# CITY UNIVERSITY OF HONG KONG
# Change Management Standard

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

## 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 | | Typo corrections and multiple rephrases.<br>Replaced “IT Security Officer” with “Information Security Unit” |
| 1.2 | 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 ("University") must ensure that changes to the University's IT environment, including information systems, IT infrastructures and services, are necessary and will improve the quality of the IT environment. All changes must be approved by an appropriate level of management. Overall business risk related to changes must be optimized, and changes must be adequately tested before production roll-out.

# 2 Objective

This document provides the minimal process for the introduction of required changes into the IT environment with minimum disruption to ongoing operations. Details of change management processes may vary among different systems; however, the tasks in this minimal process should be implemented.

# 3 Definition

## 3.1 Changes

Changes are defined as any alternations that are deliberately introduced to the University's IT environment, which include the followings:

- Hardware
- Software
- System components
- Operation process
- Services

Changes can take the following forms:

- Permanent or temporary
- Upgrade of existing components of the University's IT environment
- Installation of completely new components to replace the outdated one
- Remove of service, and its associated components and documentation

Regardless of form, all changes falling under this definition must be managed by the change management procedures stipulated in the following context of this standard.

## 3.2 Standard Changes

Standard changes are those preauthorized changes that are fully defined and controlled by approved procedures, and are individually recorded, but are not individually assessed by Change Management. These changes are made routinely.

Standard changes have limited impact on the University's IT environment and its member. For example, change of network switch used for the University's Intranet; enhancement for the University's financial system by adding a new report.

Standard changes include routine changes that are performed repeatedly before and is part of the operational procedures of the University. For example, change of user profile in the University's information system.

### 3.3 Non-standard Changes

Non-standard changes are all other modifications of the IT environment that are not Standard changes described above. Examples of non-standard changes are addition of new features to the service or removal of features or existing services.

## 4 Responsibilities

### 4.1 Project Sponsor

The Project Sponsor is responsible for providing and securing resources, including financial, human and others, for the project.

### 4.2 Change Initiator

The Change Initiator initiates changes by raising a change request, and responsible for:

- complete all required details on the Change Request Form ("CRF")
- discuss and obtain appropriate authorizations from initiator's supervisor if applicable
- financial resources involved in the source (if any), and also responsible for obtaining approval from corresponding sponsor, after the price for change is concluded
- submit CRF to the corresponding Change Manager for approval
- conduct post execution review and acknowledges the successful/unsuccessful completion of the changes
- Perform User Acceptance Test, if there is no other designated Change Tester from the user department

Change Initiators could be anyone who is a stakeholder of the service concerned.

### 4.3 Change Manager

The Change Manager is responsible for:

- filtering, accepting and classifying all change requests
- assess the appropriateness and impact of changes, and prioritize change requests
- approve or obtain the required approval for change requests
- estimate resources (e.g. financial, human, etc.) required, risks and impacts of significant changes, from both business and technical viewpoints
- prioritize tasks and define change schedules for multiple change requests
- manage and control the change processes
- seek advice from Change Advisory Boards ("CAB") (see 4.4) when there are uncertainties in approving a CRF
- escalate to CAB if it is a critical change or this change request he or she cannot make up decision

With different change natures on different systems or IT services, different Change Managers will be responsible for making the decision (see section 6.4).

## 4.4 Change Advisory Board/ System Owner

### 4.4.1 Authority and Responsibilities

The Change Advisory Boards ("CAB") shall be established for the mission critical services of the University. For those services where CAB is not established, System Owner assigned by the sponsor must perform the functions of CAB. CAB or System Owner should be the final approval authority and decision-making body to approve or reject request of its service. Major responsibilities of CAB/Service Owner include:

- provide advice to the Change Manager on whether to approve changes;
- estimate resource required, risks and impacts of significant changes, from both business and technical viewpoints
- make decisions or provide recommendations on the adoption or rejection of significant changes;
- review change schedule and results of changes;
- monitor implementation status of significant changes;
- review the Change Management Process and identify areas of further improvements; such as sample check the changes to identify if there are wrongly classified or prioritized changes and monitor the change review process

Each assessment by CAB shall agree internally among the CAB members on the minimal number of votes needed to accept or reject a change request.

