Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: February 2025
Review: January 2026

Acceptable Use, IT Enforcement and Accountability - Policy & Procedures

1.0 Purpose

1.1 Establishing guidelines for the ethical and appropriate use of IT resources to ensure secure, reliable, and equitable access for the AUIB community.

2.0 Scope

2.1 This policy applies to all AUIB community members, including students, staff, faculty, contractors, and authorized guests who utilize AUIB's IT resources.

3.0 Definitions

3.1 Acceptable Use - refers to the proper, ethical, and legal utilization of AUIB's IT resources in line with the university's objectives, policies, and legal regulations. It involves supporting AUIB's administrative, research, and educational activities with IT services, tools, software, and data. Activities that interfere with other users' rights and access that are unlawful, or disruptive to the network are examples of unacceptable use.

3.2 User - refers to any individual who is authorized to access and use AUIB's IT resources. This includes, but is not limited to, students, staff, faculty, contractors, visitors, and any third-party personnel or authorized guests who have been granted access to the university's digital resources.

3.3 IT Resources - includes all AUIB's networking, computing, and communication resources, such as but not limited to:

- Hardware (desktops, laptops, servers, printers, scanners, etc.)
- Software (licensed applications, proprietary systems, open-source tools, etc.)
- Networks (internet, intranet, email services, cloud-based services, etc.)
- Data storage systems and devices (servers, external drives, cloud storage)
- Communication systems (phones, video conferencing, etc.)

3.4 University Data - refers to any data owned, managed, or created by AUIB. This includes student records, staff information, research data, financial data, proprietary software or information, and other forms of data used in the operation and management of the university. University data must be treated as confidential unless explicitly stated otherwise, and unauthorized access or misuse of university data is prohibited.

3.5 Unauthorized Access - refers to accessing AUIB's IT systems or resources without permission, either by attempting to bypass security controls or by using someone else's credentials. Unauthorized access is a violation of AUIB's policies and is subject to disciplinary actions, including suspension of privileges and legal consequences.

3.6 Confidential Information - includes any non-public data related to AUIB operations, academic activities, research, and administrative processes. It includes personal information about students, staff, and faculty, research data, financial records, intellectual property, and any other information that must be protected under the law or university policy.

3.7 IT Department - refers to the department within AUIB responsible for managing, maintaining, and securing the university's IT infrastructure and services. It is also responsible for monitoring policy compliance, offering support for technical issues, and ensuring that AUIB's IT resources are used effectively and securely.

4.0 Policy

Importance of Utilizing IT Resources

4.1 All AUIB community members must adhere to the university's policies related to IT usage. Any actions that violate these policies will result in consequences.

4.2 Users must review relevant AUIB policies to ensure the proper use of IT resources.

Compliance and Guidelines for IT Resource Usage

4.3 Compliance with all policies, procedures, and laws related to accessing and using AUIB's information technology resources is essential. To guarantee the safety and security of AUIB's resources, people must read and comprehend these rules completely.

4.4 It is essential that everyone follows these rules to ensure a smooth and efficient procedure. The same rules that govern normal users must be scrupulously followed by any visitors granted access to our IT resources.

4.5 For any inquiries regarding authorized access, usage, or other matters outside the scope of AUIB policies, rules, standards, guidelines, and procedures, it is essential that people seek system administrators or data custodians for clarification.

4.6 The user's responsibility is to safeguard the desktop or laptop, and the information stored on it from damage, loss, and theft.

4.7 In the event of a damaged, stolen, or lost laptop or mobile device, it is vital to inform University Information Technology Services promptly.

4.8 It is advised that the user should not leave their laptop or mobile device unattended in public without keeping a watchful eye on it.

4.9 Users must password-protect their lock screens immediately after they are done using their laptop, desktop, or mobile devices.

4.10 As a user of AUIB's information technology resources, responsibility lies with individuals to ensure the content of personal communications. AUIB cannot be held responsible for any unauthorized or personal use of resources by users.

4.11 Users must be aware that the Information Technology Department prioritizes security and ensures complete protection of user data. It is important to take precautionary measures. AUIB does not guarantee absolute security and privacy. Users should follow the appropriate security procedures.

4.12 The user must not alter the operating system or system administrator password or any other administrative settings on any AUIB-IT-issued devices. Users are strongly discouraged from using the AUIB University network on their laptops.

4.13 Witnessing any policy violations, it is crucial to report them to the appropriate management authorities and/or to the IT Department.

Shared Access to IT Resources

4.14 Computers, networks, and electronic information systems are critical to the fulfilment of AUIB's mission of instruction, research, and service. Therefore, shared access to these resources is offered to the community members by AUIB.

Access Information Technology Resources

4.15 IT resources and related services will be allocated to employees and students based on their membership status determined by AUIB's Human Resources Management and Registration Management offices.

