MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

IT Change Management Framework

Standard

Effective Date: September 24, 2015

Authority & Alignment

Authority: D1200 Code of Conduct, D3300 Internal Controls, D8030 Technology Management
Alignment: Infrastructure Technology Infrastructure Library (ITIL) v3

Overview

Changes occur in response to identified resolution to problems, project requirements or deliverables, and academic and administrative requirements such as reducing costs or improving services.

Change in any form carries risk - risk of failure, disruption of operations, technical challenges, resource constraints, and unanticipated consequences.

The goal of the change management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents on service quality, and consequently to improve the day-to-day operations of MacEwan University (the "University").

To make an appropriate response to a change request entails a considered approach to the assessment of risk and business continuity, impact of the change, resource requirements, scheduling, and change approval. This considered approach is essential to maintain a proper balance between the need for change and the impact of the change.

Scope and Definitions

This standard will apply to changes to all IT production environments. A Change Advisory Board, guided by a Change Manager, will determine the scope of change characteristics, by platform, subject to the change management procedure(s).

Compliance & Exceptions

Responsibility for compliance with University policies and standards extends to all members of the University community. Non-compliance may create risk for the University and will be addressed accordingly (see clause 4.5.1 "Respect for the law and University governance" of the University's policy D1200 Code of Conduct – Employees for additional guidance).

Standard Requirements

1. The Director of the IT Compliance and Information Security Office is responsible for the requirements of this standard and is accountable to the CIO for the ongoing effectiveness of all controls established to fulfill the requirements.
2. The change management procedure(s) will be documented. Each production change must go through the change management process. All changes will progress through each phase of the procedure at different rates depending on the magnitude, complexity, and the impact to the stakeholders.
3. The Change Manager is appointed by the Director of the IT Compliance and Information Security Office.

4. The Change Advisory Board is appointed by the Director of the IT Compliance and Information Security Office and convened on a regular basis to execute the change management procedure.
5. An Emergency Change Advisory Board is established by the Director of the IT Compliance and Information Security Office to respond to emergency change requests.
6. All changes will be categorized according to their impact. Determining the category of a change will involve an analysis of the degree of risk and the impact according to established criteria.
7. Every change will be assigned a priority based on:
    a. The impact of the problem; and
    b. The urgency for the remedy.
8. Change requests will be tracked according to an established set of statuses.
9. The Change Manager and the Change Advisory Board will establish the requirements for change request test plans.
10. System owners or their delegates will be consulted on change requests that affect their systems, applications, and services.
11. Adequate notification will be provided to stakeholders of approved outages to systems, applications, and services.
12. Every change will be assigned a change window.
13. The Change Manager will establish the requirements for change request approvals.
14. The change management procedure(s) will have adequate segregation of duties to ensure the separation of the requester, approver, and implementer roles.
15. A post implementation review will be conducted on all changes that were not implemented according to plan.

Related Content

Type	***Title***
Policy	D8030 Technology Management Policy
Procedure	Infrastructure Change Management
Procedure	Business Application Change Management

Measurement

- ✓ Number of production failures resulting from the implementation of approved changes.
- ✓ Number of changes that needed to be reversed.
- ✓ Number of non-compliant events.
- ✓ Number of unauthorized changes.

Contact

Director, IT Compliance and Information Security Office