CITY UNIVERSITY OF HONG KONG Communications and Operating Management Standard

(Approved by the Information Strategy and Governance Committee in January 2023)

PUBLIC **Date of Issue: 2023-01-28**

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2023-01-28	Revised the link and reference material in this document.

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/cio/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

The City University of Hong Kong or hereinafter referred as the "University" must ensure the correct and secure operation of information processing facilities.

2 Objective

This document describes the requirements and guidelines for the distribution of operational details and implementation of operational controls to reduce the likelihood of intended and unintended human errors.

3 Documented Operating Procedures

To reduce chance of human error and protect continuity of manual and/or automated operations, proper documentation of important normal and emergency functions should be developed and, maintained to ensure that they are current and relevant.

The scale and level of detail should be commensurate with the value, criticality and complexity of the information processing facilities. To reduce effort required in maintaining documents, documentation should be effectively and barely sufficient.

The correctness and readiness of documents are important and the University should ensure that:

- Users of manuals should report insufficiency and incorrectness to owner of documents
- The manuals should be reviewed and revised on a regular basis
- The manuals should be up-to-date, and latest version are distributed to all relevant staff
- Old versions should be removed on the arrival of new versions
- The manuals shall be secured from unauthorized modifications
- The manuals should be made available in the workplace for ease of access, e.g. published on-line using, or uncontrolled hard copies

Resources for developing and revising documents should be planned and allocated when planning for new or modification to existing systems, operations or processes.

3.1 Information System Documentation

Documented procedures in form of "User Manual" and "Administration and Operation Manual" should be provided to users and administrators who have roles in the operations on a need-to-know basis.

Documented procedures should also be used as training materials for new users.

"Administration and Operation Manual" should document sufficient instructions for execution of day-to-day activities carried out by system administrators to provide the services.

The manual should provide sufficient detail and information to enable responsible staff to work alone, independently. The follows should be documented:

- System Information
    - responsible personnel, physical location, network connection and power connection
    - Security requirements and information classification
- System Startup Procedure
- System Shutdown Procedure
- System Monitoring Procedure
    - Audit trails, performance and utilization thresholds
- System Backup Procedure
- Routine Jobs, including daily, monthly, yearly, etc.
- Clock synchronization
- System Availability requirements, work scheduling requirements, and interdependencies with other systems if any
- Diagnostic Procedures
- Error Handling Procedures
- Support escalation procedure and problem alert communication procedure

"System Administration Manual and Operation Manual (Document Template)" of Central IT serves as a template for manual writing.

"User manual" and "Administration and Operation Manual" are formal documents and controlled by the Change Management process documented in "Change Management Standard"

4 Segregation of Duties

The University shall allow no single person to access, modify, use assets, or subverting a critical process without authorization or detection. Roles and responsibilities shall be defined. The University should rotate and segregate duties and areas of responsibilities to minimize the chance of accidental or unintended access or modification, as far as resources are available and it is practical.

If duties are not segregated, the University shall implement appropriate detective controls such as monitoring of activities, audit trails and management supervision.

Information security audit and assessment must be independent.

5 Separation of Facilities

To reduce the risks of unauthorized access or changes to production (operational) environment, development, testing, and production facilities should be separated.

Development and testing software should run on a different computer system other than the computer system with production software. Production network should also be separated from development and test networks, as well as other production networks.

Access control should be implemented to enforce separation of facilities.

Transfer of software systems from development or test environment to operational facilities must conform to the "Change Management Standard"

Transfer of production data from production environment should be prohibited, unless with consent from data owner, controller or custodian. Sensitive data must be sanitized.

Compilers, editors and other development tools or systems should not be accessible from production environments when not required, and should be removed after use.

Reference

The following documents were consulted during the preparation of this document:

City University of Hong Kong (2023), *Information Security Policies*

City University of Hong Kong (2023), *Change Management Standard*