The American University of Kurdistan
Policy of Network Account

Policy Number: IT004
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 clarify the network responsibilities, this includes, but is not limited to desktop computers, laptops, servers, printers, tablets, Chromebooks, smart phones, irrespective of ownership.

c. **Scope**: The scope of the policy covers all users and all equipment irrespective of ownership that is attached to network data points on the AUK network or uses the AUK operated wireless network.

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

AUK depends heavily upon its IT Network for research, teaching, and administrative activities. It is essential that the stability, integrity, and security of the IT network be safeguarded for use by all members of the AUK.

The IT Network is the infrastructure that connects devices allowing the exchange of data to support the AUK business and operations.

The management and oversight of the IT Network is the remit of IT Services under the management of the Director of IT. AUK reserves the right to refuse a connection for any non-standard device.

IV. DEFINITION

a. Permission must be obtained from IT Services before any non-standard device is connected to the network. This process is handled through the IT Service Desk.
b. IT Services may employ measures to ensure compliance with this policy, the IT regulations and the associated policies e.g. remote audit and security penetration testing.
c. For security and network maintenance purposes, authorized individuals within IT Services may monitor equipment, systems and network traffic at any time.
d. All devices must use DHCP for IP configuration, with the exception of essential IT Infrastructure devices.
e. All users of the network must be aware of and abide by the AUK Acceptable Usage Policy.
f. New physical connections of equipment to a data port of the University's network may only be made by IT Services. Under no circumstance should a user attach any device to a data port. Any unauthorized device found attached to a data port will be removed and disposed of without warning.
g. Connected equipment must be maintained in accordance with manufacturers' recommendations. In particular, operating system and application software should be kept up-to-date to ensure that security vulnerabilities are not created.
h. Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches, without the prior approval of the Director of IT Services.
i. Users must not attempt to circumvent any firewall or software designed to protect systems against harm.
j. Unauthorized use of IP addresses or changing of a System MAC address is prohibited.

V. POLICY PROCEDURE

Wireless Network Policy:

a. All wireless connections to the AUK network must be individually authenticated, logged, and be trackable back to the user.
b. All wireless access points which connect to the AUK network must be owned by AUK and operated by IT Services. Users must not turn their device into an access point or an ad hoc network unless all devices on the ad-hoc network are isolated from the University's network.
c. Rogue wireless access points will be located, removed and disposed of by IT Services.

d. Personally owned Mobile Devices including any device not owned by the University is only authorized to connect to the WLC_OpenAccess wireless profile for Internet access only.

Firewall:
All parts of the AUK network (i.e. all of the IP address space allocated) will be protected by a centrally managed AUK Firewall.

VI. POLICY HISTORY

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

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