The American University of Kurdistan
Data Classification Policy

Policy Number: IT003
Effective Date: November 13, 2022

CONTENT

I. INTRODUCTION

a. **Authority**: The Board of Trustees (herein referred to as “Board”) at The American University of Kurdistan (herein referred to as “AUK” or “University”) is authorized to establish rules and regulations to govern and operate the University and its programs.

b. **Purpose**: The purpose of this policy is to establish the categorization of AUK data and the safeguards that are required for each classification.

c. **Scope**: This policy applies to all AUK Staff, faculties, students, workers, contractors, and anyone who has access to data, collected, stored, or processed by AUK, in both electronic and non-electronic media.

II. ROLES AND RESPONSIBILITIES

a. **Responsible Executive**: Vice President for Administration and Finance

b. **Responsible Administrator**: Director of IT

c. **Responsible Office**: IT

d. **Policy Contact:** Director of IT

III. DEFINITION

AUK's data is divided into three categories:

- Public data
- Internal data
- Confidential data

1. Public data

Some common types of public data are:

- Course Catalogs
- Events Calendars
- Published vacancies
- Internet web pages
- AUK announcements
- Press releases

Data and information from the public domain can be widely disseminated without causing harm to AUK, its students, workers, or stakeholders. These materials may be shared with others outside of AUK. There are no limitations on who can access or use such data or information.

2. Internal data

Some common types of internal data are:

- Intranet web pages
- Training announcements
- Public information prior to official approval
- Internal Service Level Agreement
- Internal Policies & Procedures
- University internal memos, internal reports and plans
- Non-public contracts
- Internal emails

Unauthorized access, transmission, alteration, storage, or dissemination of internal data and information must be avoided. Only AUK employees have access to internal data. Any illegal data disclosure would be unsuitable. This categorization applies to some administrative data.

3. Confidential data

Some common types of confidential data:

- ✓ Students:
    - Name of the student
    - KR and Iraqi identification numbers
    - Passport information
    - Student ID number
    - Demographic information

  - Family information
  - Contact information, including personal phone number
  - Protected Health Information

- ✓ Employees:
  - Name
  - KR and Iraqi identification numbers
  - Passport information
  - Employee data
  - Demographic information
  - Family information
  - Contact information, including personal phone number
  - Protected Health Information

- ✓ Institution:
  - Donor contact information and giving history
  - Information on grants and non-public gifts
  - Faculty/staff personnel files, benefits information, salaries
  - Information covered by non-disclosure agreements
  - Password, password hashes, encryption key
  - Financial reports
  - Procurement reports and suppliers’ proposals
  - Audit reports
  - Employment applications
  - AUK Proprietary Research Data (not yet published)

Government regulations, contractual obligations, and AUK policies all protect confidential information. Individuals should only be given access to confidential information if they have a specific need to know.

If anyone violates the confidentiality of the above or similar data set, then s/he will be subject to the Employee Code of Conduct.

IV. POLICY STATEMENT

University documents, data, and systems will be categorized and secured in accordance with their significance to the AUK mission and the potential harm to the University's reputation if they are disclosed or disrupted.

V. POLICY PROCEDURES

a. Data Owner determines level of accessibility including information security requirements.
b. Data Custodian.

The data custodian is responsible for labeling information and following necessary requirements to protect and maintain the integrity of the data. The data custodian:

- Provides and manages security for the information asset.
- Protects information and information systems.

VI. POLICY HISTORY

a. **Approved by**: Board of Trustees

b. **Adopted**: November 13, 2022