October 2022

Document title: [Information Security Policy – October 2022]

Approval date: [May 2017]

Purpose of document: [To define AUC's information security program main pillars and components]

Office/department responsible: **[** Office of Information Security**]**
Approved by: **[** Mr. Brian MacDougall - Executive VP for Administration & Finance
Ms. Hanan Abdel Meguid - Vice President for Digital Innovation
Ms. Nagwa Nicola – Chief Technology Officer**]**

Document classification level: [PUBLIC]

Document accessible: [www.aucegpyt.edu/xxx/xxx]

Related documents/see also: [Acceptable Use Policy, Email Policy, Servers Policy, Password Policy, Peer-to-Peer File Sharing Policy]

Information Security Policy

Policy Statement

Information Security is one of the AUC organization's control areas, with responsibility for ensuring that our information assets are adequately protected. The American University in Cairo (AUC) Information Security Policy is a critical component of our security framework.

Reason for Policy/Purpose

Since AUC is committed to providing excellence in its services, information security/cybersecurity is an important pillar among the whole organization's activities that need to be defined, prioritized, and executed as per the business needs. AUC is committed to complying and covering all requirements demanded by US Federal institutions, International standards like ISO 27001, and US and Egyptian laws and regulations. AUC senior administration is committed to supporting this policy and other related ones to deliver the adequate information security level to all stakeholders

Who Approved This Policy

Mr. Brian MacDougall - Executive VP for Administration & Finance
Ms. Hanan Abdel Meguid - Vice President for Digital Innovation
Ms. Nagwa Nicola – Chief Technology Officer

Who Needs to Know This Policy

All AUC community in general

In specific, AUC community members involved in sponsoring, developing, designing, approving, supporting, implementing, administrating, operating, or otherwise delivering Information related/IT solutions must read and comply with this document.

Management has specific responsibility for ensuring that relevant staff are aware of and comply with this material.

AUC students, faculty, staff, contractors, partners, and any person who interacts with AUC information are targeted by this policy

The reader is also subject to Acceptable Use Policy and other developed AUC policies

Web Address for this Policy

Please list the location on the university's website where this policy is located.

Contacts

Responsible University Official: **Wessam Maher, Chief Information Security and Risk Officer**

Responsible University Office: **Office of Information Security.**

If you have any questions on the policy or procedures, you may send an e-mail to **infosec@aucegypt.edu**

Definitions

None

Policy/Procedures

1 Information security framework

Information Security is a specialist area within the university's operational risk management. The head of Information Security "Chief Information Security and Risk Officer" is responsible for formulating strategy, policies, and standards and for maintaining a consistent and effective information security framework across AUC.

2 Information Security Office

The primary role of the Information Security office is to set the AUC's agenda for Information Security, its communication, and implementation as well. It ensures that the information security processes are implemented in a consistent, risk-based manner across AUC. These activities are concerned with delivering an optimum Governance, Risk, and Compliance state within the Information Security scope. A framework/program for these activities is prepared by Information Security head, including policies, principles, standards, technical architecture, and methodologies that must be used throughout AUC.

Below are some main components of the Information Security strategy and program: -

2.1 Risk Assessment

Information Security requirements must be identified through a methodical assessment of risks. Expenditure on controls needs to be balanced against the business harm/cost likely to result in case the risk has been exploited. Risk analysis considers:

a) Identifying mission-critical information systems and repositories

b) The business harm is likely to result, taking into account the potential consequences of a loss of confidentiality, integrity, or availability of the information and other assets; whether tangible or non-tangible
c) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and the controls currently implemented.
d) Assessing the risks posed by business partners, cloud services adoptions, and integrations.
e) Determining legal and compliance implications and contingent liability concerns.
f) Ensuring Information solutions are hardened and patched in accordance with industry best practices.

According to the university's risk appetite, the identified risks are handled through one of the following actions: - Risk Acceptance, Risk Avoidance, Risk Limitation, or Risk Transfer.

AUC will ensure to perform Information Security risk assessments in periodic and ad hoc ways, whether done by internal or external entities, in order to manage Information Security priorities and activities. Also, AUC will be taking into consideration the continuously evolving threats mindset plus confirming that proper controls are in place as well as taking into consideration any new business requirements and priorities.

2.2 Digital Forensics Investigations

The Information Security Office is responsible for conducting Information security investigations and digital forensics activities with regard to any AUC's digital nature subjects. Also, the office is responsible for collecting and validating any digital information/logs and acts as a central point of contact with any investigation parties, whether internally or externally.

Accordingly, the Information Security office has the right to request data, metadata, technical logs, and history input from AUC system's owners and administrators within the investigation's scope and through documented communication.

2.3 Business Continuity and Disaster Recovery Plans

As business continuity and disaster recovery activities are risk-based activities, the Information Security Office is responsible for leading these activities with regards to the Information and systems sides through planning, data collection, formulating business impact analysis, validating plans' components,…etc.

2.4 information security awareness program

AUC's management, faculty, and staff are the main targets for the Information Security awareness program in order to cover all threats related to human behaviors that can affect AUC assets. On the other hand, students' awareness is important, as well as they are the end customers who use AUC systems. Information Security office is responsible for planning and managing all activities related to this subject

2.5 Digital solutions acquisition assessment

Overseeing and evaluating digital solutions and service providers from Information Security's perspective is an essential task in order to ensure that proper safeguards are in place to protect AUC's valuable assets.

2.6 Penetration testing

Penetration testing is an essential activity for detecting vulnerabilities in the system and for checking how effective the controls are in preventing any breaches. Information Security office is responsible for managing these activities, whether the testing is done through internal resources or an external entity.
Caution must be exercised while running these activities in order to safeguard AUC resources from crashing, non-controlled data exposure, or unplanned downtime.
All these activities must be done with a pre-defined and aligned scope.

2.7 Vulnerability Management

Vulnerability/patch management is an ongoing risk-based task that is led by Information Security to ensure that all systems are patched and updated against security threats. The actual implementation of patching is done by the respective operations teams.

2.8 Continuous Monitoring Activities

The Information Security Office is responsible for establishing a business-accepted Information Security Operation Center (SOC) that will monitor, respond to, and report any security violation or suspicious behavior. Accordingly, all needed feeds and data logs from AUC systems need to be accessible in order to provide the proper visibility and, accordingly, better detection and protection of AUC's assets.

2.9 Design validation

Information Security office is responsible for assessing Information systems design like network systems, software systems, cloud solutions, hardware security adequacy, …etc. in order to ensure that security requirements and constraints are implemented on the ground. Read procedures, hardening guides, and checklists are to be generated for reoccurring assessments.

2.10 Information Lifecycle

Information Security office evaluates and enforces security controls and design restrictions towards the information lifecycle and its related systems, whether regarding the Information processing, storage, classification, disposal, transmission, …etc.

3 Continuous Improvement

AUC will ensure to evaluate the output of all the above components in order to adjust the Information Security program adequately and continuously.

Forms/Instructions

List applicable forms or other university and external documents that provide helpful, relevant information. Include where these documents can be located.

Related Information

List related university policy documents or cross-references and where they can be located.

Appendices *(optional)*

Appendices are used for informational material that is helpful in understanding the policy but not directly related to the implementation of the policy, i.e., not procedures. Content may include graphics or text.

History/Revision Dates

Origination Date:	May 2017
Last Review Date:	October 2022
Next Review Date:	October 2025