Technology Services Change Management Policy

TU Dublin Policy for Change Management in Technology Services

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

TU DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance
Owner	Chief Information Officer
UET Sponsor	*Dr Dympna O'Sullivan, Vice President, Research & Innovation*
Reference number	TSCMP2025
Version	1.0
Status	Approved
Pre-approval Body/Bodies	UET, ARC
Approved by	Governing Body
Approval date	18th February 2026
Next review date	18th February 2029
Document Classification	TU Dublin Public

2. Introduction

IT Change Management is a critical process within Technology University Dublin (hereafter referred to as "TU Dublin" or "the University") which ensures the stability and reliability of its IT infrastructure. It helps minimize disruptions to academic and administrative activities by systematically managing changes to IT systems, applications, and services.

The policy mitigates risks, ensures compliance with regulatory standards, and aligns IT changes with the university's strategic goals. By maintaining detailed documentation and oversight, the policy enhances accountability and transparency, fostering a secure and efficient technological environment that supports the university's mission of education and research.

3. Purpose

This document outlines the policy regarding the control and communication of changes made by Technology Services (hereafter referred to as "TS") to supported IT systems, platforms and applications within TU Dublin.

The control of such changes provides TU Dublin with a mechanism to evaluate the risk of a proposed change or the risk of a proposed change not proceeding as planned and the impact that this may cause on services provided by the university. This policy also outlines the decision points and procedures should a change need to be reversed or rolled back. Another component of the change management process is the communication plan which defines who needs to be informed in advance of the change and who must be notified should the change not proceed as expected.

This process is not intended for business-as-usual, day-to-day changes, which arise out of normal system, platform or application administration and which are not expected to be service affecting. Typically, changes are requested as enhancements to a system, to resolve an issue or problem, to facilitate the release of a new update or feature, or for scheduled or unscheduled maintenance and have the potential to affect or disrupt the IT service.

This **Technology Services Change Management Policy** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- **Govern (GV)**
  - Roles, Responsibilities and Authorities
    - GV.RR-01

    - Policy
        - GV.PO-01
        - GV.PO-02
    - Oversight
        - GV.OV-01
        - GV.OV-02

- **Identify (ID)**
    - Risk Assessment (ID.RA)
        - ID.RA-06
        - ID.RA-07

4. Scope

The Technology Services Change Management policy governs all changes to TU Dublin IT infrastructure, resources, applications and services managed by the Technology Services department that is required for the successful operation of university business. Changes that may potentially have a negative or disruptive effect to university activities or services should be formally reviewed by a Change Advisory Board (CAB) as part of the TS Change Management process in line with this policy.

The Change Advisory Board shall review all proposed changes that may impact the IT environment, including but not limited to:

- Hardware and software upgrades
- System configurations
- Network changes
- Application deployments
- Security updates
- Process improvements
- Any other modifications affecting IT Services

4.1 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

Governing Body:

- To review and approve the policy on a periodic basis.

TU Dublin Executive and Management Teams:

- To review and approve the policy on a periodic basis.

TU Dublin Vice President of Research and Innovation:

- To ensure the policy is reviewed and approved by the Executive and Management Teams.

TU Dublin Chief Information Officer:

- To review and approve the contents of the policy.

Technology Services Management:

- To define and implement standards and procedures which enforce the policy.
- To enforce compliance with this policy where technically possible on TU Dublin systems.

Change Advisory Board Manager:

- To develop and distribute the agenda for CAB meetings, ensuring all relevant changes are included for review.
- To chair CAB meetings, guiding discussions, and ensuring all members have the opportunity to contribute.
- To make final decisions on changes when consensus cannot be reached within the CAB.
- To ensure that all changes adhere to the organization's change management policies and procedures.
- To act as the primary point of contact between the CAB and other stakeholders, including senior management and TS teams.
- To monitor the performance and effectiveness of the CAB, implementing improvements as necessary.
- To ensure accurate documentation of CAB activities and decisions and provide regular reports to senior management.