### 4.4.2 Composition

The CAB members should be selectively chosen to ensure that the requested changes are thoroughly checked and assessed from end-user usability, IT and operations perspective.

To streamline the Change Management Process, the CAB allows permanent and ad-hoc membership. Permanent members should attend all meetings held by the CAB and ad-hoc members should attend the meetings if certain IT or operations areas they concern are involved.

The representatives from the following areas shall be designated as permanent CAB member:

- System Owner
- User Manager, who serves as a liaison between the service team and users
- User Group, who represents the end users
- Application Developers
- Specialist Technical Consultants
- Service and Operations or related system(s)
- Third Parties (if outsourcing)

Members from technical and operations teams shall also evaluate security impacts of the changes. Members from Information Security Unit (ISU) of the Office of the Chief Information Officer (OCIO) should be requested to join the CAB when needed on an ad-hoc basis.

Ad-hoc membership can include the remaining Board members that are not designated as permanent.

## 4.5 Emergency Change Advisory Board (ECAB)

ECAB is a subset of Change Advisory Board that makes decisions about high-impact emergency changes. For services without ECAB, System Owner shall also perform the functions of ECAB.

## 4.6 Change Developer

The Change Developer is responsible for planning, developing and testing a change in the IT environment.

## 4.7 Change Tester

The Change Tester is responsible for performing the tests in accordance with the test plans / cases and documenting the test results.

## 4.8 Change Deployer

The Change Deployer is usually the Manager of the IT Operations Team and is responsible for verifying that the change has been tested and accepted, and authorizing the production release of the change. The Change Deployer is responsible for:

- implement changes into the production environment in accordance to the approved change requests
- manage and report the status of changes
- escalate any issues relating to the changes
- assists in the verification process which ensure the correctness of changes
- notify change manager for change completion

# 5 Process Flow Summary

This and the next section present the standard procedures for Change Management Process for the University.

System Owners may customize a Change Management Process suitable for the service, depending on properties of service such as size, complexity, scope, criticality, etc. However, the customized Change Management Process must be documented.

The following figure illustrates the process flow for change management, and the primary responsible parties for the corresponding tasks. The tasks and roles will be explained in the following sections.

| | |
|---|---|
| Change Recording | • Change Initiator |
| Filtering/Acceptance | • Change Manager |
| Change Classification | • Change Manager |
| Approval and Planning | • Change Manager or CAB/System Owner |
| Change Development | • Change Developer<br>• Change Tester |
| Change Execution | • Change Deployer |
| Post Execution Review | • Change Initiator |
| Management Review | • CAB/System Owner |

# 6 Change Management Process

## 6.1 Change Recording

If a change is governed by this Change Management Process, Change Initiator identifies the change and raises a change request by completing a Change Request Form ("CRF"), which is a formal document that records and keep tracks of change request. For different purposes, there could be different formats of CRF.

Before submitting a CRF, Change Initiator shall discuss internally within his or her Department or Unit to obtain a common consent about the proposed changes, and obtain the appropriate authorities from his or her supervisor.

Depending on the size and nature of change, CRF may accompany with different supporting documents, e.g. change proposal, project initiation document and etc.

All CRF should have a unique identifier and logged.

In CRF, Change Initiator should provide adequate information for Change Manager to filter and classify assess the impact and priority of the change request.

Change Initiator should provide required information as far as possible. On demand, Change Initiator might be requested by Change Developer, Change Manager and/or CAB to provide extra information to supplement to the CRF.

