Information Technology Services
Change Management Policy

Category	Information Technology
Type	IT Policy
Approved by	Director Information Technology Services
Date Policy Took Effect	1 November 2023
Last Approved Revision	1 November 2023
Sponsor	Director, Information Technology Services
Review Date	2 November 2025

Purpose

Occasionally systems require outages for planned upgrades, maintenance, or fine-tuning. Managing these changes is a critical a part of providing a stable infrastructure. Effective management and communication of updates, maintenance, and regular releases help to minimise customer impacts.

The purpose of this policy is to ensure changes are made in a well-communicated, planned, and predictable manner that minimises unplanned outages and unforeseen system issues. Effective change management requires planning, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the University community.

Organisational Scope

This policy applies to all staff and contractors involved in IT application or system changes, updates, or patches both operational and project based.

Policy Content

A. GENERAL

1. All system and application additions and changes in Information Technology Services (e.g., operating system, computing hardware, networks, applications, data centres) are subject to this policy and shall follow change management, architecture and Cyber Security procedures.

2. The following general requirements shall be met in the change management procedure:
    (a) Stakeholders shall be informed of upcoming application and system changes that impact system availability or operations.
    (b) Unplanned outages/emergency changes shall be communicated immediately to stakeholders with regular updates on progress towards resolution and resumption of service.
    (c) Regular system and application patching schedules shall be communicated to users and performed in such a way as to minimise system downtime and impact on user productivity.
    (d) Changes affecting environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity) shall be reported to and coordinated with the Property and Campus Development Division and stakeholders shall be notified through standard change management communications channels.
    (e) Device configurations shall be backed up and rollback procedures must exist prior to implementing a change.

3. When there is a material change to either the Architecture or Cyber Security posture because of the change, the following general requirements shall be met, or an exemption approved by the Enterprise Architect or Senior Manager Cyber Security and Assurance:
    - Solution Architecture artifacts are updated to reflect the change. If none exist, relevant artifacts should be created.
    - Cyber Security artifacts are updated to reflect the change. If none exist, relevant artifacts should be created.
    - Relevant Disaster Recovery and Business Continuity Plans are updated to reflect the change.

B. IT CHANGE APPROVAL BOARD

1. The IT Change Approval Board (ITCAB) shall provide oversight of Information Technology changes within the organisation, assess their impact, and provide guidance and recommendations around how information technology changes are implemented within the University of Otago.

2. The IT Change Approval Board provides governance of Information Technology changes and ensures that they are well planned and communicated across the University. Members of the IT Change Approval Board undertake to be responsible for Information Technology changes within the University of Otago.

3. Membership
    - Information Technology Services Senior Leadership Team.
    - AskOtago (Senior Manager / delegated representatives).

C. CHANGE REQUEST MANAGEMENT

- Change requests shall be submitted for all changes, both scheduled and unscheduled as per the IT Change Control Process in Confluence.

D. CHANGE REJECTION

- The IT Change Approval Board or their designee may delay or reject a scheduled or unscheduled change for reasons including, but not limited to:

    - Inadequate change planning or unit testing
    - Lack of stakeholder acceptance and notification (where applicable)
    - System concerns
    - Missing or deficient roll-back plans
    - Security implications and risks
    - Timing of the change negatively impacting key business processes
    - Timeframes do not align with resource scheduling (e.g., late-night, weekends, holidays, or during special events such as graduations or examination periods).

E. ADMINISTRATION

- A Change Management log shall be maintained for all changes. This log must contain, but is not limited to:

    - Date of submission and date of change.
    - Owner and Technical contact.
    - Nature of the change.
    - Indications of success or failure.
    - Notes and follow-ons.

- The change log is located here: ITS Change control.

F. Audit Controls and Management

- Documented procedures and evidence of practice should be in place for this policy. Satisfactory examples of evidence and compliance include:

    - Historical logs of change events.
    - IT Change Approval Board monthly review meeting minutes.
    - Documentation and communications showing regular compliance with the policy.

Enforcement

Staff members found in breach of this policy may be subject to disciplinary action.

Related Procedures, Processes and Forms

- IT Change Control Process
- IT Change Approval Board
- ITS Standard Change Register
- ITS Change Control Log
- ITS Change Control CAB Dashboard

Contact for further information about this Policy

If you have any queries regarding the content of this policy or need further clarification, contact the ITS Divisional Office on ITS.Director@otago.ac.nz