The American University of Kurdistan
Data Security Policy

Policy Number: IT002
Effective Date: June 6, 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**: AUK restricts access to confidential and sensitive data to protect it from being lost or compromised, and in order to avoid adversely impacting stakeholders, incurring penalties for non-compliance with applicable laws and regulations, and suffering damage to AUK's reputation.

c. **Scope**: This Policy applies to everyone including, but not limited to, all AUK's faculty, staff, students, researchers, visitors, vendors, contractors, and volunteers who accesses AUK's data or networks or who stores data through the use of AUK's credential. Therefore, the Policy applies to every server, database and informational teachnology system that handles such data, including any device that is regularly used for email, web access or other work-related tasks.

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. POLICY STATEMENT

The University collects and processes a range of data relating to active institutional members including faculty, staff, and students for a variety of purposes related to employment and the learning experience. The University also holds data relating to wider activities and engagement with partners, contractors, and customers. With the ability to collect and process data comes a responsibility to ensure that this data is collected, used, stored, and protected appropriately. The AUK, therefore, ensures that data is managed in accordance with relevant rules and guidance and that those involved in data handling and processing are aware of their responsibilities.

IV. POLICY PRINICPLES

The University recognizes that data is a fundamental asset to a knowledge-driven organization, and it is the AUK's policy to ensure that data is protected against the adverse affects of failures in confidentiality, integrity, availability and compliance with legal requirements. Achieving this objective requires all members of the University complying with this Policy.

V. DEFINITIONS

1. **Data** – Information contained in either University computer systems or in physical copy that is utilized for the purposes of conducting University business or learning.
2. **User** – All persons that have access to AUK's data.
3. **Computer** – This includes all end user computing devices as well as servers.
4. **Authorization** – The function of establishing an individual's privilege levels to access and/or handle data.
5. **Unauthorized access** – Searching, reviewing, copying, modifying, deleting, analyzing, or handling data without proper authorization.
6. **Strong Password** – A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and characters.
7. **Centralized Computer Systems** – Computer hardware including, but not limited to, servers, routers, switches and access points. Also, computer software including, but not limited to, web hosts, customized databases, and AUK's databases maintained by the IT Department and located in areas managed by IT personnel.
8. **Decentralized Computer Systems** – Computer hardware including, but not limited to, servers, routers, switches and access points. Also, computer software including, but not limited to, web hosts, customized databases, and AUK's databases maintained by a non-IT Department.

VI. POLICY

1. CLASSIFICATION LEVELS

All AUK's data is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the data. The classification levels are:

A. Restricted Data

- Certain AUK's data classified as Restricted including, but not limited to, individual's bank account number, identity card and/or passport numbers, racial or ethnic origin, political affiliation, religion, physical or mental health, or sexual orientation.
- Sharing of Restricted Data within AUK may be permissible if necessary to meet AUK's legitimate needs. Except as otherwise required by law, no Restricted Data may be disclosed to parties outside AUK, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted Data; (ii) not to disclose the Restricted Data to any other party for any purpose absent AUK's prior written consent or a valid court order; and (iii) to notify AUK in advance of any disclosure pursuant to a court order unless the order explicitly prohibits such notification.

B. Confidential Data

- AUK's data is classified as Confidential if it falls outside the Restricted Data classification, but is not intended to be shared freely within or outside AUK due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Data include all non-Restricted Data contained in personnel files, misconduct and law enforcement investigation records, internal financial data, and education records.
- Sharing of Confidential Data may be permissible if necessary to meet AUK's legitimate needs. Unless disclosure is required by law, when disclosing Confidential Data to parties outside AUK, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of data; (ii) not to disclose data to any other party for any purpose absent AUK's prior written consent or a valid court order; and (iii) to notify AUK in advance of any disclosure pursuant to a court order unless the order explicitly prohibits such notification.

C. Unrestricted Data Within AUK

AUK's data is classified as Unrestricted if it falls outside the Restricted and Confidential Data classifications, but is not intended to be freely shared outside AUK. One example is the faculty, staff, and students' social media accounts. The presumption is that Unrestricted Data will remain within AUK. However, this data may be shared outside of AUK if necessary to meet AUK's legitimate needs, and the proposed recipient agrees not to disclose the data without the AUK's consent.

D. Publicly Available

AUK's data is classified as Publicly Available if it is intended to be made available to anyone inside and outside of AUK.

2. Data Confidentiality, Privacy, and Security

All users are expected to respect the confidentiality and privacy of individuals whose records they access. Users are responsible for maintaining the confidentiality of data they access or use and for the consequences of any breach of confidentiality. Data must

be secured by AUK with appropriate technical and organizational measures against unauthorized processing, and against accidental loss, destruction or damage.

