IT Change Management Policy

Policy number: 800-IT-5
Policy owner: ITS

Date of initial publication: December 19, 2022
Date of latest revision: NA

SECTION I. PURPOSE

The purpose of this policy is to ensure that all changes to University IT Resources are tracked, to support continuity of IT services, and reduce negative impact on services and Users.

SECTION II. SCOPE AND APPLICABILITY

This policy applies to all St. Thomas employees (faculty, staff, and student workers), student clubs and organizations, contractors and volunteers

SECTION III. DEFINITIONS

When used in this policy, the following terms have the following meanings:

a. ***Category III – Orange Data*** means data that, if made available to unauthorized parties, may adversely affect individuals or the business of the University of St. Thomas. This classification also includes data that the University is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor.

b. ***Category IV – Red Data*** means data that includes any information that St. Thomas has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the University to notify the affected individual and state or federal authorities.

c. ***Change Advisory Board*** means the cross-functional ITS working group designated to continuously review and maintain the change management process, and review and approve proposed changes.

d. ***Change Control*** means a systematic approach to managing all changes made to University IT Resources. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

e. ***Emergency Change*** means a change that must be implemented as soon as possible, for example, to resolve a major incident or implement a critical security patch.

f. ***IT Resources*** means computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

g. ***ITSM*** means IT Service Management System. The system used by IT to track requests, incidents, inventory, and other work related to the management of IT services.

h. ***Normal/Standard Change*** means any service change that is not a Planned or Emergency Change. This includes changes with more than a low risk of service interruption, or which involve user experience changes.

i. ***Planned Change*** means pre-authorized changes that are low risk, relatively common, and follows a procedure or work instruction.

j. ***Routine Level Change*** means changes made to systems that are of a routine nature, are very low risk and generally involve using the system as designed, such as adding a new user, adding or updating a new record, changing user permissions.

k. ***SaaS (Software as a Service)*** means systems used by the university that are hosted and maintained entirely by a 3rd party vendor. Examples, Microsoft Office365, Canvas and Qualtrics.

l. ***Tier 0 and Tier 1 Systems*** means systems defined at the highest two priorities according to the ITS Disaster Recovery Plan, and require the most urgent level of recovery in the event of a major incident because of their critical nature to university operations.

SECTION IV. POLICY STATEMENT

A. Change Management Parameters and Requirements

1. All University IT Resources changes must be documented per the Change Control Process.

    a. Routine level changes will be handled in the ITSM ticketing process.

    b. Planned, Normal and Emergency level changes will use the ITS Change Management tracking system.

    c. Changes to SaaS solutions made by the vendor should be tracked in the Change Management System when significant and prior notice is provided.

2. All changes to University IT Resources must follow the Change Management process to ensure appropriate tracking, approval, planning, and execution.

3. Change requests may not be required for non-production (e.g., DEV, Test, QA) environments unless there is a significant upgrade or an impact, or the system contains Category III – Orange or Category IV – Red data.

4. Production change requests must note that the change has been successfully applied, tested, and verified in a non-production environment when an applicable environment(s) exist.

5. Changes to production environments undergo impact examination before the submission of the change request per the Change Management process. This information will be used to determine the impact of the change by considering:

    a. The impact the proposed change will have on business services, if it is expected to cause a widespread outage, a loss of connectivity or functionality to a specific group or groups;

    b. The risk involved in not making the change;

    c. The risk if the change does not go as planned; and

    d. Predictability of the success of the change.

6. Significant User experience changes must be conveyed to the Change Advisory Board (CAB) and communicated to the affected audience(s) via ITS communication processes.

7. The Change Advisory Board (CAB) must include all key functional areas, including but not limited to Information Security, Infrastructure, Networking and Support Services.

8. Any change item affecting Category III – Orange data, Category IV – Red data, or Tier 0 or 1 critical systems require additional lead time for review to ensure proper consideration.

9. A lessons learned session should occur in the event of an incident during a change request, or whenever an undocumented change leads to an incident.

B. Approval and Defrerrment of Change Items

Authorization of a change item occurs after the change is reviewed and depends on the priority of the item as described in the table below.

Type	Description	Approval Required	Notes
Routine Work	Changes made to systems that are of a routine nature, are very low risk and generally involve using the system as designed, such as adding a new user, adding or updating a new record, changing user permissions.	Predefined based on operating procedures	Tracked in ITSM. Examples: Permissions changes, user creation, adding a workstation to domain, activating a new network port.
Planned	Pre-authorized change that is low risk, relatively common, and follows a procedure or work instruction.	Service Team Owner	Considered SOP (standard operating procedures). Examples: patching servers, scheduled SaaS updates.
Normal	Any service change that is not a Planned or Emergency Change. This includes changes with	Change Advisory Board (CAB)	Examples: Upgrade system to major new version,

Type	Description	Approval Required	Notes
	more than a low risk of service interruption, or which involve user experience changes.		update to a system with user experience change.
Emergency	A change that must be implemented as soon as possible, for example, to resolve a major Incident or implement a critical security patch.	ITS Leadership or Major Incident Manager	Examples: Shutting down a production system to prevent security incident or ensure continuity, shift system(s) to alternate site or zone, critical security patch that cannot wait until next patch window.

C. Compliance with Legal and Regulatory Requirements

The University has many federal laws and regulations that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry (PCI) Data Security Standard (DSS). The process of change management should support these, and other applicable University policies found on the University Policy Repository website.

D. Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

E. Emergencies

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the ITS Incident Response process. These actions may include rendering systems inaccessible. Exceptions to this policy will be handled in accordance with the Data Security Policy Compendium.

F. Exceptions

Exceptions to this policy will be handled in accordance with the Data Security Policy Compendium.

G. Review

This policy, and all policies, standards, handbooks and supporting materials contained within, will be reviewed by ITS on an annual basis.