Document title: **Digital Computing Asset Management – February 2018**

Approval date: **February 2018**

Purpose of document: **This document is to keep the AUC community aware of the existence of security requirements to protect the digital computing assets of the university.**

Office/department responsible: **Office of IT**

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 Computing Asset Management

Policy Statement

AUC digital computing assets must be protected by all means and listed by a rigid inventory. No violations of use are accepted. AUC has the right to protect its assets and ensure its compliance.

Reason for Policy/Purpose

The purpose of this digital computing asset security policy is to enable AUC to ensure community are fully aware of the requisite security needed to protect a digital computing asset, be it in a secure office environment or any other location and describe the controls necessary to minimize information security risks affecting AUC digital computing assets.

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
Responsible University Office: Information Security Office
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 computing assets	AUC supplied/provisioned electronic device like computer, laptop, tablet, phone….etc.
Malware	Malicious or unwanted computer program that can steal data and or harm the data/device

Policy/Procedures

1. Users who use an AUC digital computing asset are primarily responsible for its safekeeping and for the security of any information it contains. Users must protect AUC digital computing asset to minimize the possibility of loss or theft, unauthorized use, or tampering.
2. Users must follow all IT and Information Security rules, guidelines, limitations concerning the protection of AUC digital computing asset and its content.
3. IT and Information Security have the right monitor the use of digital computing asset for purposes of security, compliance and administration purposes.
4. IT and Information Security have the right to limit and control the scope of use of the digital computing assets to serve AUC objectives efficiently and effectively.
5. IT and Information Security have the right to install and enforce software packages and features changes for enabling/disabling features, limiting administrator privileges, measuring performance and applying security controls. Users doesn't have the right to disable, control or limit these actions. A documented approval and risk acceptance must be signed for any exception.
6. IT and Information Security must approve and validate all purchasing requests for digital computing assets to ensure its adequacy from operational and security perspective.
7. All data output, analysis outcome, application developed, research results…etc. that are resulted and realized through the use of AUC digital computing asset are considered owned by AUC unless an formal exception is granted by AUC senior management.
8. AUC digital computing assets should only be used for AUC approved business needs only
9. Cryptocurrency mining using AUC digital computing assets is forbidden.
10. Digital computing assets should be compliant to copyright laws, telecommunication laws and all applicable laws
11. Whenever required by law, AUC will provide relevant information and access to digital computing assets to law enforcement entities

12. AUC has the right to access, collect and confiscate any digital computing asset for investigation, digital forensic, or compliance needs. Access rules and procedures are handled by Information Security, Legal and Physical Security offices.
13. AUC has the right to analyze the outgoing and incoming traffic to any digital computing asset connected to its network for performance management, problem solving, information security and compliance needs

Inventory

A digital computing asset inventory must be in place that include all relevant digital data like MAC address, operating system type and version, device vendor, model name and number, list of software installed name and version….etc. This inventory is essential for operational support, upgrade plans as well as information security controls enforcement and risk assessment.

Inventory of newly added assets and retiring assets should be performed adequately.

Live inventory/monitoring tools and agents can be used to identify the device status when applicable.

Ownership

Ownership of digital computing assets must be documented and adequately updated at all times. Digital computing assets must be delegated to a custodian/person at all times.

Assets Return

Digital computing assets should be returned to AUC as the ultimate owner whenever the asset is not in use, outdated, the owner has ended his/her relation with AUC.

University Servers and Associated Applications

1. Ownership of AUC servers and its associated applications must be clarified and documented at all times in a detailed inventory.
2. An application admin and a system admin should be identified for every AUC server and digital service
3. Application and system admins are data custodians, data owners have the ultimate hand on access granting and revoking.
4. Application admin is the responsible person for operating and maintaining the application to meet the business objectives.
5. System admin is the responsible person for operating and maintaining the operating system and any server backend services/packages that are essential for the application to run.
6. New AUC servers/services/applications must have the following prerequisites before going live: -
    a. Documented high and low level architecture
    b. Data flow chart
    c. Documented risk assessment and business impact analysis

Acceptable Use of digital computing assets

1. Ensure that you log out and clear your data and credentials when you use any public access computer, like lab/library PCs
2. The physical security of AUC digital computing asset is your responsibility, so take all reasonable precautions. Be sensible and stay alert to risks.
3. Keep AUC digital computing asset “that is in your custody” in your possession and within sight whenever possible. Be careful in public places such as airports, railway stations, or restaurants.

