Version Number: 1.0
Implementation Office(s): it

Information Security Framework

Purpose

AUB Information Systems and institutional data must be protected from unauthorized access, loss, or damage by complying with information security principles framework that is defined by a set of system and data security policies and procedures.

Responsibilities

Position/Office/Role	Responsibilities
Executive Management	The CIO is responsible for overseeing the development, implementation, and maintenance of the IT security program. He ensures the security process is governed by policies and practices.

Principles

The information security framework secures and ensures:

- AUB information assets against theft, fraud, malicious or accidental damage
- Data Confidentiality (data and information is accessed only by those authorized to do so and used only for authorized purpose.)
- Data and information integrity (data and information not modified inappropriately)
- Data and information availability (data and information is available when required)
- Data and information traceability (data and information access is tracked to avoid and be aware of any illegal movements)
- AUB meets its legal and contractual obligations.
- Safeguard the reputation of AUB
- Foster an information security culture.

Framework Principles:

1. Proper measures must be taken at all times to ensure that the right people access the right information at the right time.

2. All data must be categorized and protected based on its sensitivity and possible impact arising from improper access and modification.

3. Policies must be put in place to ensure compliance with applicable laws and standards that protect data confidentiality, integrity, and ownership. At minimum, there must be policies to cover the below

Policy	Matched Principle
Data Classification	Categorized data according to sensitivity
Identity and Access Management Policy	Ensure Proper Access
Information and Computer Resources Acceptable Use	Outline the acceptable use of information systems and data, and other resources at AUB

4. Proper information security education, training and awareness must be delivered throughout AUB.

5. Proper measures and guidelines must be put in place to reduce risks associated with uncontrolled changes to information-processing environment.

6. Measures must be taken to ensure that data is not unintentionally changed in transit.

7. All data systems must be protected from unauthorized access (physical and remote).

8. Measures must be taken to minimize the effects of system failures, disasters or disruption and take the necessary steps to ensure that the business is able to resume operation in a timely manner.

9. Processes must be put in place to regularly identify the vulnerabilities and threats to systems with critical AUB data, and to assess the possible impacts to determine where to implement security controls.

Definitions

Information System
Any electronic system that stores, processes, or transmits information.

Institutional Data
Data that is owned or licensed by AUB.

History and Review

Originally Issued

21 February 2019 by Suzanne Elhorr

Next Review Date

February 2022