Table of Contents

Section 1 - Scope

Section 2 - Definition

Section 3 - Policy Statement

Section 4 - Access Authorization

Section 5 - Notification Protocol

Section 6 - Related Policies

Back to Top

(To download this policy in Word format, click here)
For any comments, feedback, or query, please contact: policies@aub.edu.lb.
Last updated on: March 21, 2014
Section 1 – Scope

This privacy policy applies to all individuals (Users) with an AUBnet USERID or with access to data files (as defined herein). Related and complementary AUB policies are listed at the end.

Section 2 - Definition

Electronic communications and electronic files collectively known as “Data Files” include: (1) electronic communications and electronic files stored on AUB-owned computers; (2) network communications including electronic mail and voice mail, stored on, encrypted on, or in transit to or from individual computer or voice mail accounts on AUB owned systems/devices; (3) telecommunications traffic (voice and data) using the university IT infrastructure.

Section 3 - Policy Statement

AUB recognizes the critical importance of privacy and expects all its Users to do the same. The purpose of this policy is to affirm and protect the privacy of Data Files and to describe the exceptional circumstances under which a User’s expectation of privacy may be subsumed to other values critical to ensuring the strong health and essential operations of the University.

In deriving this policy, the University does not endorse censorship, routine inspection of Data Files, or routine monitoring of the network activities related to individual Users. Moreover, university policies that govern freedom of expression in alignment with AUB’s mission also govern electronic expression.

Except as otherwise governed by applicable university policy, laws, employment or other agreements, or the terms of research funding or other similar arrangements, AUB does not claim ownership of underlying intellectual property rights, including copyright, in Data Files.

Following carefully prescribed processes, Data Files may be accessed by authorized university officials, without the consent of Users, under the following circumstances:

1. Operational Integrity
   a. To identify or diagnose vulnerabilities or problems or otherwise preserve the integrity of university IT systems or essential business functions.
   b. When there is a legitimate business reason to access the Data Files of Users who were members of the AUB faculty or staff when the User’s employment at AUB has ended.
2. **Emergencies**

   a. To address an emergency or to avoid or minimize exposure of the University to substantial risk of harm.

   b. To preserve public health and safety.

3. **Institutional Integrity**

   a. Where there is credible information that a violation of law or a significant breach of university policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

   b. To respond to the terms of a valid subpoena, warrant, other legal order or request, or when required by contract, sponsorship agreement, or an applicable law, rule, or regulation.

**Back to Top**

### Section 4 - Access Authorization

Consistent with the privacy interests of Users, this policy requires the following authorizations in the event of access to Data Files without the consent of the User:

1. **For the purpose of addressing operational integrity issues**: access shall be approved in writing in accordance with the regularly established policies and procedures of the University, including those specifically relating to Information Technology (IT).

2. **For the purpose of addressing emergency issues**: access shall be approved in writing by the university manager having responsibility for the operational area affected.

3. **For the purpose of addressing institutional integrity issues**: access shall be approved in writing by (a) the president in consultation with (i) the provost (for faculty and student related Data Files) or (ii) the chief operating officer (for staff related Data Files) or (b) the chair of the Audit Committee of the Board of Trustees in consultation with the board chair. Keeping in mind the privacy principles expressed in this policy, the president or the audit committee chair shall consider and determine, in their sole judgment, (a) the credibility of information relating to institutional integrity issues or the significance of a breach of university policy and (b) whether alternate means are available to obtain information needed to address institutional integrity issues.

Access to Data Files, with or without consent, requires clear written procedures and secure documentation of activity logs with alarm notification (or manual activity logs in circumstances where system generated logs are not available). The University, through systems administrators or other specifically authorized individuals, will log all instances of
access without consent. System administrators will also log any emergency access within their control for subsequent review by the president, provost, and COO, or the chair of the Audit Committee of the Board of Trustees.

In accessing or granting access to Data Files, university personnel will comply with all applicable university policies and procedures.

Section 5 - Notification Protocol

The affected User(s) will receive prior written notice that their Data Files will be reviewed, except when (1) prior notification is not feasible or appropriate due to the urgency or nature of the circumstances; or (2) such notice may result in destruction, removal, or alteration of data.

Where prior notification is not feasible or appropriate, reasonable efforts will be made to notify the affected User(s) as soon as possible following access, unless the nature of the circumstances make follow-up notification unnecessary or inappropriate.

Section 6 - Related Policies

Records Retention
Archives
Principles of Ethical Conduct
Code of Business Ethics
Information and Computer Resources*
AUB-IT-000005 Data Security*
Intellectual Property*
Privileged Access*
AUBnet (Email) Accounts*
AUBnet Residential Acceptable Use Policy*
AUBnet Code of Conduct for Users of Computing Systems and Internet Services*
Internet Code of Conduct*
Administrative Application (ADM-APPS) Data Access*
Information Technology Management Principles, Policies, and Guidelines*
System Authentication*

*To be reviewed and harmonized