Carleton UNIVERSITY
Canada's Capital University

Policy Name:	ITS Change Management
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Chief Information Officer (CIO)
Date of Original Policy:	April 2009
Last Updated:	November 2015
Mandatory Revision Date:	November 2016
Contact:	Manager, Client Services, ITS

Policy:
ITS will perform changes to ITS-managed IT (Information Technology) systems in a manner that will ensure the effective management of change while reducing the inherent risk associated with changes to IT systems. The Change Advisory Board (CAB) is the change management decision-making authority for ITS; however, not all changes need to be approved by the CAB.

Purpose:
This Policy describes a framework to be used for controlling software, hardware, and configuration changes made to ITS-managed IT systems.

Scope:
This Policy applies to all IT systems managed by ITS.

Procedures:

1.0 Changes that Require CAB Approval

The CAB operates under the auspices of the Chief Information Officer (CIO), and serves as the governing body for all changes covered by the scope of this Policy. The CAB is accountable for all changes to systems managed by ITS. Changes must follow the RFC (Request for Change) guidelines and be approved by the CAB.

IT changes that require CAB approval include the following:

- Installation of software updates and security patches on IT equipment
- Replacement, upgrade or maintenance of IT equipment
- Upgrade on applications
- Deployment of new systems, applications and infrastructures

1.1 Change Initiation

Initial authorization of a change is required by the functional owner for the validity of the change request. Functional owners may delegate the approval authority to the IT specialist for the affected system(s).

1.2 CAB Review of Changes

Per the RFC Guidelines, a formal RFC form must be completed and submitted to the CAB by the Change Initiator, prior to the approval of the change. The RFC, once approved, will serve as the official record of the change.

1.3 Testing of Changes

A testing plan must be executed as deemed necessary by the CAB. The complexity of the testing process will vary with the nature of the change. The testing process may consist of system testing, unit testing, quality assurance testing, regression testing, or user testing.

Formal testing plans, including back-out plans, must accompany RFCs when it is deemed necessary by the CAB. Where possible, testing should be done in a separate testing environment and promoted to the production environment once testing has been completed.

Verification testing of system changes will be performed as deemed necessary by the CAB.

1.4 Monitoring of Change

In order to determine whether the deployed change has been effective, changes must be monitored by the Change Implementer.

The degree of monitoring required will vary based on the nature of the change. The degree of monitoring will be determined in consultation with the CAB.

1.5 Change Tracking

The approval of planned changes will be recorded, and the status of the change will be updated after the change has occurred.

1.6 Communication of Changes

The ITS Service Desk serves as the primary conduit for communicating change activities to members of the campus community. For each change, the CAB will determine the necessary client groups to distribute targeted communications.

2.0 Changes Made to PCI Environment

For systems in-scope of the Payment Card Industry Data Security Standard (PCI DSS), there must be documented processes for the testing and approval of all:

- Network connections
- Changes to firewall and router configurations

For any changes made to the PCI environment, including software modifications, implementation of security patches, and changes to network connections and firewall/router configurations, procedures must be in place to verify that:

- The impact of the change is documented
- Functionality testing is performed to verify that the change does not adversely impact security
- Back-out procedures must be documented

3.0 Consideration of Other Institutional Policies

The ITS Change Management Process takes into account other institutional policies which govern IT operations. In circumstances where another policy conflicts with the Change Management process, the CAB must be consulted.

Roles and Responsibilities:
The following key roles are associated with the ITS Change Management process:

Change Manager
Appointed by the CIO, is responsible for managing the activities for the overall Change Management process, and serves as the Chair of the CAB.

Change Initiator
Typically someone in a business unit or the ITS Manager responsible for the affected system(s) who champions the request for the change and submits the RFC to the CAB and documents the changes in-scope of PCI DSS.

Change Implementer:
Responsible for executing hands-on tasks related to the change, and for documenting changes in-scope of PCI DSS

Compliance:
Non-compliance to this Policy may result in disciplinary action.

Contacts:
Manager, Client Services, ITS

Links to Related Policies:
N/A