CITY UNIVERSITY OF HONG KONG
Information System Acquisition, Development and Maintenance Standard

---

(Approved by the Information Strategy and Governance Committee in December 2013; revision 1.1 approved by Chief Information Officer in September 2015)

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2015-10-19

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-06-19	Typo corrections and multiple rephrases Added “Agile” to sample list of SDLC methodologies Removed the term “System controller” to avoid ambiguous Replaced “IT Security Officer” with “Information Security Unit” Modified to required “source code review for security” to be conducted for systems which process “CONFIDENTIAL” or “RESTRICTED” information

Distribution

Copy	Issued to	Location
Master	Public	http://www6.cityu.edu.hk/infosec/isps/docs/?page=00.about

Contents

1 Policy Statement

The City University of Hong Kong ("University") must ensure all information system projects are authorized and tested prior to implementation. The initiating departments are responsible for ensuring the developed system meet the goals and objectives required by the users and the Information Security Policies and Standards of the University.

2 Objective

This policy is established to specify the security practices during information system acquisition, development and maintenance, in order to ensure sufficient security in all information systems, and prevent errors, loss, unauthorized modification or misuse of information in the University's information systems.

3 Scope

This standard covers the development or acquisition of new information systems, or major modification of existing systems of the University. Both in-house developed and outsourced developed systems are covered in this standard.

4 Project Planning and Feasibility Study

During the planning phase of the Software Development Life Cycle ("SDLC"), the Project Initiator shall assemble the project team, which includes staff from both the Project Initiator's unit and external service provider, if any.

Head of Department shall appoint a system owner, who is a member of the unit, and fully responsible for the quality of project management and deliverables (e.g. scope, cost, time, fitness for use, etc.) of the project. The project team shall select an appropriate SDLC methodology to follow, such as traditional waterfall, Rapid Prototyping, Rational United Process, Agile, etc. Assistances and advices from Central IT should also be sought if needed.

The Project Initiator should establish a high-level view of the intended project and determines its goals. The Project Initiator is required to specify the business requirements for new information systems in the planning documentation. Security controls should be considered during project planning, and advice from Central IT could be sought when needed.

5 System Analysis and Requirements Definition

System owner is normally the person accountable for the overall business and application features and functionality of the system. The System owners shall ensure that security is built into their information systems.

System owner should liaise with the users and define the detailed user requirements.

System owner shall work with trained Information Security professionals to identify, justify, agree, and document security requirements in relation to the user requirements.

6 System Design

Security controls shall be designed into information systems to detect or prevent errors, unauthorized modification or misuse of information. These controls should include but not limited to:

- Validation of data input to applications systems to ensure that it is correct and appropriate
- Audit trail logging to maintain record of user activities for ensuring the traceability and accountability of users for their actions taken
- Incorporation of validation checks into systems to detect corruption caused by processing errors or through deliberate acts
- Encryption to safeguard the confidentiality, integrity and authenticity of classified data during transmission or in storage
- Message authentication techniques for applications to protect the integrity of message content from unauthorized changes or corruption
- Effective security controls to protest against common vulnerabilities identified in
    - OWASP Top Ten Project of the Open Web Application Security Project (OWASP) < https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project >
    - CWE/SANS Top 25 Most Dangerous Software Errors of SANS Institute < http://www.sans.org/top25-software-errors/ >
- Periodic vulnerability assessment to identify potential risk of information leakage and security weaknesses

7 Application development

The project developers shall bear in mind the importance of information security throughout the whole project lifecycle. Security loop holes, such as back doors, unused variables, opened ports, shall be properly removed or disabled after use. To identify security loop holes and vulnerabilities, the developers and the system owner could arrange to conduct static code scanning for vulnerabilities by trained personnel. For systems which process “CONFIDENTIAL” or “RESTRICTED” information, source code review for security shall also be conducted by trained personnel.

Application developers shall work on the approved change requests and shall only make the required changes.

8 Protection and Segregation of Environments

Development, testing and production environment shall be established for developing, testing and operations of business application software. If resources permit, this separation shall be achieved via separated physical or virtual computer systems. Otherwise, separate directories or libraries with stringent access controls shall be employed.

To ensure that IT development and support activities are conducted in a secure manner, access to information system files shall be controlled by the system owner, who is responsible for:

- Ensuring strict controls are exercised over the implementation of software on operational systems.
- Ensuring all information system test data is protected and controlled.

Development and support environments shall be strictly controlled to maintain the security of information system software and data. These controls can take the form of:

- Strict control over the implementation of changes to minimize the potential for corruption of information systems.
- Test data / software / hardware shall be distinguished from production data / software / hardware.
- Changes shall be justified, assessed for risk, tested and approved by the business owner before being introduced into the production environment.
- Procedures shall be established so that emergency changes can be made in a controlled manner with proper user authorization, documentation and audit trails. In case where programmers need access to production environment, special temporary accounts or access will be created. These temporary accounts shall be disabled upon completion of the emergency change.
- When changes to the operating system occur, review of information systems shall be conducted to ensure that there is no adverse impact on security.
- Discouraging the modification of vendor-supplied software packages.

