

The American University of Kurdistan
Policy of Information and Computer Resources

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

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