3. Access Control

Access to AUK's data and its resident computing system will be restricted to those users that have a legitimate need and appropriate authorization for access to such data. Users must ensure that data is secured from unauthorized access and are responsible for safeguarding this data at all times through the use of strong passwords.

4. User Accounts

The University has two levels of user accounts:

- Full access to AUK's full network. Typically, this is the level of access provided to active faculty, staff, and students. Alumni are granted permanent AUK email accounts.
- Guests of AUK including, but not limited to, partners, researchers, orcontractors, may be granted temporary access to the AUK's network.

5. Password Management

Passwords for new students will be set by the student during their matriculation process. New members of faculty or staff will be informed of an initial and temporary password, which must be communicated in a secure manner and must be changed by the new member immediately.

6. Network Management

Users should note that it is not permitted to connect personally owned equipment to any network socket or equipment which has not been provided specifically for the purpose. It is, however, permissible to connect personally owned equipment to AUK's wireless networks. Any device connected to an AUK's network must be managed effectively.

7. Computing Systems

All computing systems shall be in compliance with this Policy and AUK's security standards regardless of whether they are centralized or decentralized.

8. Remote Access

Only authorized users will be permitted to remotely connect to AUK's computer systems, networks and data repositories to conduct AUK's related business.

9. Backup and Recovery

The IT Department will backup essential AUK data consistent with industry standards and store/back-up such data at a secure site (e.g. cloud hosting). Computing systems will have available, at a minimum, a documented recovery plan covering backup procedures, timelines, storage locations/procedures and recovery.

10. Security Incident Response and Handling

All suspected or actual security breaches of AUK, college or departmental/unit system(s) must be reported immediately to the IT Department to assess the level of threat to the University or affected individuals and respond according to this Policy.

11. Service Providers

Service providers utilized to design, implement, and service technologies must provide contractual assurance that data is protected according to AUK's or commercially reasonable standards. Such contracts must be reviewed by the Legal Counsel of AUK for appropriate terminology regarding use and protection of data.

12. Computer Labs

AUK provides robust computing lab resources for utilization in legitimate and lawful academic endeavors. Computing equipment in these labs will conform to all requirements of this Policy.

13. Software

Only properly licensed software may be installed on the University's computer systems.

14. Penalties and Enforcement

Penalties and enforcement of this Policy will be in accordance with AUK's policies. Appropriate disciplinary and/or legal action will be taken when warranted in any area involving violations of this Policy.

15. Breaches

The following occurrences are considered breaches to this Policy:

- Unlawful procurement of data by anyone not entitled to access such data;
- Unfair processing (i.e. processing data for a purpose other than that for which it was provided);
- Processing of inaccurate data, particularly if data was known to be inaccurate or steps could have been taken to ensure its accuracy;
- Unlawful disclosure (i.e. sharing of data with anyone not entitled to receive it or loss of any data subject to this Policy);
- Collection, storage or processing of inadequate, irrelevant or excessive data; unlawful disclosure, inadequate/irrelevant/excessive data are all breaches of this Policy.
- Any violations/breaches of this Policy by an employee or student will result in a disciplinary action taken in accordance with the Employee Code of Conduct or Student Code of Conduct.

16. Notification of Breach or Loss of Data

All breaches or suspected breaches of the Policy or any loss of data as classified in section (1) must be reported to IT Department Team as soon as it is discovered.

17. Policy Review and Revision

This Policy will be subject to periodic review and revision by the IT Department to ensure the effectiveness of current data security measures.

VII. ROLE OF the IT DEPARTMENT

The IT Department is charged with the responsibility to manage and implement the policy and procedures with the objective to ensure the protection of important and sensitive institutional data. At the same time, the IT Department shall comply with relevant applicable laws, regulations, and institutional policies.

VIII. RESPONSIBILITIES OF THE IT DEPARTMENT

- Implement adequate security measures for computing systems containing AUK's data.
- Implement appropriate security strategies for both the transmission and the storage of AUK's data.
- Disseminate technical guidelines related to data security to the appropriate stakeholders.
- Review and evaluate AUK's current practices and the associated risks to the institution.
- Review and evaluate actions needed to address risks through appropriate policy and associated guidelines.
- Identify new processes that are needed.
- Function immediately when incidents of breach are reported.

IX. USER RESPONSIBILITIES

AUK's faculty, staff, and students (when acting on behalf of the AUK through service on AUK's bodies), and others granted use of AUK's data:

- Shall not disclose sensitive data to unauthorized individuals.
- Shall not modify or delete AUK's data unless authorized to do so.
- Shall maintain AUK's data in a secure manner.
- Shall keep their passwords confidential and not share them.
- Shall immediately report incidents of breach to the IT Department Team.

1. POLICY HISTORY

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

b. **Adopted**: June 6, 2022