Change Advisory Board (CAB):

- To evaluate the details and implications of proposed changes to IT systems and infrastructure.
- To identify and assess potential risks associated with each change, including security, operational, and compliance risks.
- To make informed decisions to approve, reject, or request modifications to proposed changes.
- To verify that proposed changes comply with organizational policies, standards, and regulatory requirements.
- To facilitate communication between stakeholders to ensure everyone is informed about upcoming changes and their impacts.
- To oversee the implementation of approved changes to ensure they are executed as planned and within the defined scope.
- To conduct reviews after changes are implemented to evaluate their success and identify any issues or areas for improvement.
- To ensure that all change-related documentation is accurate, up-to-date, and accessible for future reference.

Emergency Change Advisory Board (ECAB):

- To prioritize and expedite review of emergency change requests.
- To assess the severity and urgency of the emergency change requests.
- To determine the immediate actions required to address an emergency.
- To approve emergency changes based on their impact and risk.
- To coordinate with relevant stakeholders to implement emergency changes promptly.

Change Owner:

- To submit the change request, including all necessary details such as business justification, implementation plan, communications plan, change details, schedule and remediation plan.
- To organise and plan activities related to the change.
- To attend CAB meetings and provides necessary inputs if required.
- To present the change at CAB meetings and address any questions.
- To review and document the change plan.
- To resolve any issues related to the change.
- To update users with the change activity.
- To conduct testing activities before and after the implementation of the change.

If you have any queries on the contents of this policy, please contact the IT Service Desk.

5. Definitions

Change: Refers to any modification, addition, or removal of hardware, software, configurations, or other IT components that could impact the university's information systems or services. This includes updates, upgrades, patches, new installations, decommissioning of systems, and changes to processes or procedures. The goal of managing these changes is to ensure they are implemented in a controlled and systematic manner, minimizing risks and disruptions while maintaining the integrity, security, and availability of IT services.

Change Advisory Board (CAB): A group who run formal meetings to assess, prioritize, authorize, and schedule changes as part of the change control process. The CAB consists of a CAB Manager and CAB members who represent teams/departments that may be involved or impacted by IT changes.

Emergency Change Advisory Board (ECAB): A subset of the CAB that shall convene specifically to evaluate and approve emergency changes that require immediate attention to mitigate severe disruptions or security risks.

Change Advisory Board Manager: The CAB Manager acts as a chairperson and is responsible for overseeing the entire change management process. They must ensure that changes are properly assessed, authorized, and implemented according to policy and process.

Change Advisory Board Member: A nominated individual responsible for reviewing, assessing, and approving proposed changes to the university's IT systems and infrastructure. CAB members typically include representatives from various departments, such as IT, security, and operations, ensuring a comprehensive evaluation of the impact and risks associated with each change. Their role is to provide expert advice, ensure alignment with organizational goals and policies, and facilitate informed decision-making to maintain the integrity, security, and efficiency of the university's IT environment.

Change Owner: Is the individual responsible for requesting, initiating, planning, and executing the change, ensuring it is well-documented and implemented correctly. They are responsible for the change's execution and implementation.

Service Owner: Is the individual or team responsible for the overall management, administration and accountability of a specific IT service.

Change Request: A formal proposal/request by a TU Dublin staff member to modify an IT system or service.

Back-out Plan: The formal plan used to reverse a change made to a system or service if that change is found to be disruptive or failed to apply correctly.

Change Calendar: An approved calendar and schedule of planned changes and their potential impact on systems and services.

6. Policy Details:

6.1 Policy Overview

The TS Change Advisory Board (CAB) is a critical governance body established to oversee the change management process within Technology Services. Its primary role is to assess, evaluate, and approve proposed changes to the IT infrastructure, systems, applications, and services. The CAB ensures that changes are implemented in a controlled and systematic manner to minimize disruptions, mitigate risks, and ensure alignment with business objectives.

6.2 Policy Details

6.2.1 Change Advisory Board

The Change Advisory Board (CAB) consists of a panel of nominated Technology Services staff members who may approve or reject proposed change requests to the TU Dublin IT environment.

