جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	System Acquisition and Development	Last Review date	19/5/2021
	Policy Number	IT-29	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

The objective of this Policy is to ensure all aspects of Acquisition and management of Information Systems and Applications developments are conducted as per the operations, security, change and release management processes set forth by the university of Sharjah's Information Technology Centre.

Scope

The scope of this policy applies to UoS ITC and third party vendors involved in the Acquisition, Application development and management of Information Systems.

Purpose

The purpose of this policy is to ensure that the operational and security requirements are considered throughout the application development life cycle. (SDLC).

Abbreviations and Definitions

SDLC – System Development Life Cycle

Policy

General

1. The university of Sharjah ITC shall ensure that controls to develop coding practices shall be implemented and followed based on the following high-level steps:
    a. Business requirements analysis
    b. UAT scenario development and use case
    c. High-level design and system testing plan
    d. Low-level design and integration testing plan
    e. Coding and development
    f. Unit testing
2. Coding and programing practices shall be performed by ITC or coordinated with third party vendors / outsourced parties to ensure that:
3. Information Systems business, academic and security requirements and specifications are included in all phases of application development.
    a. Secure processing of Information Systems is included when developing software for UoS.
    b. Securing Information Systems Files, Source Codes and Data is considered.

c. Managing Changes in Software Development is based on UoS ITC change management process.
d. Testing is done to ensure secure development of software.
e. Deployment of Information Systems / Applications is followed
f. Cryptographic Controls are considered on need basis.

Inception and business case

1. ITC business and academic requirements should be included in all business cases, requests for proposals and work requests, related to acquisitioned or in-house developed.
2. ITC shall approve the systems design documents addressing the business, academic and security requirements covering all the relevant platforms (e.g. operating systems, browsers, portable computing devices, etc.)
3. ITC shall approve the secure coding standards for information systems software / mobile application / web application development.
4. ITC shall approve the design of the architecture for the development & deployment of information systems.
5. ITC shall implement adequate configuration management process during information systems design, development, implementation and operation.

Development of software

1. Develop and follow a System Development Life Cycle (SDLC) process.
2. Securing the development environment by adopting strong access management controls and segregation of duties, to handle source code.
3. Identifying business, academic and security requirements of the software during the design phase of the project.
4. Controls shall be adopted to track version changes to the source code and software.
5. Security Modules shall be applied to the application, which covers all secure controls.
6. If third party software is being considered for critical business / academic activity, UoS ITC should license the source code from the third party where ever feasible.
7. Use of open source software will be allowed after appropriate approval based on a formal Risk Assessment.
8. Systems acceptance and user acceptance tests shall be done before deploying the source code to production.
9. Input validation and output validation checks shall be conducted.
10. Test data shall be secured during testing to ensure the confidentiality of classified data.

11. Periodically testing software code of all information systems/ applications developed in house or by an external party.
12. Security tests shall be done on a regular basis to identify vulnerabilities in critical systems and an action plan shall be developed to close the vulnerabilities. Tests include, but not limited to:
    a. Application penetration test
    b. Dynamic application test
    c. Source code test
    d. Relevant infrastructure environment test

Deployment of code to production

1. Change Management Process shall be implemented and followed.
2. Secure coding shall be adapted on both staging and production environments.
3. The change shall be effectively communicated to the stakeholders before adopting to the production environment. This communication shall produce details including the dates and duration of the change and shall be approved by the stakeholders.
4. Changes shall have roll back plans defined to revert to original settings, if required.
5. Relevant system deployment procedure shall be followed
6. All information systems / applications shall be deployed after confirmation of proper implementation of security controls and security sign off.

Security in Software Development

1. Protection of development environment
    a. No changes to any software shall be made until its goes through a formal Change Management Process
    b. Any new software, code or technology shall be evaluated, before it is deployed into production
    c. Access to source code and test data shall be controlled
    d. Segregation of duties will be adopted, to ensure that the same personnel will not have access to code and production at the same time.
    e. Backups shall be taken frequently for critical information. (E.g. Source code, settings and register entries)
2. In the software design phase, security and privacy concerns shall be included. In addition, a structured approach to threat scenarios during design phase shall be planned.
3. Security code review shall be conducted to analyze the source code prior to compile.

4. Final security review usually shall include examining threat models, tools outputs, and performance against the quality requirements and bugs defined during the Requirements Phase.

Acquisition

1. Acquisition, deployment and upgrade of information systems, should address the University of Sharjah's requirements for ensuring proper change management process implementation and in line with UoS's baseline configuration requirements, prior to acceptance or deployment of the software.
2. The application / software acquisition shall consider the following requirements, at minimum:
    a. University of Sharjah shall specify to the supplier the availability requirements of the acquired software / IT service. This will be documented in the form of a service level agreement, which should address scheduled operation time, performance level, downtime, availability measurement, and performance monitoring and error analysis.
    b. Service Level for Reporting, Review and Resolution.

Exception

Minor code changes for existing production service shall be approved internally as per change management process

In an exceptional situation where development is carried out ITC boundaries a Risk acceptance and control measures shall be provisioned.

Out of scope:

Research dev in academic environment which is not deployed to UOS IT production

Departments which are doing their own developments

Reference

Sl No	Standard Name	Control Reference
1	ISO 27001:2013	A.14.1.1, A.14.2.2, A.14.2.4, A.14.2.5, A.14.2.7, A.14.2.8,

		A.14.2.9, A.14.3.1