Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: January 2024
Review: January 2025

Acceptable Use of Computing, Information, and Technology Resources Policy & Procedures

1.0 Purpose

1.1 AUIB provides Information Technology Resources for advancing its educational, research, service, and business objectives. The aim of this policy is to establish the ethical and appropriate utilization of IT resources at AUIB. It is imperative that all members of our community (students, staff, and faculty) are provided with reliable and protected IT resources, free from any unauthorized or malicious activities.

1.2 Practices that lack security measures put the students, faculty, and staff of AUIB at risk of various threats, such as harmful applications; the consequences of IT service failures can lead to data and information loss including confidential ones. Any access or use of IT Resources that interferes, interrupts, or conflicts with this policy is unacceptable and will be considered a violation of this policy.

2.0 Scope

2.1 This policy applies to all members of the AUIB community, including students, faculty, and staff, authorized guests, delegates, and independent contractors who use, access, or otherwise employ, locally or remotely, AUIB's IT Resources, whether individually controlled, shared, standalone, or networked. This policy is binding and covers all IT resources owned or leased by AUIB, including privately-owned equipment connected to the campus network.

2.2 These resources, without exception, comprise computer equipment, software, operating systems, tablets, smartphones, multimedia devices, storage media, the campus network, and university data. It is the unwavering responsibility of both system manager and users to ensure the security and protection of these valuable assets from misuse or malicious activity.

3.0 Definitions

3.1 Acceptable use - access to information, data, and systems, is strictly limited to authorized individuals who are members of the University community. Any unauthorized use of this information and these systems for personal gain, personal business, or fraudulent activities, is absolutely prohibited. It is imperative that all individuals adhere to these guidelines to maintain the integrity and security of our university community.

3.2 User - encompasses all individuals and entities using the University's information and IT resources, including faculty, staff, students, developers, contractors, vendors, visitors, and any other relevant parties. An individual or entity that possesses the right to access AUIB's computer or network resources is referred to as an authorized user.

3.3 University data - is a critical asset that is owned exclusively by the university, and it supports the institution's mission and operations. It must be treated with utmost care and protection to ensure its integrity and availability. Securing shared university data and limiting access to authorized individuals are crucial measures. Additionally, strict protocols and guidelines must be established for external data sharing to safeguard individual privacy and data integrity.

3.4 Availability - is the capacity of systems to operate efficiently and provide uninterrupted service to authorized users. A lack of availability means there is a disruption in accessing or using information or an information system.

3.5 Confidentiality - is the act of safeguarding sensitive information and making sure authorized individuals only access it. Any unauthorized disclosure of information is considered a breach of confidentiality according to this policy.

3.6 Integrity - it is imperative that the integrity of information and systems is always upheld. Any alteration or damage inflicted upon the information can result in a severe loss of integrity.

3.7 Information technology (IT) resources - made up of numerous components, including computers, software, servers, network usage, storage usage, virtual machine capacity, tablets, phones, multimedia devices, storage devices, and any other resource that the IT team maintains and manages. Included in this definition are computer labs, classroom technologies, computing and electronic communication devices and services, such as modems, wireless access points, e-mail, networks, telephones, voice mail, fax transmissions, video, multimedia, instructional materials.

3.8 Potential impact - must not be underestimated as it pertains to the level of damage that may arise from the compromise of confidentiality, integrity, or availability affecting the university's operations, assets, or individuals.

3.9 Security incident - in the realm of information technology, a security incident pertains to any unplanned or deliberate occurrence that impacts data or associated technology, leading to data loss. or a disruption and/or denial of availability.

3.10 Security measures - processes, software, and hardware, used by system and network admin to ensure the confidentiality, integrity, and availability of the information technology resources and their authorized users. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues.

4.0 Policy

4.1 Importance of Utilizing IT Resources

4.1.1 As a member of the AUIB community, it is imperative that individuals understand the importance of utilizing our IT resources. Adherence to all relevant AUIB Policies and Procedures without exception is required.

4.1.2 These policies cover vital topics such as harassment, plagiarism, commercial use, security, ethical conduct, and laws that prohibit theft, copyright and licensing infringement, unlawful intrusions, and breaches of data privacy laws. Disregarding these policies will result in severe consequences that individuals must take seriously.

4.2 Compliance and Guidelines for IT Resource Usage

4.2.1 Compliance with all policies, procedures, and laws related to accessing and using AUIB's information technology resources is essential. It is imperative that individuals review and fully understand these regulations to ensure the safety and security of AUIB's resources.

4.2.2 It is imperative that all individuals adhere to these guidelines to guarantee a seamless and effective process. All guests given access to our information technology resources must strictly adhere to the same policies that apply to regular users.

