Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: May 2025
Review: April 2028

Information Technology Devices Usage - Policy & Procedures

1.0 Purpose

1.1 To establish guidelines for the acceptable use of AUIB-issued devices and network resources. Also, inform users of their responsibilities in safeguarding these resources.

2.0 Scope

2.1 This policy applies to all devices issued by AUIB IT and covers all staff and faculty members who use AUIB IT devices.

3.0 Definitions

3.1 AUIB IT devices - any equipment, including but not limited to laptops, desktops, tablets, smartphones, printers, and other hardware, issued by AUIB IT for official university use.

3.2 Network resources - all components of AUIB's information technology infrastructure, including internet access, intranet, servers, and associated software systems.

3.3 Unauthorized access - any access to AUIB IT devices or network resources that has not been explicitly permitted by the AUIB IT department.

3.4 External devices - any computer, smartphone, or other electronic device not issued by AUIB IT but connected to the university's network.

3.5 Password sharing - the act of providing one's login credentials (e.g., username, password, or PIN) to another individual who is not authorized to access AUIB IT devices or network resources.

3.6 Malware - malicious software, such as viruses, worms, or Trojan horses, designed to damage, disrupt, or gain unauthorized access to AUIB IT devices or network systems.

3.7 Mass email (spam) - unsolicited bulk messages sent via electronic messaging systems, often disrupting regular operations or inconveniencing users.

3.8 Malfunction - any situation where AUIB IT devices fail to perform as expected due to technical or physical issues.

3.9 University-related activities - Work, research, or educational tasks directly tied to the mission and operations of AUIB.

4.0 Policy

4.1 No individual shall use any AUIB IT devices or network resources without appropriate authorization. Attempting unauthorized access to any of AUIB's devices or network facilities is strictly prohibited.

4.2 External computers or devices may only be connected to AUIB's networks if they comply with the technical and security standards set by the AUIB IT department.

4.3 AUIB IT devices and network resources are strictly for university-related activities. Use of these resources for non-university business is prohibited unless specifically authorized.

4.4 Sharing passwords for AUIB IT devices or network facilities with unauthorized personnel is forbidden. Users are not permitted to obtain or use others' passwords. Only designated AUIB IT administrators are allowed to configure device settings.

4.5 No one shall read, alter, or delete another individual's files or emails without authorization, even if system settings allow such access.

4.6 Copying, installing, or using software or data in violation of copyright laws or license agreements is prohibited. This includes downloading or distributing unauthorized software or electronic media.

4.7 Creating, installing, or knowingly distributing computer viruses, Trojan horses, or any other destructive programs on AUIB IT devices or network facilities is forbidden, regardless of intent or outcome.

4.8 Unauthorized modification or reconfiguration of AUIB IT devices or network facilities is prohibited.

4.9 Users are fully responsible for the data they store on AUIB IT devices and transmit via AUIB network resources. Storing or transmitting data that violates laws or university policies is prohibited.

4.10 Electronic messaging services (such as email) are intended for communication among individuals or defined groups. Unauthorized mass emails (spam) that disrupt AUIB's information technology resources or users' ability to operate are prohibited.

4.11 All users are responsible for the careful, safe, and responsible use of AUIB IT devices and resources allocated to them.

4.12 Any malfunction or problem with AUIB IT devices must be immediately reported to the designated AUIB IT staff.

4.13 Repeated improper use, wastage of supplies, or actions compromising the safety of equipment or individuals may result in disciplinary action.

4.14 If an AUIB-issued device malfunctions or underperforms, the device must be submitted to the AUIB IT department for evaluation. A committee will assess the issue, determine accountability, and decide on appropriate actions.

5.0 Procedures

Authorization for Access

5.1 Users must seek approval from the AUIB IT department to gain access to any AUIB IT devices or network resources.

5.2 Requests for access must be submitted via the official IT service desk or email.

Connecting External Devices

5.3 Before connecting an external device to AUIB's network, the user must submit a request to the IT department.

5.4 External devices must comply with AUIB IT's technical and security standards.

Reporting Malfunctions

5.5 Users must report any device or network issues immediately to the AUIB IT service desk.

5.6 The device must be brought to the IT department for inspection if necessary.

Assessment of Malfunctioning Devices

5.7 Upon receiving a malfunctioning device, the AUIB IT department will initiate an evaluation.

5.8 A designated committee will assess the issue, determine whether the malfunction was caused by misuse or negligence, and decide on further actions, including repair or replacement.

Safe and Responsible Use

5.9 Users must handle AUIB IT devices with care to prevent physical damage, unauthorized reconfiguration, or software misuse.

5.10 Any breach of usage guidelines, such as downloading unauthorized software, will result in disciplinary action.

Data Responsibility

5.11 Users are responsible for ensuring the security and legality of data stored on AUIB IT devices or transmitted via the university's network.

5.12 Sensitive or confidential data should be stored and transmitted using AUIB-approved encryption methods.

Addressing Unauthorized Access

5.13 Any attempts to access or modify AUIB IT devices or network resources without proper authorization will be investigated.

5.14 Identified violations will be reported to university management for further disciplinary measures.

Communication and Email Usage

5.15 Users must avoid sending mass emails or messages without explicit authorization from the AUIB IT or communications department.

5.16 Misuse of email services will lead to a review and potential suspension of access.

Disciplinary Measures

5.17 Repeated improper use or negligence of AUIB IT devices and network resources will result in escalating disciplinary actions, up to and including suspension of IT privileges or termination of employment.

Related Policies and Documents