## 6.2 Change Request Filtering and Acceptance

Change Manager makes initial assessment to check if any of the information provided by the Change Initiator is unclear, illogical, impractical or unnecessary. If yes, reject such request with reasons, and ask the Change Initiator to modify and resubmit the CRF again.

## 6.3 Change Classification

Once a change request has been accepted, Change Manager review and if necessary, adjust its urgency and impact accordingly. Each service may decide their change classification scheme, with reference to the scheme below:

| **Urgency** | **Description** |
|---|---|
| Low | Change leads to minor improvement to current services / systems / networks that is not contractually necessary. |
| Medium | Change will solve irritating errors or missing functionality on the current services / systems / networks, and can be scheduled. |
| High | Change needed as soon as possible (potentially damaging current services / systems / networks). |
| Emergent | Change needed now (otherwise severe business impact to current services / systems / networks. |

| **Impact** | **Description** |
|---|---|
| Minimal | Expects no impact to current services / systems / networks expected 0 downtime interruption; OR expects no impact to the active users against respective service's user base during the change implementation. |
| Minor | Impact on current services / systems / networks expected <= 15 minutes interruption; OR estimated below 10% active users of respective service's user base will be affected during the change implementation. |
| Major | Impact on current services / systems / networks expected <= 30 minutes interruption; OR estimated below 20% active users of respective service's user base will be affected during the change implementation.<br><br>This includes batch updates and/or version upgrade |
| Critical | Impact on current services / systems / networks expected > 30 minutes interruption; OR estimated more than 20% active users of respective service's user base will be affected during the change implementation.<br><br>This includes removal of a service, or transfers of a service the user or a different party. |

Based on the Urgency and Impact levels, Change Manager assigns a priority to the change request according to the following priority matrix:

| | | Impact | | | |
|---|---|---|---|---|---|
| | | Minimal | Minor | Major | Critical |
| Urgency | Low | Low (1) | Low (1) | Medium (2) | Medium (2) |
| | Medium | Low (1) | Medium (1) | Medium (2) | High (2) |
| | High | Medium (1) | Medium (1) | High (2) | High (2) |
| | Emergent | High (3) | High (3) | High (3) | High (3) |

Changes shall be handled following the assigned priority. The CAB and the Change Manager shall assign appropriate resources to each priority level to avoid resource starvation.

For those changes with "Major" or "Critical" impact, Change Manager should request the Change Initiator to prepare a change proposal, containing a full description of the change together with a business and financial justification for the proposed change.

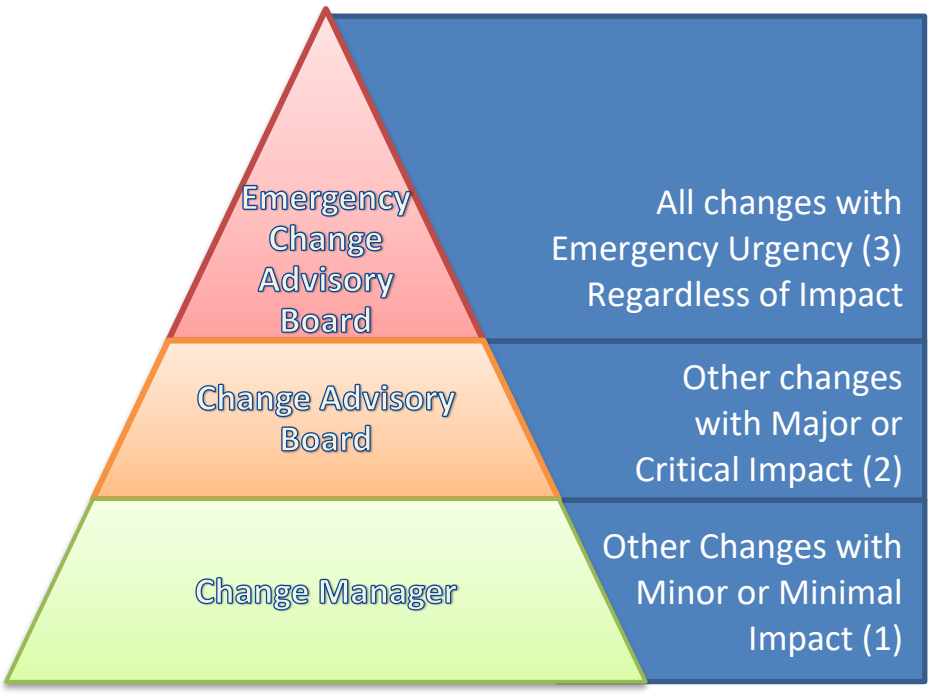
The change proposal must include signoff by appropriate levels of business management.

