October 2022

Document title: **Digital Asset Disposal Policy – October 2022**

Approval date: **June 2018**

Purpose of document: **The document explains the requirements for the disposal of AUC digital assets in order to secure the confidentiality of AUC data that could have been stored on them.**

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

Approved by: **Nagwa Nicola, Chief Technology 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

Digital Asset Disposal Policy

Policy Statement

AUC digital assets must be cleared adequately from any AUC data before any disposal action

Reason for Policy/Purpose

The purpose of this policy is to enable AUC to: Ensure the community is fully aware of the required security needed to protect its data while disposing of any digital asset by doing the proper cleaning and wiping for AUC data.

Who Approved This Policy

Nagwa Nicola, Chief Technology Officer
Wessam Maher, Principal Campus Information Security Officer

Who Needs to Know This Policy

Entire AUC community

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

Definitions

Term (alphabetical order)	**Definition as it relates to this policy**
Digital assets	AUC supplied/provisioned electronic devices like computers, laptops, tablets, phones,….etc.

Policy/Procedures

1. Users who use AUC digital assets are primarily responsible for ensuring that any AUC data are kept out of any device that will be replaced, disposed or sold
2. IT is responsible for wiping and securely cleaning all devices/digital assets before it is transferred to the AUC warehouse
3. Wiping/Secure cleaning action applies to all kinds of digital assets. Exceptions are handled by the information security office
4. Secure cleaning instructions are set by the Information Security Office and may differ according to the asset type
5. Warehouse and inventory functions should ensure that IT certifies any asset that goes in or out of the warehouse, whether for internal use or for being disposed of or sold, is cleaned securely.
6. IT and the warehouse should keep an inventory of cleaned devices with their proper identification. Example: - FA number, Serial number, …etc.

7. According to stored data criticality and information security feedback, some assets need to be disposed of physically or have their hard disks destroyed physically.

Exceptions

Exceptions should be a minimum; if they exist, they should be approved by the 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
Peer to Peer Sharing Policy

History/Revision Dates

Origination Date:	December 2017
Last Amended Date:	June 2018
Last Review Date:	October 2022
Next Review Date:	October 2025