Digital Services Change Management Policy

Category	Information Technology
Type	IT Policy
Approved by	Chief Digital Officer (CDO) Digital Services
Date Policy Took Effect	1 November 2023
Last Approved Revision	28 August 2026
Sponsor	Chief Digital Officer (CDO), Digital Services
Person Responsible:	Head of Information Systems, Digital Services
Review Date	28 August 2028

Purpose

Occasionally digital infrastructure and systems require outages for planned upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a stable digital environment. Effective management and communication of updates, maintenance, and regular releases help to minimise impact on the University community.

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

Organisational Scope

This policy applies to all Digital Services staff and contractors involved in digital infrastructure, application or system changes, updates, or patches; both operational and project based.

Policy Content

A. General

1. All digital infrastructure, system and application additions and changes in digital services (e.g., operating systems, computing hardware, networks, applications, data centres) are subject to this policy and shall follow change management, architecture and cyber security policy, procedures, processes, standards and guidelines.
2. Change requests (scheduled and unscheduled) shall be submitted for all changes as per the IT Change Control Process in Confluence.

3. The following general requirements shall be met:
   (a) Stakeholders shall be informed of upcoming digital infrastructure, application and system changes that impact 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 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 communication channels.
   (e) Device configurations shall be backed up, and roll-back procedures must exist prior to implementing a change.

4. When there is a material change (i.e. change that may alter or create meaningful risk such as changes to underlying architecture and/or cyber security posture), the following general requirements shall be met, or an exemption approved by Enterprise Architecture or Cyber Security and Identity (respective to their responsibilities). The:
   (a) Digital Systems List record is updated to reflect the change.
   (b) solution architecture artifacts are updated to reflect the change. If none exist, relevant artifacts should be created with the support of Enterprise Architecture (via arb@otago.ac.nz).
   (c) cyber security review and control documentation is updated to reflect the change. If none exist, relevant artifacts should be created with the support of Cyber Security and Identity (via cybersecurity@oago.ac.nz).
   (d) relevant Disaster Recovery and Business Continuity Plans are updated to reflect the change.

   Where it is unclear whether architecture review, cyber security review, or another governance pathway is required, the change owner should seek advice from the Enterprise Architecture team to help determine the appropriate review pathway(s).

B. Change Approval Board

1. The Change Approval Board (CAB) shall provide oversight of changes initiated by Digital Services within the University of Otago, assess their impact, and provide guidance and recommendations around how such changes are implemented within the University.

2. The Change Approval Board provides governance of digital service changes and ensures that they are well planned and communicated across the University.

3. Members of the Change Approval Board undertake to be responsible for digital service changes within the University of Otago.

4. Membership:
   - Digital Services Leadership Team (or delegated representatives)
   - AskOtago (Senior Manager or delegated representative)

C. Change Rejection

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

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

D. Administration

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

    a) Date of submission and date of change
    b) Owner and Technical contact
    c) Nature of the change
    d) Indications of success or failure
    e) Notes and follow-ons

E. Audit Controls and Management

1. Documented procedures and evidence of practice will be used to audit the compliance with this policy. Satisfactory examples include:

    a) Historical logs of change events
    b) Digital Services monthly review meeting minutes
    c) Documentation and communications showing regular compliance with the policy

Enforcement

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

Related Information

- 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 Digital Services Divisional Office via cdo@otago.ac.nz