## 6.4 Change Approval and Planning

Only Emergency Change Advisory Board (ECAB) can approve "Emergency" Urgency, i.e. Changes shaded by red and marked as (3) in the priority matrix.

For those changes with Major or Critical impact, Change Manager shall arrange CAB meeting to evaluate and approve them, i.e. Changes shaded by orange and marked as (2) in the priority matrix.

Change Manager can approve those changes with Minimal or Minor impact, i.e. Changes shaded by green and marked as (2) in the priority matrix.




The following aspects should be considered when approving changes:

- cost, benefit and budget
- risk, impact, necessity and feasibility
- capacity and performance of the affect services;
- reliability and revocability
- availability and IT service continuity plan
- required cycle time of the change
- any conflicts with other changes

Change Manager shall prepare a plan for the approved changes, and distribute it to all the relevant parties.

## 6.5 Change Development

Suitable Change Developer should be appointed in accordance with the requirements in terms of technology, scale, priority and type.

Change Manager and Change Developer shall liaise with Change Initiator and any stakeholders to ensure that the changes are developed in accordance with the user requirements and comply with the University's Information Security Policies and Standards. For example, the following security attributes should be considered:

- Access control and password ("Logical Access Control Security Standard")
- Protection of sensitive information ("Information Classification and Handling Standard")
- Restriction of physical access to components related to the changes ("Physical Access Security Standard")

### 6.5.1 Test

Change Tester, Change Developer, Change Manager and Change Initiator shall conduct sufficient tests in testing environment to verify that the developed changes are capable of realizing the user requirements and not posing negative impact on security of the University's IT environment.

Depending on the type and scale of change, the following tests should be performed:

- Unit Test verifies the functionality of changed section within an IT component of the University. Where applicable, Unit Test must be performed by the Change Developer or designated Change Tester of the IT unit.
- System Integration that verifies the interaction of the changed IT component with external systems or parties. Where applicable, System Integration Test must be performed by the Change Manager and Change Developer or designated Change Tester of the IT unit.
- Vulnerability Test / Scan verifies the information security of the changed IT components and detects any existing vulnerabilities, which may be exploited by known threats. Where applicable, Vulnerability Test / Scan must be performed by the Change Developer or designated Change Tester of the IT unit.
- User Acceptance Test verifies the overall functionality of the changed IT component during the simulation of real-world scenarios. Where applicable, User Acceptance Test must be performed by the Change Initiator or designated Change Tester of user department.
- Regression Test uncovers new defects introduced by the changes, and Stress Test that verifies the performance of system is not affected. Where applicable, Regression Test should be performed by Change Developer or Change Tester of user department, and Stress Test should be performed by Change Developer.

Upon completion of the testing, if no issue is noted around the change, the Change Developer, Change Initiator and the Change Manager, who approved the change, must sign on the test results as evidence of their acceptance.

The University shall retain the test plans and results for at least 12 months to allow further reference or facilitate investigation on problems occurred after the changes.

### 6.5.2 Test Data

Test data should be protected and controlled. Production data, sensitive information including personal information must not be used as test data, unless specific approval is obtained from the Data Owner in written and necessary sanitization is performed based on Data Owner's requirements before testing.