The Change Advisory Board shall be established and meet all of the following criteria:

- The board shall consist of a CAB Manager and CAB Members.
- The CAB Manager is responsible for creating and managing change control processes, creating the agenda for each meeting, leading discussions, and ensuring all applicable parties are involved in change discussions.
- CAB Members are representatives from different groups that may be involved or impacted by the changes. These members attend CAB meetings to discuss and approve changes under the guidance of the CAB Manager.
- The CAB shall meet at on a regular basis and each meeting shall be attended by the CAB Manager and CAB Members.
- The CAB shall review and then approve or deny each change on the agenda, documenting reasons for denying a change if applicable.
- The CAB must use knowledge, experience and background to assess change requests for risks and issues
- The CAB should fully understand the proposed change requests by asking questions of the Change or Service Owner.
- The CAB should ensure the proposed time does not conflict with business needs or other change requests.
- The CAB should ensure that technical and architectural standards are maintained.
- The CAB should make recommendations to reduce risk, increase likely success and reduce potential business impact
- The CAB should consider any documentation that may need to be updated as a result of the change requests.

6.2.2 Change Control

- All changes that are not identified as emergencies should be scheduled.
- High and medium impact/risk changes should be completed in an agreed change window.
- Each change request must identify any risks associated with the change.
- Each change must define what the impact to the university will be if the change does not go to plan.

6.2.3 Change Types

Change management must balance the need to make beneficial changes that deliver additional value to the university with the need to protect users from adverse effects of the change. For changes to be effective and efficient, it is essential that the correct change authority is assigned to each change correctly.

In order to determine the change type, all changes should be classified as **Standard, Normal, Major** or **Emergency**. The following criteria should be used to determine change type:

- **Urgency**
  - How quickly does the change need to be implemented?
- **Risk**
  - What could happen if the change goes wrong?
- **Impact**
  - How impactful is the change? Is it for a single endpoint, or the entire network?

6.2.3.1 Standard Change

Routine changes that follow established procedures and require minimal assessment. These changes are low-risk and have minimal impact on operations. A standard change does not need CAB approval but must be logged in the change management system for audit purposes.

Examples: Software updates, patch installations, and minor configuration changes.

6.2.3.2 Normal Change

A change that requires assessment and approval through the standard change management process. Normal changes are planned and scheduled, involving moderate risk and impact. A normal change requires CAB approval.

Examples: System upgrades, new feature implementations.

6.2.3.3 Major Change

Significant alterations to systems, applications, or infrastructure that may have a substantial impact on operations. Major changes require extensive planning, testing, and approval from Senior Management and the Change Advisory Board (CAB).

Examples: Hardware upgrades, network reconfigurations, and large-scale software deployments.

6.2.3.4 Emergency Change

Urgent modifications required to address critical issues, mitigate security threats, or restore service availability. Emergency changes bypass the standard approval process and are expedited to address urgent situations and should be reviewed by ECAB. Emergency changes may be made immediately in exceptional circumstances but must be reviewed by ECAB retrospectively as soon as possible.

Examples: Security patches for critical vulnerabilities, emergency fixes for system failures, and immediate configuration changes to address security breaches.

6.2.4 Change Request

- Changes are submitted to a change management system using a change request template.

- Each change must have a detailed implementation plan.

- Each change request must describe a back-out plan.
- Service owners of services affected by the change must be identified and notified in advance of the change going ahead.
- Communications with the service owners should include details of the maintenance windows and the scope of expected outages. The service owner's approval of the change is a requirement for CAB Approval.
- Service users should be identified and notified if the proposed change will be overly disruptive to the normal business activities of the be service users.
- While it is important that changes are captured and controlled, not all changes need to go through the formal change management process. Standard Changes i.e. regular, operational tasks with minimal risk and impact need not go through the formal change management process.
- The CAB process is not intended for business-as-usual or day-to-day changes, which arise out of normal business administration and are not envisaged to be service affecting.

