AUB Office of Information Technology: Code of Conduct

Introduction

Individuals working at the AUB Office of Information Technology (hereafter indicated as IT@AUB) hold positions of trust. We operate and protect AUB's central information technology assets, including networks, computers, telephones, access controls, information, and databases. We provide technology-related services that are vital to the smooth functioning of AUB and to the members of the AUB community. In these roles, every one of us must adhere to the highest professional and ethical standards.

This Code of Conduct applies to all IT@AUB employees, including student employees, as well as to all others who work for IT@AUB as consultants, contractors, temporary staff, or in any other capacity, on a full-time or part-time basis.

Failure on anyone's part to comply with these standards may lead to disciplinary action, up to and including dismissal, as well as referral, as appropriate, to authorities for legal action. IT@AUB reserves the right to amend this Code of Conduct at any time and without notice, in its sole, good faith, discretion.

The purpose of this document is to help all of us in IT become and remain familiar with the Code of Conduct. This document should be read in conjunction with the Principles of Ethical Conduct, Code of Business Ethics and the other related policies such as Information and Computer Resources Use Policy, Intellectual Property, Privacy Policy on Electronic Communication and Files.

Seven guiding principles summarize the code. Information about each principle is provided in related sections of the Code, on pages indicated below.

All individuals working at the IT@AUB office are required to acknowledge that they have read , understood and are in compliance with this document when they join the team, and at least once a year there after.

Guiding Principles

For clarification of any item in the document or of any related policy, please consult your team leader, supervisor, manager, director, or anyone on IT@AUB Leadership Team.

I. COMPLIANCE

Guiding Principle: *It is your responsibility to stay familiar with and comply with the policies, laws, and regulations that affect your AUB responsibilities.*

Relevant policies, laws, and regulations include, but are not limited to, the AUB employment policies, and specific IT@AUB policies, as well as e-commerce law, copyright law, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and other US and Lebanese applicable laws.

IT@AUB strive to help individuals fulfill their obligations to remain up-to-date with the regulations and compliance needs by providing information and links on the Internal and External web sites, briefings about relevant policies, laws, and regulations, as well as guidance and training available and various meetings.

Any work outside of the IT department (Internal or external to AUB) should be approved by IT Leadership and in accordance with the AUB Ethical Code of conduct, conflict of interest, HR policies and law.

II. AUB COMMUNICATIONS

Guiding Principle: It is your responsibility to safeguard *the confidentiality, privacy, and security of AUB communications.*

As a US institution operating in Lebanon, we need to comply with both Lebanese and US law. US Federal law prohibits unauthorized disclosure of communications of any kind (voice, data, e-mail, or other non-voice communication) transmitted over AUB's networks or the public or private networks that AUB utilizes, or even the fact that a transmission was sent or received.

You are therefore required to:

1. Keep confidential what you see and hear when handling transmissions that use voice, data, facsimile, and other technologies, as well as when onsite visits providing any IT@AUB service. Information from any communication or the fact that a communication has taken place may not be used for your personal benefit or for the benefit of others.

2. **However, if you learn of an emergency involving immediate danger of fatality or serious injury, immediately contact the AUB Protection Office (+ 961 1 350 000 ext 2400).** Then, immediately report that contact and the related information to IT@AUB management, i.e., your immediate supervisor or a member of the IT@AUB Leadership Team.

3. Except when explicitly authorized by IT@AUB Leadership Team, and after ensuring that you are complying with the Privacy Policy, do not comply with any request for providing such information as:
   - who is talking or has talked on a circuit;
   - who communicates or has communicated by e-mail or other electronic means;
   - who transmits data to or from a particular location on the AUB network or the Internet;
   - the specific location a person or computer is transmitting to or receiving from;
   - what has been communicated;
   - the nature of the business being handled.

   Refer to IT@AUB Leadership team any subpoena or other request for information. (See Section V.)

4. Keep unlisted phone extensions, e-mail addresses, and related data confidential. Some telephone extensions, e-mail addresses, and other data are not listed in AUB directories for specific reasons. Such information should not be disclosed, except when explicitly authorized by the IT@AUB Leadership Team and after ensuring that you are complying with the Privacy Policy.

5. Listening to, reading, monitoring, recording voice or data communications, as well as permitting such behavior by others are all prohibited activities, except to the extent that you have been authorized to do so by IT@AUB Leadership Team for the performance of your job and after ensuring that you are complying with the Privacy Policy.

