AMERICAN UNIVERSITY OF BEIRUT
Mediterraneo

Information Technology

Information and Computer Resources Acceptable Use Policy

Contents

1. Purpose

Information technology resources are provided by the University to further the University's mission of research, education, student life, and health care.

Inappropriate use of these resources exposes American University of Beirut Mediterraneo Campus (AUBMED) and its community to risks and possible violation of existing laws.

The purpose of this policy is to outline the acceptable use of computer equipment, information systems, network, data, and other information technology resources at AUBMED.

2. Scope

This policy applies to the use of information, data, electronic and computing devices, and network resources that are used to conduct AUBMED business.

This policy also applies to any equipment, devices, or systems that interact with AUBMED networks and systems.

This policy applies to any individuals who have access to and use AUBMED information, systems, and networks.

3. Policy

3.1.1 All access to AUBMED systems and data must be authorized and authenticated in compliance with the System Authentication Policy.

3.1.2 Any device connecting to the AUBMED network must be properly authorized and authenticated per the *System Authentication Policy*, and must be properly maintained - including up-to-date anti-virus protection.

3.1.3 Circumventing or disabling user authentication or security mechanisms of any system, network, or account is prohibited.

3.1.4 It is the responsibility of every user to protect their data and authentication credentials. Each individual must take responsibility in managing their own information security by exercising due care in protecting their systems, accounts, accesses, and data by flowing safe computing best practices.

3.1.5 Sharing authentication credentials is not allowed with anyone including family or other employees.

3.1.6 AUBMED proprietary information created by university employees within the scope of their employment and stored on any electronic and computing device remains the sole property of AUBMED.

3.1.7 Individuals are required to promptly report the theft, loss, or unauthorized disclosure of AUBMED proprietary information to their immediate supervisor and to the IT Security Office at it.security@aub.edu.lb.

3.1.8 Occasional personal use of the AUBMED IT resources is allowed if it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this and other university policies.

3.1.9 AUB information technology resources are not to be used for non- AUBMED related commercial purposes.

3.1.10 Individuals are prohibited from engaging in any activity that is illegal under local or international law while utilizing AUBMED -owned IT resources.

3.1.11 Using AUBMED information technology resources to gain unauthorized access or to impair or damage the operations of any networks, systems, or data is strictly prohibited. This includes using AUBMED computer systems or network infrastructure for conducting or getting involved in malicious cyber activities, cyberattacks, social engineering attacks targeting any organization or individual whether affiliated with AUBMED or not.

3.1.12 Any form of harassment via email, telephone, or paging, whether through language, graphics, videos, frequency, or size of messages is strictly prohibited. This includes using any AUBMED computing asset to actively engage in procuring or transmitting material that is in violation of the Policy on Sexual and Other Discriminatory Harassment or that

may lead to an hostile workplace in the user's local jurisdiction or any other applicable jurisdictions.

3.1.13 Users may not implement their own network infrastructure or modify the existing AUBMED network infrastructure without explicit authorization from the CIO. This includes, but is not limited to, installing network devices such as hubs, switches, routers, network firewalls, and wireless access points to the existing AUBMED network.

3.1.14 Eaves dropping on any network and communications – including port scanning and intercepting network data - is expressly prohibited without proper written authorization from the CITO or the President.

3.1.15 Unauthorized copying and downloading of copyrighted material is prohibited. This includes, but is not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AUBMED or the end user does not have an active license is strictly prohibited.

3.1.16 Wasting computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings is prohibited.

3.1.17 Sending inappropriate email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is prohibited.

3.1.18 AUBMED may from time to time conduct audits on its data, networks, and systems to ensure compliance with AUBMED policies and applicable laws. Any such audit will be compliant with the University Privacy Policy on Electronic Communication and Files.

3.1.19 Engaging in any activity that violates the privacy policies of AUBMED is prohibited.

4. Policy Compliance

All users must acknowledge that they have read and understood this policy before gaining access to any AUBMED networks, systems, or data once every 12 months.

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5. Non-Compliance

Individuals who violate this policy may be denied access to AUBMED information technology resources. In such situations, AUBMED may suspend, block, or restrict access to an account.

Individuals found to have violated this policy may also be subject to legal as well as disciplinary action, up to and including termination of employment.

6. Acknowledgement

I, _____, the undersigned acknowledge that I have read and understood this policy and consequences of non-compliance.

Signature _____ Date _____

7. Proprietary Information Revision History

Date of Change	Responsible	Summary of Change
April 15 2024	Suzanne Elhorr	Initial draft
September 2025	Suzanne Elhorr	Final Draft