# IT Change Management Policy

**Authority Source:** Chief Digital Officer

**Approval Date:** 26/07/2024

**Publication Date:** 01/08/2024

**Review Date:** 31/07/2026

**Effective Date:** 01/08/2024

**Custodian:** Chief Information Officer

**Contact:** cio@canberra.edu.au

**Accessibility:** Public

**Status:** Published

In developing this policy the University had regard to the provisions of section 40B(1)(b) of the Human Rights Act 2004 (ACT).

## 1. PURPOSE:

1.1. The purpose of this policy is to communicate the University's requirement that all changes to IT information, applications, infrastructure, architecture, systems, and services must be managed efficiently and effectively, using standardised methods and procedures to mitigate the risk and impact of changes to the University.

1.2. **Goals of Change Management process**:

1.2.1. Ensure that standardised methods and procedures are used for the timely and effective implementation of required changes, in order to appropriately manage risk and minimise negative impact of change to service quality, and business operations. The Change Management process is especially important in ensuring only authorised change is made to production environments.

1.2.2. Respond to the University's changing business requirements while maximising value.

1.2.3. Ensure that IT changes continue to align with the University's business needs.

## 2. SCOPE:

2.1. This policy covers the Release of any new functionality or Change to the University's IT architecture.

2.2. The University's IT architecture includes, but is not limited to, hardware, software, operating systems, data and voice network and applications.

## 3. PRINCIPLE:

3.1. IT Service and infrastructure Changes shall have clearly defined and documented scope.

3.2. All requests for a Change shall be recorded and classified, e.g. standard, normal, enhancements and emergency/fast track standard. Requests for Changes shall be assessed for their risk, impact, and

business benefit.

3.3. Change Management shall include the manner in which the Change shall be reversed or remedied if unsuccessful.

3.4. Submitted Changes shall be vetted and, where approved, shall be implemented in a controlled manner.

3.5. Details of Changes will be communicated to all stakeholders on a regular basis.

3.6. There shall be a procedure to handle the authorisation and implementation of Emergency Changes.

3.7. The scheduled implementation dates of Changes shall be used as the basis for Change and Release scheduling. A schedule that contains details of all the Changes approved for implementation and their proposed implementation dates shall be maintained and communicated to relevant parties.

3.8. There shall be clear accountabilities for the authorisation and implementation of all Changes.

3.9. There shall be an appropriate administrative separation of authorisation and implementation roles for each Change, reflecting the risk associated with the Change.

3.10. Change Advisory Board (CAB) meetings shall be held regularly with attendees from DITM and relevant business units.

## 4. RESPONSIBILITIES:

4.1. The University specifies detailed roles and responsibilities in relation to Change Management.

4.2. Suppliers of goods and services pertaining to the University's IT Architecture bear the responsibility of following the prescribed DITM change management process and procedures.

4.3. Suppliers of externally hosted services are responsible and accountable for informing the University of its role and responsibilities in the supplier's change management process.

4.4. Where an externally hosted service is hybrid (e.g.: also contains service components owned/managed by the University) the supplier's and the University's IT change management processes will work collaboratively during change or service transition activities.

4.5. Staff, end-users and stakeholders of the University's IT environment share responsibility for Change Management:

4.5.1. ***End-User/Functional User*** – has responsibility for submitting a change request, including appropriate authorisation and participation in the testing.

4.5.2. ***Business System Owner*** – has the responsibility for ensuring that the change process is followed for all business systems.

4.5.3. ***DITM Staff Technical Role*** – has responsibility for following the prescribed change management processes and procedures.

4.5.4. ***Change Advisory Board (CAB)*** – has responsibility for advising the Change Manager in the assessment, prioritisation and scheduling of changes.

4.5.5. ***Change Manager*** – has responsibility for approving changes to the IT architecture.

4.5.6. ***Emergency CAB*** – has responsibility for reviewing/approving high urgency, high impact emergency changes (required in less than 24 hours).

4.5.7. ***DITM Management*** – has overall governance responsibility for overseeing the change management policy and processes. This includes, but is not limited to, policy dissemination, process enforcement, grievance and final approval for those changes requiring escalation by the CAB.

4.6. **Evaluation**: The Change Management process will be reviewed as required by the CIO for compliance with the policy.

## 5. LEGISLATION:

5.1. This policy is governed by the following legislation:

5.1.1. Territory Records Act 2002

5.1.2. Freedom of Information Act 1982

5.1.3. Privacy Act 1988

5.1.4. Evidence Act 1995

5.1.5. Electronic Transaction Act 1999

5.1.6. Crimes Act 1914

5.1.7. Telecommunications (Interception and Access) Act 1979

5.1.8. University of Canberra Act 1989

## 6. SUPPORTING INFORMATION:

6.1. **Context**

This policy fits within the University's IT Infrastructure Library (ITIL) service management framework (Service Transition)

6.1. **Other Related Documents**

DITM and Records Management Policy Manual

## 7. DEFINITIONS:

| Terms | Definitions |
|---|---|
| Change | A Change is defined as any addition, deletion and/or modification to an IT resource and may be characterised as permanent, transitory, or remedial. |
| Change Advisory Board (CAB) | A dynamically formed group of functional experts, who assist in assessing, prioritising and scheduling changes. |
| Change Management | The process responsible for controlling the lifecycle of all changes. The primary objective of change management is to enable beneficial changes to be made with minimum disruption to IT Services (ITIL) and end users. |
| Change Manager | Authorises and documents changes to the IT infrastructure and components to minimise disruption on operational services. |
| Corporate IT Application | All applications that support the business of the University. |

| | |
|---|---|
| Emergency Change | Any change to the University's IT Environment, that is not pre-approved, and is required within 24 hours. |
| Emergency Change Advisory Board (ECAB) | A smaller subset of CAB (including a director or delegate) responsible for reviewing/approving high urgency, high impact emergency changes. |
| ITIL | Information Technology Infrastructure Library: A best practice framework for the delivery of managed IT services. |
| Non-Standard Change | Any new capability or, any change that is not pre-approved, to the University's IT Environment. |
| Release | ITIL definition: A collection of hardware, software, documentation, processes or other components required to implement one or more approved Changes to IT Services. |
| Standard Change | A pre-approved change listed on the Standard Change Catalogue. |
| Suppliers | Third parties responsible for the supply of services and/or goods for the delivery of IT services. |