4.2.3 For any inquiries regarding authorized access, usage, or other matters outside the scope of AUIB Policies, Rules, Standards, Guidelines, and Procedures, it is imperative that individuals seek clarification from the system administrators or data custodians.

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

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

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

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

4.2.8 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.

4.2.9 Users must be aware that we prioritize security and ensure 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.

4.2.10 It is imperative that the user refrains from making any modifications to the administrative functions on their portable computer, which includes the operating system or system administrator password. It is strongly advised that users do not connect their personal computers to the AUIB University network.

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

4.3 Shared Access to IT Resources

4.3.1 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.

4.4 Access Information Technology Resources

4.4.1 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.

4.5 Access Rights

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

4.5.2 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.

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

4.5.4 Software copying, and distribution, or intercepting information or seizure 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 and commercial transactions and patents.

4.6 Responsible Use of Community Resources

4.6.1 Our community resources are extremely valuable and must be managed with utmost responsibility to maintain their integrity, security, and availability for appropriate educational and business activities. We expect our authorized users to use these resources efficiently, effectively, and responsibly. Any deviation from these expectations will not be tolerated.

4.6.2 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, violate the law, or negatively impact the university's mission-related activities.

4.6.3 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 halt or curtail non-priority use of IT resources, such as non-academic, non-business services.

4.6.4 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 is in violation of sexual harassment policy or laws, or illegal activity.
- Using an AUIB University computing asset for any private purpose or for personal gain.

4.6.5 The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms:

4.6.6 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:

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

4.6.7 An attempt will be made to contact the person responsible for the account or equipment prior to 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.

4.6.8 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.

4.6.9 Violations of AUIB University Acceptable Use of Information Technology Resources policy may be referred for disciplinary action. AUIB may assess a charge to offset the cost of the incident.

5.0 Procedures

5.1 It is imperative that users refrain from engaging in any activities that violate university policies. The following guidelines are not exhaustive but provide a framework for unacceptable activities. The IT Director has the authority to include additional prohibited uses as the university adopts modern technologies or compliance requirements.

5.2 Failure to comply with this policy will result in appropriate disciplinary measures in accordance with the "Conduct Code," as well as relevant staff and faculty employment policies or collective bargaining agreements. Furthermore, the university has the authority to impose a fee to cover the costs incurred because of the incident. In severe instances, legal action may be required.

5.3 In the event of a policy violation, the user will face consequences including a warning, required agreement to certain conditions for continued service, or suspension/denial of privileges as determined by the IT Director or disciplinary body.

The user's explanation will be taken into consideration before a final determination is made.

5.4 The use of university computers and systems for personal purposes is prohibited except in rare and critical situations. However, individuals are permitted to utilize the university's internet access on their personal devices for any legal purpose that adheres to university policies and regulations. Staff members must stay informed about laws that grant access to public records, which cover most information stored on university IT resources.

5.5 It is essential to prioritize the use of IT resources for activities related to the university's core missions of teaching, learning, scholarship, and outreach. Since university IT resources have limited capacity and are in high demand, it is necessary for individuals to use them responsibly.

5.6 It is prohibited to partake in activities that are considered unacceptable for the AUIB systems. Engaging in security breaches or any malicious utilization of network communication is categorically unacceptable. These activities comprise, but are not limited to:

- Gathering information about the configuration of a network or system the user does not have administrative access to.
- Engaging in activities that conceal the user's identity is prohibited unless anonymous access is expressly granted.
- Engaging in activities that intentionally harm university systems, or result in a compromise of confidentiality, integrity, or availability of university data or services is prohibited.
- Deliberately causing disruptive traffic on the network or its connected systems.
- Deliberately creating disruptive Wi-Fi activity that obstructs wireless communication.
- Unauthorized access to systems that are not explicitly authorized by the user is prohibited.
- Preventing or disrupting other users from accessing the campus network is forbidden. Moreover, it is prohibited to use university IT resources to disrupt or deter service to individuals outside of the university.

5.7 If an individual misuses university computing facilities, the university may temporarily disable their service.

- Violating a license agreement or infringing on intellectual property rights.
- The occurrence has the potential to compromise the confidentiality, integrity, or availability of the IT resources of the university.
- Causing significant harm to another person is not acceptable. May result in liability to the university.
- If an account needs to be temporarily disabled, the responsible person will be notified promptly. They can give reasons why their use is not a violation

or show that they have authorization for it. However, numerous actions may be sealed due to law enforcement.

Related Policies and Documents

Academic Integrity and Misconduct - Students
Academic Integrity and Misconduct - Faculty and Staff
Acceptable Use Agreement
Code of Conduct
Data Classification and Handling
Digital Copyright Compliance
Electronic Communication
Information Security
Intellectual Property
Non-academic Misconduct- Students
Use of Personal Devices