October 2022

Document title: **[IT Data Center and IT Rooms Access Policy – October 2022]**

Approval date: **[March 2018]**

Purpose of document: **This document addresses the management of access to the IT data center and IT rooms**

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 **]**

IT Data Center and IT Rooms Access Policy

Policy Statement

AUC central digital computing assets must be protected; by all means, this includes securing adequately the physical security of IT devices located in the IT data center and IT rooms. All reasonable controls should be implemented as securing AUC data starts with securing the devices and core network infrastructure.

Reason for Policy/Purpose

The purpose of this patch management policy is to enable AUC to:

Ensure the community are fully aware of the requisite security needed to secure the data centers and IT rooms from any unauthorized access

Who Approved This Policy

Nagwa Nicola, Chief Technology 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	Definition as it relates to this policy
Vulnerability	Weakness in system or application that allows attackers or abusers to take advantage and affect the system/application confidentiality, integrity, or availability.
Patch	Is a code or software update that covers/solves a certain vulnerability
Digital Computing Asset	PC, Laptop, Server, Printer, Network device, storage device, phones……etc.

Policy/Procedures

1. All infrastructure devices and IT services should be protected from any physical tampering, sabotage, interference, or unauthorized physical access.
2. All IT services and their associated devices shall be collected in centralized, physically protected places like data centers and dedicated IT rooms in buildings.
3. Devices setup and arrangement should follow international standards to ensure adequate protection for the assets.
4. Data Centers and IT rooms should be protected by appropriate physical controls like appropriate locks and CCTV surveillance according to the criticality.

5. Data Centers and IT rooms cannot be used for any other purpose or as a storage facility.
6. Access to Data Centers and IT rooms should be granted to authorized persons only.
7. Visitors must be escorted at all times.
8. All visits and access actions should be logged appropriately.
9. Protection against disasters and environmental incidents should be well implemented.
10. Access rights should be reviewed periodically.
11. When applicable, racks doors should be locked
12. Access controls logs and CCTV surveillance recording logs should be kept adequately, and historical data should be kept for an acceptable time span.
13. Central IT Office is the only entity authorized to allow the creation of IT data centers and IT rooms, Schools and special research units should grant IT formal approval.
14. AUC IT services shouldn't be allocated outside the approved central IT data center/IT rooms. Exceptions must be approved by both the CTO and Chief Information Security and Risk Officer.

Exceptions

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

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:	March 22nd, 2018
Last Amended Date:	March 22nd, 2018
Last Review Date:	October, 2022
Next Review Date:	October 2025