Change Management Policy

Version 1.2

Reviewed September 2024

Change Management:

Change Management is the process used to oversee the lifecycle of all changes. A change is defined as any addition, modification, or removal of configuration items that could impact IT services. This process is approved by management and aims to enhance business processes (fixes) while minimizing risks to IT services. Change Management applies to all architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items.

Type of Changes:

- *Standard Change:*

A standard Change is a pre-authorized, routine change that carries low risk, has predictable outcomes, and can be repeated using defined work instructions in a standard operating procedure (SOP). These SOPs are reviewed by the Service Owner, pre-approved by IT, and can be executed by Subject Matter Experts (SMEs) without needing further approval when a change request is made.

The crucial elements of a Standard Change are as follows:

  - The tasks are well-known, documented, and proven
  - Approval is not required by the CAB
  - The risk is usually low and always well-understood

- *Non-Standard Change:*

A Non-Standard Change is a type of change that does not include pre-authorized Standard Change or Emergency Change. These changes follow the full Change Management Process. Generally, some service requests, inputs from projects, release and deployment management, and resolutions for low to high priority incidents in incident and problem management are handled as Non-Standard Change.

  - Non-Standard Low Risk
  - Non- Standard Medium Risk
  - Non-Standard High Risk- Major

- *Emergency Change:*

An Emergency Change is a change that needs to be deployed immediately to resolve an outage, address a severe business impact, or mitigate significant security risks. These changes follow an abbreviated process and must include a Post post-implementation review with a Root Cause Analysis. All resolutions for major and critical incidents adhere to the Emergency Change process.

Scope:

- *In Scope:*
  - Production: All hardware, operating system, and software changes to the Data Center (including
  - Production: Software changes or OS Upgrade to 200> workstations.
  - Non-Production: All infrastructure, including hardware (excluding applications) in development, test, or pre-prod environment. This includes anything shared with other departments (There is no non-production network equipment so any network changes will be considered production).
  - Changes to Enterprise applications
  - Informational changes driven by vendors or third parties.
  - Break/Fix situations where we are restoring production systems and wide-scale issues back to normal state emergency changes.
- *Out of Scope*
  - Including, but not limited to, Service Requests for access requests, individual desktop/laptop/mobile device changes, etc.)
  - Lab equipment that does not impact anyone other than those supporting it.
  - Break/Fix situations where we are restoring back to a normal state for a single user. This is handled within Incident/Service Management process.

Lead Time:

Type of Change	Lead Time	Approval Process	Example
Standard Change	Same Day	• Pre-Approved change • Ticket Submission • Targeted communication is necessary/ through ticket or other methods.	• DHCP configuration • Building switchport configuration • DNS entries • Third Party SaaS upgrades • Server OS patching
Non-Standard– Low Risk	N/A	• Limited review is necessary by the ITS director and technical team and documented. • Change Management form Submission • Targeted communication is necessary. Determined by	• Datacenter switchport configuration • Addition of VLAN/subnet to building • Addition of new building or closet to network

		Director, BRM and Help Desk Manager	• Configure SaaS with one or two groups • Custom Code Installs that are isolated as one program/system that affect one user group. • Upgrade to software used by a department • Install/remove apps from 200> computers with low impact.
Non-Standard-Medium Risk	2 business days	• Review is necessary by the ITS director and evaluate if it needs to be reviewed by CAB. • Change Management form Submission • Targeted or full communication is necessary. Determined by Director, BRM, and Help Desk Manager	• Addition of VLAN/subnet to datacenter • Migration of building network uplink • Addition of VRF to backbone or metro • Configuration of SaaS with all university users impacted • Custom code installations that affect either a critical process such as payroll or registration, or impact multiple groups such as Admissions and Registrar. • Upgrades to systems used by a majority of users
Non-Standard–High Risk	6 business days	• Review is necessary by CAB • Change Management form Submission • Targeted or full communication is necessary. Determined by Director and BRM and CAB.	• Addition, modification, or removal of datacenter switch or uplink • Custom Code installations that have the potential to impact normal delivered processes.

			• Migration of a highly used on-premise system to the cloud • Upgrades to systems that are critical to university operations.
Emergency Change	N/A	• The director works with the change manager to form the CAB for the discussion. • Change Management form submission after completing the change. • Evaluate the communication list (See Appendix A) and run it by CAB. • Targeted or full communication is necessary.	• Code changes or insert, update, delete scripts provided by a vendor to resolve a production stop issue. • Zero day vulnerability patch deployment

Risk Table:

	Score		
Question	**1**	**2**	**4**
Number of Users Impacted	Single user, team or department	Multiple users, teams or departments	All users in the organization
Criticality of the service to the institution	If an outage occurs, core university functions can continue	If outage occurs, core university functions cannot be performed	Business critical, i.e. outage results in direct loss of revenue, reputation, direct exposure to fines, etc.
Number of teams involved with implementation	Activities are limited to a single IT team	Multiple teams within IT coordinate activities	Multiple teams in different departments must coordinate activities
Can it be tested? Can it be backed out?	Can be tested and backed out easily.	Either cannot be tested OR cannot be backed out easily	Cannot be tested or backed out easily.

Low Risk	*Less than 5*

Medium Risk	*5 to 10*
High Risk	*More than 10*

Change Management Request Form

CAB Meeting Agenda:

- Review the following changes from the previous week
  - Emergency changes
  - Failed changes / Action Review
  - Backed-out changes
  - Incidents resulting from implemented changes
- Review/assessment of proposed Requests for Non-Standard Changes /Major Changes
  - Risk and impact in terms of:
    - Service and Service Level impact
    - Capacity and performance
    - Downtime
    - Security and compliance
    - Financial
    - Resources involved

TDX Change Management Workflow (Does not include internal CAB processes)