October 2022

Document title: **Data Classification Policy - October 2022**

Approval date: **August 2018**

Purpose of document: **The document governs the data classification for AUC data.**

Office/department responsible: **Office of Information Security.**

Approved by: **Wessam Maher, Principal Campus Information Security Officer**

Document classification level: **PUBLIC**

Document accessible: **[[https://www.aucegypt.edu/about/university-policies]]**

Related documents/see also: AUC Data Governance Policy, Information Security Policy, Electronic Mail Email Policy, Acceptable Use Policy, Peer to Peer Sharing Policy

Data Classification Policy

Policy Statement

AUC data assets must be classified, labeled, and protected appropriately.

Reason for Policy/Purpose

This policy will facilitate the following: -

- Data will be shared responsibly with partners
- Data will be held securely
- Confidentiality will be assured
- Regulatory and legislative requirements will be met
- Business continuity plans will be prioritized according to the data classification category
- All breaches of confidentiality will be weighted according to affected data classification severity.

Who Approved This Policy

Wessam Maher, Principal Campus Information Security Officer

Who Needs to Know This Policy

AUC Staff and Faculty

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

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, you may send an e-mail to infosec@aucegypt.edu

Policy/Procedures

1. All data entered into, stored within, reported from, or transported physically or digitally via the AUC network, systems, hosted/outsourced systems, or departments is the property of AUC unless there is a legal agreement/applicable law that documents a different relation.
2. All AUC data, despite its format, must be identified and counted in an inventory among each unit/department and ultimately through the data trustees.
3. All AUC data must be classified into one of the following categories:
    a. AUC CONFIDENTIAL – pertains to all data of the highest sensitivity due to its' time-sensitive, possibly financial, or fraud potential. Such data includes all types of identifiable information, social security numbers, account numbers, payroll, personal information, passwords, code, client relations/engagements, and contracts under negotiation.

b. AUC SENSITIVE – pertains to all data having compromising or competitive elements or implications intended strictly for use within AUC. Such information includes basic financial information, security and audit information, and associate information.

c. AUC INTERNAL – pertains to all information created by an individual user of the system and is not meant to be generally shared with others. The unauthorized disclosure of this information reasonably could be expected to cause low substantive damage to AUC reputation, financials, or client relations. Such information and communication informational is intended by the creator for a specific audience only.

d. AUC PUBLIC – pertains to all data that does not require specific accountability and/or audit trails for use. The unauthorized disclosure of this data would not cause any adverse impact on AUC's reputation, financials, or client engagements. Such information includes non-strategic information, publicly available information, or non-specific application information.

4. The classification of data is independent of the technology or platform on which it is processed.
5. The access rights of data given to users and stewards should be consistent across all areas. Particular attention should be paid to data that can be downloaded or exported.
6. Data access rights, classification, and acceptable security/protection mechanisms are governed by data domain trustees and ultimately by data trustees. Information Security's role is to assess and recommend the proper controls.
7. Information Technology tools administrators are data custodians to the assigned container application/service unless the data is related to their approved business scope.
8. All data must be classified from the start of the information/data collection and development.
9. Data classified higher than Public must be:
   a. Labeled appropriately
   b. Its final format out of systems should carry the appropriate labeling.
   c. Reviewed by the appropriate manager, trustee, and Information Security for implementing the appropriate security measures to control access to this data.
10. The marking should reflect the sensitivity of the material in any output format. Output includes printed reports, magnetic media, electronic messages, and file transfers.
11. Data often ceases to be sensitive after a period of time, for example, when the data has been made public. Data classification should be updated as needed.
12. Data classification awareness and training to staff, faculty, students, and all applicable entities must be performed regularly through Data trustees, Data domain trustees and Information Security.
13. According to the Data classification, a proper retention and disposal mechanism/process must be developed and applied. This mechanism/process must be approved by the Information Security office and ultimately by the Data trustees.

Exceptions

Exceptions should be a minimum; if they exist, they should be approved by Data trustees and Information Security Office.

Enforcement

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action, up to and including termination of employment or dismissal from the University

Related Information

AUC Data Governance Policy
Information Security Policy
Electronic Mail Email Policy
Acceptable Use Policy

History/Revision Dates

Origination Date:	December 2015
Last Amended Date:	August 2018
Last Review Date:	October 2022
Next Review Date:	October 2025