6. Do not permit the installation or use of any device, which permits anyone to listen to, record, observe, or access the content of any communication transmitted over the AUB network or observe that a communication has taken place, except if explicitly approved by the IT@AUB Leadership Team and after ensuring that you are complying with the Privacy Policy. Any indication that someone has attempted to violate the privacy of a communication should be reported immediately to the IT@AUB Leadership Team. Examples of this behavior include attempts to gain access to circuits or records, connect monitoring devices, obtain password files or network data, conduct unauthorized network sniffing, obtain unauthorized access to databases or services, or obtain billing information.

7. Establishing unauthorized access or enabling anyone to access AUB services without having the proper approval to gain this access is prohibited. Do not permit anyone to connect any device to AUB facilities unless you are authorized to do so and unless the device is connected in accordance with IT@AUB practice, is installed in a safe manner, and is intended for legal use.

III. AUB DATA AND RECORDS

Guiding Principle: *Protect the accuracy, privacy, confidentiality and security of AUB data and records.*

Accurate and reliable data are essential for AUB operations. Data kept on systems managed by IT@AUB and/or serviced by individuals from IT@AUB include a wide range of subjects and must be kept accurate and available for authorized purposes at any time. These data should be disclosed only to authorized AUB personnel with a legitimate need and be compliant with the data classification policy.

You are required to:

1. Be vigilant in safeguarding records and data, including paper files and computerized records. Records containing sensitive information and data about individuals require especially attentive protection to safeguard individual privacy and to ensure their confidentiality, integrity, availability, and auditability.

2. If the work you perform entails servicing computers owned by or assigned to other members of the AUB community, it is your responsibility to maintain the privacy, security, and accuracy of the contents of the computer. You may not read, copy, or transmit any data or information found on that computer without the consent of the person responsible for the computer. Backups of the contents of the computer must be properly secured, in accord with practices approved by the IT@AUB Leadership Team.

3. Sensitive data should not be left in a public place where others may view them. Public places may include unattended fax machines or printers as well as your personal workspace. In an open workspace, take extra care to ensure that sensitive data are not left on an unattended computer screen

or out in the open. Cabinets and computers that include these records must remain secured and accessed only for authorized purposes. All backups must be properly secured.

4. The willful, unauthorized destruction, alteration, attempted destruction or alteration of AUB data, as well as making false entries or failing to make correct entries in AUB data, are violations of AUB policy and, in some instances, of the law.

5. Report to IT@AUB leadership anyone who tries or is suspected of trying to alter, destroy, steal, or obtain unauthorized access to records or data.

6. Ensure proper disposal of data containing AUB information, whether recorded on paper, magnetic media, optical media, or any other format, and properly dispose of computers, multifunctional printers, or other electronic storage devices according to the AUB policies.

IV. AUB FACILITIES, SYSTEMS, AND SERVICES

Guiding Principle: *Protect AUB services, systems, premises, property, and equipment from damage, disruption, attack, or intrusion.*

Information concerning the facilities, systems, and services that IT@AUB plans, provides, or uses could be of interest to someone who seeks to misuse or destroy them. Be careful to prevent inadvertent disclosure of sensitive information, including information about AUB's physical plant, plans for service, future construction, restoration procedures, and security procedures. Privileged access should not be breached. Report any violation or suspected violation to the IT@AUB Leadership Team.

1. Access to AUB facilities, systems, and equipment is restricted to authorized individuals. Exercise extreme care to prevent unauthorized access to facilities, systems, and services and disclosure of data, passwords, identification media and information, and sensitive procedures. Loss or theft of keys or access devices used for entry into controlled-access areas should be reported immediately to IT@AUB management. IT@AUB has a special responsibility to protect administrative access to systems and databases.

2. **If you learn of an emergency involving immediate danger to AUB facilities or encounter an unauthorized person in them, immediately contact the AUB Protection Office (+961 1 350 000 ext 2400).** Then immediately report that contact and the related information to IT@AUB management. If you suspect that an AUB system has been breached, report it immediately to IT@AUB security services (it.security@aub.edu.lb) and to IT@AUB management.

3. Do not divulge sensitive information concerning IT@AUB plans facilities, services, operating arrangements, costs, or other internal activities to anyone, including another AUB employee, who is not authorized to know it. Locations of equipment, circuits, trunks, cables, and systems should not be shared with unauthorized persons. Do not display, disclose, or transmit information from or about security systems, including lock and surveillance systems, to anyone outside IT@AUB without IT@AUB management permission.

4. Comply with building admissions procedures established by the AUB and AUB Office of Protection at each AUB location. Report to IT@AUB management any attempts to enter controlled IT@AUB space by someone who may be unauthorized to do so.