Access Rights and Software Use

4.16 Access rights for visiting faculty, hourly staff, and long-term third-party vendors will be determined by the head of the employee's or student's unit.

4.17 Under no circumstances are owners and operators of any computer, servers, IT devices, and services within the AUIB network allowed to grant access to accounts on their IT resources and services without proper approvals. This is prohibited.

4.18 Installation of unlicensed, non-standard encryption software is prohibited.

4.19 Software copying, distribution, or intercepting of information or seizure of passwords without specific permission is prohibited. License terms for any software must always be taken into consideration. Software is used in accordance with Iraqi laws in the country, including copyrights, commercial transactions and patents.

Responsible Use of Community Resources

4.20 Community resources are extremely valuable and must be managed with the utmost responsibility to maintain integrity, security, and availability for appropriate educational and business activities. Authorized users are expected to use these

resources efficiently, effectively, and responsibly. Any deviation from these expectations will not be tolerated.

4.21 Colleges, departments, and administration units align their technology use policies with the university's policies and any other relevant technology use policies.

Compliance with applicable policies is mandatory for all incidental personal use of university information technology resources. Such use must not hinder employees from fulfilling their university duties, violating the law, or negatively impacting the university's mission-related activities.

4.22 Priority for the use of IT resources is given to activities related to the university's missions of teaching, learning, research, and outreach. AUIB computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and resources. Individual users may be required to restrict non-priority use of IT resources, such as non-academic, non-business services.

4.23 Inappropriate or malicious use of IT systems, includes:

- Setting up file sharing in which protected intellectual property is illegally shared.
- Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Inappropriate use or sharing of university-authorized IT privileges or resources. Changing another user's password, access, or authorizations.
- Using an AUIB University computing asset to actively engage in displaying, procuring, or transmitting material that violates sexual harassment policy or laws, or illegal activity.
- Using an AUIB University computing asset for any private purpose or personal gain.

4.24 The Acceptable Use of Information Technology Resources Policy is enforced through the following mechanisms:

4.24.1 The university may temporarily disable service to an individual or a computing device, when an apparent misuse of university computing facilities or networks has occurred, and the misuse:

- It is a claim.
- It is a violation of criminal law.
- It has the potential to cause significant interference with university services.
- May cause severe damage to another person.
- May result in liability to the university.

4.24.2 An attempt will be made to contact the person responsible for the account or equipment before disabling service unless law enforcement authorities forbid it, or IT Services staff determine that immediate action is necessary to

preserve the integrity of the university network. In any case, the user shall be informed as soon as possible so that they may present reasons in writing why their use is not a violation or that they have authorization for the use.

4.24.3 Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if after

hearing the user's explanation of the alleged violation, an employee disciplinary body has determined that the user has engaged in a violation of the code.

4.24.4 Violations of AUIB University Acceptable Use of Information Technology Resources Policy may be referred to as disciplinary action. AUIB may assess a charge to offset the cost of the incident.

5.0 Procedures

Policy Enforcement

5.1 The AUIB IT department is responsible for the enforcement of this policy. This includes monitoring compliance, investigating potential violations, and acting against those who fail to adhere to the established guidelines.

5.2 The IT department will actively audit and monitor IT resource usage to detect unauthorized or improper use, and any non-compliance will be addressed promptly.

Responsibility of Individuals

5.3 All users of AUIB IT resources, including students, faculty, and staff, are accountable for ensuring the appropriate use and care of devices, software, and digital platforms provided by the university. Users must also report any suspicious or unauthorized activity that may violate this policy to the IT department immediately.

5.4 Users must remain vigilant in protecting their devices and systems from loss, theft, or damage, and ensure they are used only for purposes aligned with AUIB's mission and policies.

Disciplinary Action

5.5 Violations of this policy will be met with disciplinary action. The severity of the response will be determined based on the nature of the violation and any mitigating factors. Disciplinary measures may include, but are not limited to:

- Verbal or written warnings.
- Temporary suspension of IT privileges.
- Financial restitution for damages incurred due to the violation.
- In cases of severe infractions, more serious actions such as dismissal from the institution or legal proceedings may be pursued.
- The enforcement of disciplinary actions will follow a structured process, ensuring that individuals are given an opportunity to explain their actions before a final decision is made

5.6 Users must refrain from engaging in activities that violate university policies. Failure to comply with this policy will result in disciplinary measures according to AUIB's Conduct Code and staff/faculty employment policies.

5.7 Disciplinary actions, when imposed, will follow due process, and users will be informed of their right to present an explanation or defense regarding alleged violations.

5.8 In instances of severe or repeated violations, users may be permanently restricted from using AUIB's IT resources, and legal action may be taken where appropriate

Related Policies and Documents

Acceptable Use Policy
Code of Conduct Policy
IT Security Policy
Data Privacy Policy