October 2022

Document title: **Patch Management Policy- October 2022**

Approval date: **March 2018**

Purpose of document: **The document addresses management of patching activities to protect AUC assets**

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

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**]**

Patch Management Policy

Policy Statement

AUC digital assets must be protected by all means and listed by rigid and reasonable patching activities. Vulnerabilities should be patched adequately. AUC has the right to protect its assets and ensure its compliance.

Reason for Policy/Purpose

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

Ensure community is fully aware of the requisite security needed to patch a digital asset and describe the patching controls and constraints to minimize information security risks affecting AUC digital assets.

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 (alphabetical order)	**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 Asset	PC, Laptop, Server, Printer, Network device, storage device, phones……etc.

Policy/Procedures

1. All AUC digital assets, systems, or services should be patched and updated against any security vulnerability.
2. The patching scope includes but is not limited to:- operating systems, applications, database systems, program components, …etc.

3. All Information Systems shall be maintained to be patched continuously and as fastest as possible.
4. This policy is considered a general patch management procedure and shall apply to all Information Systems, digital assets, or services by default. Information Systems with special requirements may be maintained following a specific patch management procedure developed by the Data Custodian and approved by Information Security.
5. Patches must be checked for compatibility with all system components prior to being applied
6. Patches must be successfully tested on non-production systems prior to being loaded on production systems unless otherwise documented in an approved special patch management procedure
7. All patches must obtain the appropriate change control approval prior to deployment on production systems.
8. Patching shall be performed during an authorized maintenance time window unless there is an urgent situation.
9. Critical system data shall be backed up prior to the installation of new patches.
10. In general cases, the maximum tolerance time to have AUC systems/services stay unpatched is 45 days. According to vulnerability severity, Information Security will decide to shorten this tolerance time to minimize risk to AUC assets and reputation.
11. The patching process is a joint responsibility of both system's administrator and application administrator. They should work closely to ensure that.
12. Data domain trustees and data stewards are accountable for providing adequate support and maintenance time windows to enable data custodians, system and application administrators to patch the systems as needed.

Users' Managed Assets

1. Users managed assets like PCs and laptops, …etc. should be patched adequately by AUC. User is not responsible for the patching process; however, users should adhere to IT and Information Security communications with regards to any associated responsibilities like bringing the device to campus/IT, restarting the machine, stopping using certain software….etc.
2. Some users' managed assets may have some extra administrative privileges that are granted to its users, like the ability to install, uninstall programs/updates; these granted users are responsible for adhering to IT and Information Security constraints and communications with regards to patching and to execute them as needed. Violators will be revoked their administrative privilege, and disciplinary actions will be taken against them.

Patch Management

Information Security oversees the patching process all over AUC; progress reports and new patch releases should be delivered continuously. A formal and updated asset inventory

Exceptions

Exceptions should be minimum; if they exist, the Information Security Office should approve them, Data Trustee, and Data Domain Trustee.

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 29th, 2018
Last Amended Date:	March 29th, 2018
Last Review Date:	October, 2022
Next Review Date:	October 2025