **easy to access** by authorized personnel when needed
- Regular checks should be conducted to ensure all files remain accessible and functional

❖ **Security and Compliance**

- Storage methods must comply with **data protection laws and university policies**
- All digital files should be stored using systems that offer **encryption, backup, and version control**
- External hard drives must be kept in **secure, access-restricted locations**

❖ **Maintenance and Updates**

- Archives must be **The data will be regularly updated and archived in accordance with this policy**
- Outdated or duplicate files should be identified and **safely removed or archived separately**

By following these steps, the University of Duhok ensures that important administrative records are securely stored, well-organized, and accessible for future reference. This practice is essential for upholding information security, supporting efficient data management, and preserving institutional knowledge.

The Kurdistan Regional Government Law Compliance

The University of Duhok adheres to the laws and regulations stipulated by the Kurdistan Regional Government and Iraq to ensure information management and data security. The following legal frameworks will be referenced in case of policy violations:

1. **Copyright Protection**
   In accordance with the Kurdistan Regional Government Copyright Law No. 17 (2012), Articles 36 and 37 will be enforced in cases of copyright infringement involving university-owned or affiliated content.
2. **Misuse of Communication Devices**
   Any improper use of the internet, mobile phones, or electronic devices is governed by the Kurdistan Regional Government Law No. 6 (2008), "Law on the Prevention of Misuse of Communications Devices." Articles 1 through 8 apply in situations of misuse within the university's network and systems.
3. **Protection Against Unauthorised Disclosure of Data**
   For issues involving unauthorised disclosure of sensitive or confidential data, Articles 327 and 437 of the Iraqi Penal Code No. 111 (1969) will be referenced and enforced.
4. **Disciplinary Actions under Law No. 14 (1991)**
   In addition to the above, employees violating this policy may face disciplinary actions in accordance with Article 8 of Law No. 14 (1991), as amended.

POLICY DISCLAIMER STATEMENT

Any deviations from policies, procedures, or guidelines approved and made public on uplo.uod.ac by the University Policy Office (UPLO), may only be done cooperatively between UPLO and the requesting entity with sufficient time to allow for appropriate risk analysis by SCSP, documentation, and presentation to the University Council for final approval. Failure to adhere to UPLO written official policies may be met with University sanctions.

RELATED POLICIES, PROCEDURES OR GUIDELINES

- University Confidentiality Agreement.
- UoD systems access control matrix

- Data Classification Matrix
- **Alumni Engagement Policy**
- QP-DOIT-01
- The UPLO can be reached at uplo.uod.ac. Send questions or approval requests to uplo.office@uod.ac

Annex

- Kurdish Translation
- Arabic Translation