Business Practice on Change Management

Accountability:
ITS Leadership, specifically, the Associate CITO of Professional Services, the Director of Infrastructure Services, the Director of Information Security and Compliance, the Manager of Communications, and the Associate CITO of Campus Relations are accountable for oversight of the ITS Change Management process.

Key members of local IT staff meet every Thursday morning to discuss prospective changes, system upgrades or maintenance. Typical discussions deal with potential impacts, best and worst case scenarios, back-out plans, and appropriate times for the change. Targeted communications to affected users are discussed planned in Change Management meetings if applicable.

Required attendance include leaders from the Infrastructure, Professional Services, and Campus Relations teams within ITS. Attendance is MANDATORY for any technician who has submitted a Request for Change (RFC) for the upcoming change cycle.

Applicability
All employees in ITS.

- For more information about the change management process, please refer to the [ITS Change Management Process](https://drake.teamdynamix.com/TDClient/2025/Portal/KB/ArticleDet?ID=60356) knowledge base article.

Audit Requirements
Changes that necessitate separation of duties for audit requirements cannot be performed by the initiating ITS staff and will be performed by personnel designated as production control based on instruction documented in the change management system.

Communication
Normal changes will be communicated within ITS through the use of the change management/reporting system. When necessary due to changes with broad campus impact, ITS will communicate with the campus community via the ITS website, OnCampus newsletter, social media, and/or the ITS calendar. [ITS staff must enter titles, descriptions and business impacts of changes into the change management system in terms that can be understood by the campus community](https://drake.teamdynamix.com/TDClient/2025/Portal/KB/ArticleDet?ID=60356). Changes that do not have an adequate communication plan will be rejected by the CAB.

Deviation Authority Process
The CAB may grant deviations from the Change Management Business Practice when legitimate needs require such deviations. Each person requesting a deviation from the Change Management Business Practice should submit deviation requests in writing to the CAB. Each deviation authorization or denial will be provided in writing by email from a representative of the CAB to the person requesting the deviation.

Testing
Changes must be tested and the test plan documented in the change management system where appropriate. Changes that are not tested or without adequate test documentation may be rejected by the CAB.
Definitions

Campus Community

Who is included:
Everyone affiliated with Drake who could be impacted by a ITS Change. This includes all faculty, staff and students as well as alumni, parents, trustees, applicants for admission, etc.

Responsibility:
- Review the change calendar to understand the impacts of change on business operations.
- Provide feedback on applied changes.

Change Advisory Board (CAB)

Who is included:
A group of people with different perspectives, backgrounds and areas of expertise that review changes from a process and governance standpoint to assure that all foreseeable risks have been identified and mitigated, and compensatory techniques are in place for any elements of exposure. This group includes but is not limited to leadership representatives from ITS departments. Representatives from other campus groups may be added as deemed appropriate by ITS leadership.

Responsibility:
- Maintain overview responsibility for implementation of this policy.
- Review and update this policy as appropriate.
- Review and approve or deny changes weekly; determine needed review on applied changes.
- Provide feedback to ITS staff on denied changes.
- Track and report on Key Performance Indicators and make adjustments to meet performance metrics.

Emergency Change

There are 2 levels of emergency change. See Priority for further definitions.

ITS Staff

Who is included:
Drake employees, consultants and contractors within Drake Information Technology Services.

Responsibility:
- Develop, test, document and submit changes.
- Review all submitted changes for potential issue or conflict and alert the CAB if issue or conflict exists.
- Associate feedback to changes applied to production to ensure that they are working as desired.

Priority

Business Emergency - A critical business process or communication cannot proceed without a change.

Emergency - A system is down and unusable.

Normal - A change that can be completed during regular ITS maintenance intervals.

Web change - A change that only affects our ITS public website.

Production Environment

The applications and systems, and supporting systems infrastructure, that the end users and the customers of Drake access and use on an operational basis to execute their business processes and transactions.

Production Environment Control

Who is included:
These are the personnel who are responsible for applying or rolling back change. For the purposes of information security (separation of duties) this role is essential in rolling out changes to information sensitive environments like the ERP system, however in other cases, this may be the same personnel who are developing and submitting change. For audit purposes it is essential to have this as a separate role when possible.
Responsibility:

- Apply and rollback approved changes.
- Document outcome of change application process.

Request for Change (RFC)

The formal request made by ITS Staff to make a change to the production environment.

Request for Change service request form.

Risk

The likelihood of a change being unsuccessful and causing a service outage.

A number of different factors will need to be considered when assessing the risk of a change to determine its category. These include the complexity, scope, testing, recovery and timing associated with the change, but general guidelines are as follows:

LOW

- Recovery/back out plan known AND tested
- Non-complex change (e.g. server reboot)
- Change that replicates normal user activity
- Change that is seamless or does not directly affect users
- Change tested successfully in an environment that fully replicates the production environment
- Significant history of successful implementation
- Change is isolated (e.g. single site, platform, service, or network)
- System that impacts ITS only and doesn’t prevent day-to-day activities

NORMAL

- Recovery/back out plan known AND tested
- Change to a component that has a history of some risk
- Change to a non-critical component
- Change tested successfully but where environment does not fully replicate production environment
- Change spans more than one ITS system or area (e.g. sites, platforms, services or networks)

HIGH

- Recovery/back out plan unavailable
- Change validation dependent on client usage (i.e. cannot be checked until user load applied)
- Change spans multiple sites, platforms, services or networks
- A single change delivering multiple fixes/builds/updates
- Change involves input from multiple support areas
- Change to a critical production component (i.e. a component that the service will not work without)
- Change not tested (at all, or to the maximum level of testing available)

NOTE: Emergency repairs may be made outside of the above times based on urgency and particular situation.

Support Center

Who is included:
Both student and full time employees of the Drake Support Center within the Campus Relations department of Information Technology Services and any other Information Technology Services personnel responsible for level 2 support.

Responsibility:

- Collect feedback.