The American University of Kurdistan
Policy of Information and Computer Resources

Policy Number: IT005
Effective Date: November 13, 2022

CONTENT

I. Introduction
II. Roles and Responsibilities
III. Definition
IV. Policy Statement
V. Policy Principles
VI. Policy Procedures
VII. Policy History

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 outline the acceptable use of computer equipment, information systems, network, data, and other information technology resources at AUK.

c. **Scope**: policy applies to the use of information, data, electronic and computing devices, and network resources that are used to conduct AUK business.

This policy also applies to any equipment, devices, or systems that interact with AUK networks and systems.

This policy applies to any individuals who have access to and use AUK information, systems, and networks.

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

For the purpose of this Policy, the terms below have the following definitions:

Availability (Of Information Technology Resources)

Ensuring timely and reliable access to and use of information.

Authentication Method:

Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.

Confidentiality (Of Information Technology Resources)

Ensuring Electronic Information and Information Technology Resources are protected from unauthorized access.

Desktop, Laptop, Mobile, or Other Endpoint Device:

Any device, regardless of ownership, that has been used to store, access, or transmit Electronic Information, not classified as a Server. These devices are intended to be accessed directly by individuals and include, but are not limited to desktops, laptops, mobile phones, and tablets.

Electronic Information (Often referred to as Electronically Stored Information (ESI))

Any documents or information stored, in electronic form.

Information Technology Resources:

AUK-owned facilities, technologies, and information resources used for AUK processing, transfer, storage, and communications. Included, without limitations, in this definition are computer labs, classroom technologies, computing and electronic devices and services, email, networks, telephones (including cellular), video, multimedia, and instructional materials. This definition is not all inclusive but rather reflects examples of equipment, supplies and services. This also includes services that AUK-owned, leased, operated or provided by AUK or otherwise connected to AUK resources, such as cloud and Software, or any other connected/hosted service.

Integrity (Of Information Technology Resources)

Guarding against improper information modification or destruction.

Server:

A computer program or device that provides dedicated functionality to AUK community. These are normally managed by professional information technology practitioners.

Two-Step Authentication:

A method to protect an account or system that requires more than one means to access it, such as providing a password as well as a response to a verification code sent to a physical device.

IV. POLICY STATEMENT

Access to Information Technology Resources is a privilege and continued access is contingent upon compliance with AUK policies.

Users of Information Technology Resources are responsible for the content of their individual communications and may be subject to personal liability resulting from that use.

V. POLICY PROCEDURES

a. All access to AUK systems and data must be authorized and authenticated from IT Department.
b. Any device connecting to the AUK network must be properly authorized and authenticated per the AUK domain and must be properly maintained.
c. Circumventing or disabling user authentication or security mechanisms of any system, network, or account is prohibited.
d. It is the responsibility of every user to protect their data and authentication credentials. Individuals must take responsibility in managing their own information security by exercising due care in protecting their systems, accounts, accesses, and data by flowing safe computing best practices.
e. Sharing authentication credentials is not allowed with anyone including family or other employees.

f. AUK proprietary information created by university employees within the scope of their employment and stored on any electronic and computing device remains the sole property of AUK. It is the responsibility of each individual to preserve this information in compliance with the Data Classification Policy, and it is the responsibility of the Faculty or Administrative Unit to make sure this data is handed over before an employee is discharged and as part of the clearance process.
g. Individuals are required to promptly report the theft, loss, or unauthorized disclosure of AUK proprietary information to their immediate supervisor and to the IT Department.

h. AUK information technology resources are not to be used for non-AUK related commercial purposes.
i. Individuals are prohibited from engaging in any activity that is illegal under local or international law while utilizing AUK-owned IT resources.
j. Using AUK information technology resources to gain unauthorized access or to impair or damage the operations of any networks, systems, or data is strictly prohibited.
k. Any form of harassment via email, telephone, or paging, whether through language, graphics, videos, is strictly prohibited.
l. Users may not implement their own network infrastructure or modify the existing AUK network infrastructure without explicit authorization from the IT Department. This includes, but is not limited to, installing network devices such as hubs, switches, routers, network firewalls, and wireless access points to the existing AUK network.
m. Unauthorized the installation of any copyrighted software for which AUK or the end user does not have an active license is strictly prohibited.
n. Wasting computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings is prohibited.
o. Sending inappropriate email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is prohibited.
p. AUK may from time-to-time conduct audits on its data, networks, and systems to ensure compliance with AUK policies and applicable laws. Any such audit will be compliant with the University Privacy Policy on Electronic Communication and Files.

Violations of any of the above would be subject to the Employee and Student Code of Conduct Policies.

VI. POLICY HISTORY

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

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