The following controls should be applied to protect production data or sensitive information, if they are used for testing purposes:

- Implement control procedures to ensure only the Change Developer, the Change Initiator or other designated Change Testers have access rights to the test data;
- Separate authorization from the Data Owner must be obtained in writing each time the production data or sensitive information is copied to the testing environment; and
- Production data or sensitive information must be erased from the testing environment immediately after use.

### 6.5.3 Release Package

Upon the approval of the change implementation and test result, the change implementation team should build a release package, or provide the installation kit for the IT Support team for building the package.

The release package should contain all required items to update the current situation to the desired situation of the change. Example items in a release package are:

- Hardware, software, instruction and their corresponding configuration
- Training material
- Updated System Administration Manual and Operation Manual, if revision is necessary
- Signed acceptance of test results
- Documentation including deployment instructions, known errors, and etc.
- Deployment plan, including schedule
- Success and failure criteria

For service with segregated facilities for development, test and production, release package should be built using development environment, verified in test environment and prompted to production environment.

## 6.6 Change Execution

Upon approval, Change Manager assigns the change request to a suitable Change Deployer.

The Change Deployer must verify the acceptance record of test results in release package, in order to ensure that the changes have been tested and the acceptance from IT and user department are obtained and documented in testing environments.

For “Major” and “Critical” changes authorizations from the CAB, or for “Emergency” change authorizations from ECAB must also be obtained prior to production release.

Subject to the arrangement of System Owner, release package could contain deployable change prepared by Change Developer, or source to be built. In the latter case, the Change Deployer is responsible for building and testing the changes.

The Change Deployer is also responsible for implementing the changes. Change Developer and Change Tester are responsible for providing assistances during the building, testing and implementing of changes.

When applicable, multiple release packages should be grouped into one release.

The System Owner should automate the build, installation, and release distribution process to aid repeatability and efficiency if possible.

Unless authorized by Service Owner, all change releases must be performed by Change Deployer. Change Developer could provide on-site deployment support.

If the release could cause service outage during agreed service hours, scheduling and service interruption information should be made available in prior to affected stakeholders and end users.

The Change Deployer is also responsible for preparing the fallback procedures by backing up necessary application and data, and shall execute these procedures if necessary. Fallback procedures should be tested, if situation allows.

## 6.7 Post Execution Review

Within a reasonable timeframe after the Change Deployer has completed the change requests, Change Manager shall verify and evaluate the implemented changes to see if follow-up actions are needed.

It is recommended that change evaluation should be conducted within 1 week after implementation, while System Owner, Change Initiator and Change Managers should agree a time appropriate for their services.

If the change is successful, Change Manager closes the change request and notifies relevant parties for their closing of the incident and problem records, if applicable.

If the change is not successful, Change Manager determines the root cause of failure and requests change Initiator to create a new CRF to restart the process.

## 6.8 Tracking Reporting and Management Review

On a monthly basis, Change Manager prepares a Change Management Report, which may contain the following information:

- Number of changes implemented during the period;
- List of causes of changes and change requests
- Number of successful and failed changes during the period;
- Number of incidents related to implemented change

- Graphs and trend analysis for relevant periods
- Total costs and man-hours spent on changes

Change Manager reviews the Change Management Report to detect increasing levels and natures of change, frequent recurring types, emerging trends and other relevant information. Any actions derived from the review shall be implemented; effectiveness shall be verified and associated records shall be maintained.

## 6.9 Emergency Change

Emergency changes must be properly documented and obtain approval as per following procedure:

- Change Initiator must clearly justify the emergency nature of the change and provide all related information in the CRF.
- Change Manager must obtain approval from ECAB before taking any actions
- Change Deployer / Change Developer must thoroughly and accurately document all emergency changes. Any documentation not updated during the emergency change process must be completed prior to closing the change record.
- Change manager is responsible to verify the emergency change has properly implemented and all require documents have properly recorded.