LEBANESE AMERICAN UNIVERSITY
INFORMATION SECURITY POLICY

Approved by the President's Cabinet on February 25, 2008
Approved by the Board of Trustees on March 27 & 28, 2008

Policy Statement:

Each member of the University community (faculty members, staff, students and alumni) is responsible for the security and protection of University information and information resources over which he/she has control. Resources to be protected include; networks, computers, computer systems, telecommunication systems, applications and data. The integrity and confidentiality of information must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to third party entities must comply with the same security requirements as in-house activities.

Policy Purpose:

In order to fulfill its mission and goals, the University endeavors to provide a secure, yet open, network that protects the integrity, and confidentiality, of information while maintaining its accessibility.

University information, and information technology resources, must be recognized as sensitive and valuable, and must be protected. Depending on the scope and classification of the information, integrity constraints, and special procedures for access and handling, must be required.

Policy Scope:

This Policy applies to all University faculty members, staff, students, alumni, guests, consultants, contractors, and any other person having access to University information. All third parties who have access to University information must agree, in writing, to maintain information confidentiality, integrity and availability.

Roles and Responsibilities:

All members of the University community share in the responsibility for protecting University information.

The IT Security Department must:

- Implement, monitor, update, and enforce the Information Security Policy.
- Develop and promote security awareness.
- Head the Computer Security Incident Response Team (CSIRT)

The IT Academic Advisory Committee and the IT Administrative Advisory Committee (drawn from the IT department, faculty, and professional staff to engage the University

constituencies in setting recommendations regarding academic and administrative strategic IT needs) must:

- Review and make recommendations to the Information Security Policy and Procedures.
- Advise on the University's adherence to the Information Security Policy and Procedures.
- Appoint formal application owners, and specify their information ownership responsibilities.

The application owner must:

- Work with IT personnel to classify, and periodically reclassify, University information which he/she has been charged with, by determining the sensitivity, and criticality levels.
- Provide authorization for users to gain access to the information.
- Report suspected or known compromises of information to the IT HelpDesk team.

The authorized user must:

- Comply with the Information Security Policy and Procedures and Guidelines.
- Report to the IT HelpDesk team any abnormal or prohibited event, or behavior, related to the University information technology resources.

The HelpDesk team must:

- Notify the IT Security Department of any IT security incident.

The Computer Security Incident Response Team (CSIRT) must:

- Promptly, and correctly, handle emergencies and incidents so that they can be quickly contained, investigated, and recovered from (examples are: virus infections, hacker intrusions, denial of service attacks).

Detailed regulations on the following topics will be prepared and updated regularly:

- Organizational Security
- Asset Classification and Control
- Personnel Information Security Management
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Management
- Business Continuity Management
- Compliance

Enforcement:

All members of the University community must comply with this Policy. Non-compliance may lead to disciplinary action by the University, including, but not limited to, revocation of computer use privileges. Disciplinary action may also result in dismissal from the University.

The Information Security Policy is a living document, and should be reviewed and reassessed regularly to determine if revisions are needed to accommodate the fast changing nature of information technology.