6.2.5 CAB Meetings

- The CAB shall convene at regular intervals as determined by the Chair or as required by the volume and urgency of change requests. ECAB or emergency CAB meetings may be called for time-sensitive or critical changes.
- Decisions of the CAB, ECAB shall be made by consensus whenever possible. In cases where consensus cannot be reached, the Chair shall facilitate a final decision based on a voting process. Each member shall have one vote. The Chair will have the deciding vote if a decision cannot be reached.
- The CAB must have a quorum in order to approve or reject proposed change requests.
- All change requests, evaluations, decisions, and actions taken by the CAB, and ECAB shall be documented thoroughly and maintained in a centralized repository.
- All changes approved by CAB should be scheduled and added to the CAB calendar, which helps Technology Services to plan changes, assist in communication, avoid conflicts, and assign resources.
- Completed changes should be reviewed by CAB for lessons learned and continuous improvement.

6.3 Monitoring

TU Dublin reserves the right to monitor all TU Dublin IT resources, information assets, content and data at all times.

TU Dublin reserves the right to log any required TU Dublin data, concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

TU Dublin may also log all changes made to TU Dublin systems and applications.

6.4 Violation of Policy

Contravention of TU Dublin policies may lead to the removal of access to TU Dublin services and resources and may lead to disciplinary action in accordance with the TU Dublin Staff Disciplinary Procedures or Student Disciplinary Procedures if applicable.

Users should report any suspected violations of this policy to the TU Dublin IT Service Desk. On receipt of any such notice, (or whereby the University otherwise becomes aware), of any suspected breaches of this procedure or its policies, the University reserves the right to suspend a user's access to the University's services and resources.

Where a valid business case exists exceptions to this policy may be approved by Technology Services in line with the IT Exception Policy.

6.5 Change Process

This policy will be reviewed every three years or after any change to TU Dublin applications, IT environment or business processes that would affect the application of this policy.

7. Related Documents

This policy should be read in conjunction with the following University policies and users should ensure compliance with all University policies in addition to this policy:

- TU Dublin Password Policy
- TU Dublin Data Protection Policy
- TU Dublin Acceptable Usage Policy
- TU Dublin Information Security Policy
- TU Dublin IT Exception Policy
- TU Dublin Data Classification Policy

The above list is not exhaustive and other TU Dublin documents may also be relevant.

For further information on IT related queries please contact the IT Service Desk.

8. Conclusions

Implementing a comprehensive Change Management Policy is essential for Technology Services to navigate the complexities of technological advancements while maintaining operational integrity and security. This policy ensures that all changes to IT systems are managed systematically, minimizing risks and disruptions.

By adhering to best practices, the university can safeguard its assets, comply with regulatory standards, and foster a resilient IT environment. Clear communication, stakeholder engagement, and robust documentation are integral to the success of this policy, enabling the university to adapt to operational changes efficiently and effectively and minimise the potential impacts to IT services.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
0.1	*Initial Draft*	*ISGRC*	*31/10/2024*
0.2	*Draft*	*ISGRC*	*08/04/2025*
0.3	*TSMT Review*	*ISGRC*	*08/05/2025*
0.4	*HEAnet Review*	*ISGRC*	*27/06/2025*
0.5	*Draft*	*ISGRC*	*01/07/2025*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
0.5	*25th November 2025*	*UET*
0.5	*3rd February 2026*	*Audit & Risk Committee*
1.0	*18th February 2026*	*Governing Body*

10.3 Document Ownership

Accountability for defining, developing, monitoring and updating the content of this document rests with the Office of the Vice President of Research and Innovation.

10.4 Document Review

The Chief Operations Officer is accountable for reviewing this document in consultation with relevant stakeholders. This document should be approved by the Vice President of Research and Innovation, the University Executive Team and Governing Body.

10.5 Document Storage

This document will be stored on the TU Dublin content management systems under the Policies and Forms media folder / Technology Services sub-folder. The file will be called: “TU-Dublin-TS-Change-Management-Policy-TSCMP2025_v1.0.pdf” once released.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to TU Dublin staff, students and third parties.