Migration of application software from one environment to another shall be processed by authorized personnel. Application developers shall only be authorized to move software from development to testing environment, but shall not be allowed to move any software into the production environment.

In case the developer is also responsible for deploying software into production environment, compensating control must be implemented to prevent and/or detect developers from making unauthorized changes.

9 Testing

Changes shall be tested and approved by the system owner before being introduced into the production environment.

The project team should develop a “Test Plan” for the new or modified information system. The “Test Plan” shall include the tests to verify if security requirements are satisfied.

10 Security assessment

Security assessment shall be conducted to ensure that the security level of information system is satisfactory.

The system owner shall be responsible for checking and ensuring that all tests specified in the “Test Plan” are satisfactorily completed. The result of tests shall be endorsed by the Project Initiator’s management.

11 Installation and Deployment

Staff responsible for deployment should collect the program source codes from the testing environment, store them into the production source code library, and compile the source codes to become executable in the production environment.

Production source code shall not be changed in response to an emergency change. Instead, a controlled temporary version or a patch will be created and executed, until the production source codes have been reviewed by an independent developer.

A post execution review shall be conducted for each change deployed to the production environment, whether scheduled or unscheduled, to determine if the change is successful or not.

12 Maintenance

12.1 Change Management

Any subsequent change requests of the new or modified information system after production deployment must be handled in accordance with the "Change Management Standard".

12.2 System Documentation and Training

The project team shall prepare a "User Manual" to provide guidance and instruction on how to use the functionalities of the new or modified information systems. The "User Manual" shall be stored in a location accessible to all University's members that use the new or modified information systems.

The project team shall also prepare an "Administration and Operation Manual" to provide instructions on regular maintenance and housekeeping activities, and guidelines on error handling and diagnosis.

If necessary, training sessions should be arranged by the project team and the Project Initiator's management to facilitate users and applications for using the new or modified information systems.

13 Roles and Responsibilities

For details of roles and responsibilities, refer to "Change Management Standard" which also controls this "Information System Acquisition, Development and Maintenance Standard".

13.1 Project Initiator and Change Initiator

Project Initiator and Change Initiator could be any stakeholders of the information system. The Project Initiator shall initiate project by raising a Change Request Form or appropriate documents to the corresponding system owner and acknowledges the successful or failure completion of the project deployment. The Change Initiator may also be responsible for performing the User Acceptance Test, if there is no other designated Change Tester from the user departments.

13.2 System Owner

System Owner is the representative of the Project Sponsor. Typically, System Owner is assigned by the Head of Department which capitalizes or funds the project or service.

The System Owner is responsible for managing the information system development projects and ensuring that the deliverables meet the user specifications and the University's security requirements.

The System Owner is responsible for monitoring the overall project progress and liaises with the Project Initiator's management, qualified Information Security professionals and the CAB to resolve the outstanding issues encountered during the project life cycle.

The System Owner shall ensure that proper information security features are considered during the project planning and design stages and built into the system during the entire development lifecycle. Resource for achieving security requirement shall also be planned and reserved during the project planning and design stages.

The System Owner shall also ensure that information security assessment is conducted to evaluate the security posture of the system, and launch the system only if the appropriate security level is attained.

If the information system will process CONFIDENTIAL or RESTRICTED information, or information will be used in the public Internet or student intranet, the System Owner shall notify the IT Security Unit for the intention of building the information system.

13.3 Change Advisory Board or System Owner

The Change Advisory Board ("CAB") is a group of representatives including representatives of sponsor, user and technical experts. If CAB is not set up, the functions of CAB is performed by System Owner, who is the representative of the Project Sponsor.

The Change Advisory Board ("CAB") or System Owner is responsible for screening the Change Request Forms ("CRF") and determines the appropriateness of the project requests and the relevant project deliverables including "Information System Development Plan", "User Requirement", "Design Specification" and "Project Deployment Plan".

13.4 Information Security Unit (ISU)

The Information Security Unit (ISU) of the Office of Chief Information officer (OCIO) is responsible for providing advises on the University's security standards. The OCIO ISU is also authorized to conduct independent security assessment on all the Information Systems of the University.

14 Summary

The University must ensure information security is considered throughout the entire Software Development Life Cycle. Comprehensive quality checks on the system coding and test results should be completed with satisfactory conclusion prior to the production deployment. Full set of system documentation, including User manuals, and System Administration and Operation Manuals, should be provided. Training sessions and skill transfer sessions should be arranged to the relevant users and system administrators to ensure smooth transition to the new or modified information system.