Title: Systems Management Policy
Revision: 1.1
Owner: Samih Ajrouch

Contact Person
Samih Ajrouch
Interim Manager, IT Systems and Storage
American University of Beirut
samih.ajrouch@aub.edu.lb  |  +961-1-350-000 ext. 2275 | +961-3-699366

Note: When this document is released, it is to be followed and adhered to, and is subject to document AUB-IT-000001 “IT Document Control Policy”.

May 2013
TABLE OF CONTENTS

1. PURPOSE
2. AUTHORITY
3. MANAGING SYSTEMS
4. ACCESS RIGHTS
5. ACCESS TO ALL CORE SERVICES
6. INACTIVE CONNECTIONS
7. ACCESS TO COMMANDS AND FUNCTIONS
8. CHANGE MANAGEMENT
9. CAPACITY MANAGEMENT
10. PHYSICAL ACCESS
11. AUDIT TRAIL
12. SYSTEM TIME
13. SYSTEM PROTECTION
14. SOFTWARE UPDATES
15. AUTHORING HISTORY
1. Purpose

The purpose of this document is to describe applicable standards and guidelines for the American University of Beirut (AUB) policy on Information Technology System Management and ongoing operations. This document represents the industry best practices with which the University will align its IT system management and operations activities. This document shall be consulted prior to the acquisition and management of IT systems and ongoing operations.

2. Authority

This document describes applicable standards and guidelines for the university’s policy on Information Technology system management. This standard applies to all IT systems at AUB.

3. Managing Systems

The AUB information systems shall be managed, at all times, by qualified and trained System Administrators who will ensure proper daily operations and who will be responsible to apply necessary security and integrity measures in collaboration with system owners. These System Administrators in charge of systems management shall attend and follow particular training sessions emphasizing information security subjects.

4. Access Rights

Access Rights are a key issue that should be continuously controlled and logged. Access rights shall be maintained at all levels through a centrally managed service (whenever applicable) whereby any alterations in access rights must be approved by the authorized personnel. Logs on granted and revoked access permissions should be kept at all times.

5. Access to all Core Services

Access to any core service must be secured by a qualified logon process. Logon processes may not be limited to username and password and may include further constraints including time and location of access. To track any potential information system misuse, a log including access to any core service shall be kept and maintained for an appropriate period of time.

6. Inactive Connections

To avoid misuse and unauthorized access as a result of a non-logged-off authorized access (to any core service), inactive connections must be terminated after connection is idle for a specific period of time.
7. Access to Commands and Functions

Access to commands and functions which might alter a system’s normal operation shall be restricted to those persons who are authorized to perform systems administration or management functions. The use of such commands and functions should be logged and the logs preserved for an appropriate period, when applicable.

8. Change Management

The deployment of new or upgraded software must be carefully planned and managed. A formal Request For Change (RFC) form must be submitted and approved by the head of the concerned head of the IT department before any major change is implemented. Audit trails shall be used for all changes to systems. Changes must be tested, reviewed, and authorized before moving the new or upgraded software to the production environment.

9. Capacity Management

Capacity management of systems supporting business processes shall be monitored and projections planned for future capacity requirements made to enable adequate processing power, storage, and network capacity to be made available.

10. Physical Access

Physical access to all critical systems must be restricted to authorized persons only. Changes to the access list must be appropriately authorized before authorizing physical access to a particular system.

11. Audit Trail

Security event logs, operational audit logs, system event logs and error logs must be reviewed properly and periodically.

12. System Time

All core services clocks must be synchronized with an approved NTP server. One main NTP server shall be identified with which all systems must synchronize.

13. System Protection

All University systems shall be protected from virus and other malicious software infection using software and hardware products procured by the University’s Office of Information Technology for this purpose.
14. Software Updates

All University information systems shall run appropriately supported systems software that must incorporate all relevant security updates.
15. Authoring History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Reason for Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08-06-2012</td>
<td>Samih Ajrouch</td>
<td>Initial Document Creation</td>
</tr>
<tr>
<td></td>
<td>22-10-2012</td>
<td>Joe Hage</td>
<td>Updated Doc ID and Cover Page Date</td>
</tr>
<tr>
<td>1.1</td>
<td>24-05-2013</td>
<td>Samih Ajrouch</td>
<td>Updated document content</td>
</tr>
</tbody>
</table>