5. Individuals in IT@AUB are responsible for the protection and integrity of equipment issued to them for on-campus or off-site use. Likewise, individuals are expected to apply prudent security measures to all personally-owned equipment that they use in support of AUB business. Policies and procedures

covering the proper use of office and off-site equipment are issued periodically and must be followed.

V. REQUESTS CONCERNING AUDITS, INVESTIGATIONS OR INFORMATION

Guiding Principle: *Fulfill requests for audits, information or to conduct investigations concerning AUB data or facilities only with the express authorization of the IT@AUB Leadership Team*

1. Any court order, warrant, or subpoena requesting such investigation or release of AUB records or information must be referred first to the AUB CIO as appropriate, for consultation with AUB Legal Office. You may not take individual action to comply with the request.

2. Refer all requests from other AUB offices, or non-AUB organizations or individuals for information or investigations of records or facilities managed by IT@AUB to your director or any other member of the IT@AUB Leadership Team and AUB CIO for authorization; you may not take individual action to comply with the request.

3. All requests should be routed to IT@Security to log all requests for information. The log should include requestor name, date, purpose for request, description of requested access and the duration of the access.

VI. PROPRIETARY AND COPYRIGHTED INFORMATION

Guiding Principle: *Abide by copyright and intellectual property laws, policies and ownership agreements.*

Work products and software created by individuals working in IT@AUB as part of their job responsibilities are owned by AUB.

1. Except for internal IT@AUB use, any copyrighted materials, including copyrighted publications and vendor documentation should not be copied without the permission of the copyright owner. This includes manuals, newspapers, trade journals, magazines, and other publications, as well as copyrighted materials distributed in other media such as audio and video.

2. It is IT@AUB policy not to use software unless it has been properly licensed and paid for, and it is registered, as required, with the manufacturer.

3. Software and work products, whether developed or customized by IT@AUB, are proprietary to AUB. They should not be shared with anyone outside of our workgroups without express permission of IT@AUB. We recognize that sharing appropriate information with certain communities inside and outside AUB can provide significant benefit in the pursuit of our duties. This guideline is not meant to preclude such normal and customary exchanges of information, including the sharing of code where appropriate and authorized. Nevertheless, it is expected that official copyright policies and guidelines will be observed.

4. In general, in software acquisition agreements, AUB agrees not to take any action, such as reverse assembly or reverse compilation, to devise a source code equivalent of vendor software delivered in object code form. Such actions are therefore not permitted.

5. IT@AUB employees may, from time to time, enter into specific non-disclosure agreements with vendors. We must act in accordance with these agreements, taking care to not disclose trade secrets, private, financial, technical, and business information.

6. Except for publicly filed tariffs, the rates that AUB pays for services are typically proprietary. Do not disclose either the rates or the bills and invoices that reflect the rates unless authorized to do so by IT@AUB management.

VII. AUB BUSINESS DEALINGS

Guiding Principle: *Prevent personal interests from influencing AUB business dealings.*

Be aware that relationships with a supplier might create a conflict of interest or might appear to impair independence of judgment on behalf of AUB. Purchasing decisions should be made in accordance with the established policies and guidelines of IT@AUB and AUB. When in doubt, seek guidance from your immediate supervisor.

1. Maintaining certain interests outside of IT@AUB while an individual fulfills fiscal responsibilities at AUB may potentially create a conflict of interest. Fiscal responsibilities include managing budgets, preparing budget recommendations, authorizing expenditures, managing contracts, and other financially influential responsibilities. Designated IT@AUB staff members with such responsibilities are expected to disclose potential conflicts of interest - in accordance with the AUB policy on Duality of Interest or Conflict of Interest.

2. Any negotiation with suppliers on contracts or purchases on behalf of AUB need to be coordinated with theCampus Procurement and Contracts Administration Department. Avoid making arrangements or commitments with any supplier or contractor with whom you have a personal interest, either direct or indirect, except under the express direction of IT@AUB management and full coordination with the Campus Procurement and Contracts Administration Department.

3. No financial or contractual commitments for material or services may be made on behalf of the AUB, except with the express approval of IT@AUB management and coordination with the Campus Procurement and Contracts Administration Department.

4. In general, accepting or soliciting, even indirectly, gifts, loans, “kick-backs,” special privileges, services, benefits, or unusual hospitality is not permitted. Any exception made should be reported and approved by the AUB CIO.

I acknowledge that I have received, read, understood and agree to comply with the *AUB Office of Information Technology: Code of Conduct*

Name (printed)

_____

Signature

_____

Date

Please return this page to: AUB Office of the CIO