October 2022

Document title: **[System Development Policy – October 2022]**

Approval date: **[April 2018]**

Purpose of document: **[System development should be done properly according to international standards to serve business needs. Proper security requirements must be met by the developed systems]**

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**]**

System Development Policy

Policy Statement

System development should be done properly according to international standards to serve business needs. Proper security requirements must be met by the developed systems.

Reason for Policy/Purpose

The purpose of the System Development Policy is to manage system development activities in AUC to have a more controlled outcome that performs its goal efficiently, effectively, and securely.

Who Approved This Policy

Wessam Maher, Principal Campus Information Security Officer

Who Needs to Know This Policy

AUC Faculty and Staff

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 email to infosec@aucegypt.edu

Policy/Procedures

1. System development should be done by the right trained caliber in order to ensure the best quality of the delivered outcome
2. A data owner should be declared and assigned to own the collected, published, or processed data in the system to be developed.
3. System development includes all digital development activities like software development, application development, mobile application development, workflows development, website development, …etc.
4. International standards and processes should be followed by the developers' teams, like CMMI, OWASP…etc.
5. Source code should be securely saved and kept with proper versioning, description, and documentation
6. Development should be done in a testing environment; another staging environment should be used for near-life systems. No direct changes or development is allowed in production.
7. Proper design and requirements specifications must be documented.
8. A proper stakeholder's acceptance and sign-off should be done by the development phase.
9. A proper assessment of current alternatives, consolidation options should be considered.
10. Developers shouldn't operate or maintain the developed system. It should be handed over to application administrators with proper day-to-day running manuals.

11. Proper security segregation must be done between the front ends, middle layers, and back ends
12. Developed systems have to pass by security assessment to evaluate their readiness to go live.
13. Communication between systems should be secure by design.
14. Proper vulnerability and patch management should be performed for any developed system.
15. System regular assessment should be done to tackle the system's usability, effectiveness, and efficiency in order to decide whether it should retire, be replaced, or be kept in production.
16. No untrusted source codes, functions, libraries, or APIs are allowed to be used in system development.
17. Proper quality assurance and stress testing should be performed as needed.
18. Before granting system development actions, an assessment must be done by the proper management in order to compare whether a ready-made option would be April 2018

    more feasible to AUC or not from operational, support, and security perspectives
19. Proper security hardening guides should be followed for all system components.
20. Proper logging capabilities should be designed and enabled to integrate with the AUC information security event management solution. Logging capabilities options and features should be discussed and approved by data owners and information security.
21. A proper business continuity/disaster recovery plan should be in place before the system goes live.
22. Proper secure access control and roles segregation should be developed as needed. Information Security should be involved from the design part.
23. Proper authentication should be done when needed. Information Security should be involved with regard to the authentication need and mechanisms.
24. All developed systems' information and ownership should be kept in a proper inventory.
25. All related processes and development activities must be documented and saved for future reference.
26. An application administrator and system administrator should be assigned to every developed system.

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:	April 2018
Last Amended Date:	April 2018
Last Review Date:	October 2022
Next Review Date:	October 2025