# Lebanese American University
# Information Security Policy

Each member of LAU community (board members, officers, 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 and/or access to. In order to maintain its mission and goals, LAU endeavors to provide a secure, yet open, network that protects the integrity, and confidentiality, of information while maintaining its accessibility.

LAU information, and information technology resources, must be recognized as sensitive and valuable, and must be protected. The Information Security Policy (the "Policy") ensures that all users or networks of the IT structure within the organization's domain abide by the regulations regarding the security of data stored digitally within LAU and its affiliates.

**Roles and Responsibilities:**

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

The IT Department must:

- Implement, monitor, update, and enforce the Information Security Policy.
- Develop and promote security awareness.

The Application Owner (s) in defiferent departments recognized as such by the IT Deparment 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 from LAU community must:

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

The IT HelpDesk team must:

- Promptly notify the IT Security Department of any IT security incident.

The IT Advisory Team 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 may be found in the Information Security Regulations:

1. Application Development Regulations
2. Awareness Regulations
3. Backup and Recovery Regulations
4. Bring Your Own Device Regulations
5. Clean Desk Regulations
6. Computer and Network Regulations
7. Data Centers Regulations
8. Email Regulations
9. Exceptions Regulations

10. Exceptions Request Form
11. Firewall Regulations
12. IT Security Department Regulations
13. IT Staff Regulations
14. Log Management and Monitoring Regulations
15. Password Regulations
16. Password Construction Guidelines
17. Portable Computers Regulations
18. Servers Regulations
19. Software Licenses Regulations
20. Virtual Server Regulations
21. Virus and Malicious Codes Regulations
22. Wireless Regulations

**Effective Date:**

The foregoing Information Security Policy of the Lebanese American University was amended by the Board of Trustees on September 6 & 7, 2018 and is effective as of September 7, 2018. This Policy was originally effective as of March 28, 2008.