4. If you have to leave the digital computing asset temporarily unattended in the office, meeting room, or hotel room, even for a short while, use a digital computing asset security cable or similar device to attach it firmly to a desk or similar heavy furniture whenever applicable or put it in a safe if applicable.
5. Lock the digital computing asset away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet, or safe. This applies at home, in the office, or in a hotel. Never leave a digital computing asset visibly unattended in a vehicle.
6. Carry and store the digital computing asset in a padded bag or strong briefcase to reduce the chance of accidental damage.
7. Keep a note of the make, model, serial number and AUC asset label of your digital computing asset, but do not keep this information with the digital computing asset. If it is lost or stolen, notify AUC Physical Security, the police and inform the IT help/service desk immediately.
8. Outside office hours, digital computing assets that are left in office must be properly closed and secured in a suitable locked cabinet within their place of work whenever applicable.
9. You must use approved encryption software on all AUC digital computing assets whenever applicable, choose a long, strong encryption password/phrase and keep it secure. Contact the IT help/service desk for further information on digital computing asset encryption. If your digital computing asset is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.
10. You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends, or IT staff.
11. University digital computing assets are provided for official use by authorized persons. Do not loan your digital computing asset or allow it to be used by others such as family and friends.
12. Don’t store personal data on AUC assets, accidental access and storage can be acceptable.
13. Avoid leaving your digital computing asset unattended and logged-on. Always shut down, log off, or activate a password-protected screensaver before walking away from the machine.
14. Malwares are a major threat to AUC and digital computing assets are particularly vulnerable if their anti-virus/anti-malware software is not kept up to date. The antivirus software MUST be updated at least weekly.
15. E-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.
16. Always virus-scan any files downloaded to your digital computing asset from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically, but the IT help/service desk can tell you how to initiate manual scans if you wish to be certain.
17. Report any security incidents (such as virus infections) promptly to the IT help/service desk to reduce the damage.
18. Respond immediately to any virus warning message on your computer or if you suspect a virus (by unusual file activity) by contacting the IT help desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

19. Do not download, install, or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into AUC networks as well as affect the working condition of your digital computing asset.
20. Software packages that permit the computer to be remote controlled (e.g., Team viewer, PC anywhere...etc.) and hacking tools (network sniffers and password crackers…etc) are explicitly forbidden on AUC equipment unless they have been explicitly preauthorized by information security office for legitimate business purposes.
21. Be careful about software licenses. Most software, unless it is specifically identified as freeware or public domain software, may only be installed and/or used if the appropriate license fee has been paid.
22. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period.
23. You must ensure that you manage to run regular backups of data on your digital computing asset.
24. You need to ensure that backups are encrypted and physically secured.
25. AUC will not tolerate inappropriate materials such as pornographic, racist, defamatory, or harassing files, pictures, videos or e-mail messages that might cause offense or embarrassment. Never store, use, copy, or circulate such material on any digital computing asset and steer clear of dubious websites.
26. If you receive inappropriate material by e-mail or other means, report it to IT help desk or delete it immediately
27. Portable digital computing assets normally have smaller keyboards, displays, and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Wherever possible, place the digital computing asset on a conventional desk or table and sit comfortably in an appropriate chair to use it.
28. If you tend to use the digital computing asset in an office most of the time, you are advised to use a docking station with a full-sized keyboard, a normal mouse, and a display permanently mounted at the correct height.

Related Information

AUC Data Governance Policy
Information Security Policy
Electronic Mail Email Policy
Acceptable Use Policy
Peer to Peer Sharing Policy
https://www.aucegypt.edu/about/university-policies

History/Revision Dates

Origination Date: January, 2016
Last Amended Date: February, 2018
Next Review Date: October, 2019