| | |
|---|---|
| **Policy Title** | Information Technology: Software Development Policy. |
| **Responsible AIU Office**<br>**(Higher Management/Directorate)** | Chief Information Officer (CIO) |
| **Policy Owner**<br>**(Executive Department/Office)** | Information Technology Office<br>Information Security Office |
| **Pertinent Dates** | April, 2022. |

## I. SCOPE OF POLICY

This Policy applies to all employees (i.e., faculty, staff), consultants, and/or contractors involved in the development or modification of enterprise-level centrally-managed mission-critical applications that support AIU.

## II. DEFINITIONS

**Application:** Computer programs, procedures, rules and associated documentation and data pertaining to the operation of a computer system.
**Mission Critical:** A system or application whose failure will result in the failure of University operations.
**System Development Life Cycle (SDLC):** A standardized process for planning, creating, testing, and deploying an application.

## III. POLICY STATEMENT

Information Technology Services ("ITS") is responsible for developing, maintaining, and participating in a System Development Life Cycle ("SDLC") for AIU software projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for sensitive AIU information.

All enterprise-level centrally-managed mission critical applications developed at or for AIU must adhere to development standards and procedures documented in the ITS Application Development Standards guide. These standards include: coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards and regulatory requirements. There must be a separation between the production, development and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems.

## IV. RESPONSIBILITIES

This Policy is under the jurisdiction of ITS Application Development. The interpretation and application of this Policy is the responsibility of the Application Architect. Final decisions related to this Policy will be made by Director of System Development, where required.

## V. POLICY STANDARDS AND PROCEDURES

All applications are reviewed at predetermined checkpoints of the SDLC by the Application Architect or their designate. Any deviations are identified and corrective action is determined prior to the application being released to production. Electronic authorization indicating standards have been met is required before a new or modified application can be released to production. ITS enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the ITS Help Desk. Policy violations that come to the attention of the ITS Help Desk will be escalated to the Director, Application Development. Policy violations will be assessed and action taken to remediate the violation subject to AIU Bylaw and / or other contractual conditions. Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the ITS for further action. Periodically, the CIO will provide to AIU President a summary of all policy violations.

## VI. FORMS/INSTRUCTIONS (if applicable)

N/A

**Formatted:** Font: Bold

**Formatted:** Font color: Purple

**Formatted:** List Paragraph

## VII. APPENDICES (if applicable)

The SDLC process will adhere to the following information security controls:
Adequate procedures should be established to provide separation of duties in the origination and approval of source documents. This shall include but not be limited to separation of duties between Personnel assigned to the development/test environment and those assigned to the production environment.
Modification of code or an emergency release will follow the change control standard. Secure programming standards should be followed. Secure code training should be provided to User flow's developers.
Secure development environment will be created, based on: sensitivity of data to be processed, stored and transmitted by the system; applicable external and internal requirements, e.g. from regulations or policies; security controls already implemented by the organization that support system development; trustworthiness of personnel working in the environment; the degree of outsourcing associated with system development; the need for segregation between different development environments; control of access to the development environment; monitoring of change to the environment and code stored therein;
backups are stored at secure offsite locations; and, control over the movement of data from and to the environment.
All software deployed on Corporate or Hosted infrastructure must prevent security issues.
Code changes are reviewed by individuals other than the originating code author and by individuals who are knowledgeable in code review techniques and secure coding practices.
Overrides of edit checks, approvals, and changes to confirmed transactions should be appropriately authorized, documented, and reviewed.
Application development activity should be separated from the production and test environments. The extent of separation, logical or physical, is recommended to be appropriate to the risk of the business application or be in line with customer contractual requirements. The level of separation that is necessary between production, development, and test environments should be evaluated and controls established to secure that separation.

All changes to production environments should strictly follow change control procedures, including human approval of all changes, granted by an authorized owner of that environment. Automated updates should be disallowed without such approval.

Active production environments should not be re-used as test environments. Inactive and/or decommissioned production environments should not be used as test environments unless all private data has been removed. Test environments should not be re-used as production environments without going through a decommissioning and decommissioning process that cleans all remnants of test data, tools, etc.

Individuals who are responsible for supporting or writing code for an internet-facing application, or internal application that utilizes web technology and handles customer information, should complete annual security training specific to secure coding practices. For individuals supporting or writing code for an internet-facing application, training should also include topics specific to internet threats. The individual should complete the training prior to writing or supporting the code.

Custom accounts and user IDs and/or passwords should be removed from applications before applications become active.

## VIII. RELATED POLICIES

- Technology Acquisition Policy.
- Technology Updating/Lifecycle Management Policy.
- Web Development and Updating Policy.

## VIV. CONTACT INFORMATION

- Information Technology Office, ito@aiu.edu.eg
- Information Security Office, iso@aiu.edu.eg

| | | | |
|---|---|---|---|
| **Triggered by:** | AIU Council | Date | Sig. |
| **Created by:** | Executive Team | Date | Sig. |
| **Revised by:** | Revision Team, IT unit. | Date | Sig. |
| **Approved by:** | Senior Administrative Council | Date | Sig. |