# IT Change Management Policy
# TEC 14.0
## Office of Information Technology

Institutional Type: Operational
Applies to: Office of Information Technology Staff Members

## POLICY DATES

Issued: 12/4/2019
Revised Last: 2/23/2024
Edited by: Tina Stuchell
Reviewed: 2/23/2024

This policy establishes the requirements and processes that the Office of Information Technology uses to identify, document and authorize changes to within the Information Technology environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors.

### Definitions

| Term | Definition |
|---|---|
| Change Management | Refers to a formal process for making changes to IT systems. A process for recording changes in IT environments. |
| IT | Information Technology |
| Change Management Log Report | Log that is maintained by IT Staff Members related to changes in the IT Environment. |
| Change | The addition, modification or removal of approved, supported or baseline hardware, network, software, application, environment, system. |
| Change Authority | The person or group authorizing a change. |
| Change Control | The procedure to ensure that all changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the change. |
| Change History | Information of changes for historical purposes, for example, what was done, when it was done, by whom and why. |

### Policy Details

This policy formalizes the requirements for changes within the Information Technology environment. The change procedures are designed with the size and complexity of the environment in mind. The change process includes provisions that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

Change management generally includes the following steps:

- Planning: Plan the change, including the implementation design, schedule, communication plan, test plan, and roll back plan.
- Evaluation: Evaluate the change, including determining the risk based in priority level of service and the nature of the proposed change, determining the change type and the change process to use.
- Review: Review change plan with peers and/or appropriate change authority as determined by the type of change.
- Communication: Communicate about changes with the appropriate parties (targeted or campus wide).
- Implementation: Implement the change.
- Documentation: Document the change and any review and approval information.

Applies to: Information Technology Staff Members

- Post-change review: Review the change with an eye to future improvements.

This policy applies to all changes to architectures, tools and IT services provided by the Office of Information Technology. Modifications made to non-production systems (such as testing environments with no impact on production IT Services) are outside the scope of this policy.
Staff maintaining systems and network systems are required to document changes. The Office of Information Technology staff will record changes for the following categories of the IT Environment:

- Firewall
- Telephony/Teams environments (including audio codes)
- Network equipment (including Wireless Access Points (WAP))
- Servers, including new installation and patches
- Administrative and Academic Systems
- Mobile Apps
- Liquidation/Destruction of Hard Drives
- PCI Network
- Cash Registers
- NOC Access
- Internal Risk Assessment
- Penetration Network Tests
- Network monitoring/BitLyft

This list is not all inclusive but list the main categories that should be covered with regard to change management.

All changes to IT services must follow a structured process to ensure appropriate planning and execution.

Types of Changes:
There are three types of changes: (a) a standard change, (b) a normal change (of low, medium, or high risk), and (c) an Emergency Change.

**Standard** – A repeatable change that has been pre-authorized by the Change Authority by means of a documented procedure that controls risk and has predictable outcomes.
**Normal** – a change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process. Low, Medium, or High priority is determined by the Change Authority, IT or delegates according to the Risk Assessment Instrument included below.

a. Normal Low Changes must be reviewed and approved by the change authority.
b. Normal Medium Changes must be reviewed and approved by the Change Authority and unit director or system owner.
c. Normal High Changes must be approved by the IT Executive Team as Change Authority.

**Emergency Change** – A change that must be introduced as soon as possible due to likely negative service impacts. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps due to the urgent nature of the issue; however, any Emergency Change must still be authorized by a IT Executive.

Risk Assessment Instrument: Risk and Change Type Matrix for Normal and Emergency Changes.

- Determine the impact of the change to the service.
- Then assess the urgency of the proposed change (low can generally wait, Medium, cannot, and high needs to be done ASAP)
- The matrix shows whether the type of change is then a Normal Low, Normal Medium, Normal High, or an Emergency Change (Note: A Standard change does not need to use this matrix because risk is controlled by a pre-approved standardized process)

Applies to: Information Technology Staff Members

| | Low Urgency | Medium Urgency | High Urgency |
|---|---|---|---|
| Impact – Organization<br>Change affects more than 2,000 individuals | Normal Medium | Normal High | Emergency |
| Impact – Area<br>Changes affects approximately 1,000 or less individuals | Normal Medium | Normal High | Normal High |
| Impact – Department<br>Change affects approximately 100 or less individuals | Normal Medium | Normal Medium | Normal High |
| Impact – User<br>Change affects approximately 10 or less individuals | Normal Low | Normal Low | Normal Medium |

Changes to production systems are made only by authorized individuals in a controlled manner.

Cloud hosted/SaaS Software
Mount Union has many systems that are SaaS based. Regular upgrades to those systems are completed by the vendor on a regular schedule and communicated to Mount Union IT staff. If an emergency upgrade or patch is needed to be installed for SaaS software, the vendor completes those updates and will notify Mount Union IT staff.
It is important to record changes communicated to IT staff by vendor. The following information should be included:

- Date the change was implemented.
- Who made the change?
- Who authorized the change?
- What new functionality is available as a result of the change?
- What was the reason for the change?
- Was the change tested before implementation?
- Record version level

Mount Union on prem hosted systems.
For in house systems where possible a process for rolling back to the previous version should be identified. It is also important to document what changes have been made. The Change Management Log Report should be updated accordingly. It is important to include the following information when recording changes:

- Date the change was implemented.
- Who made the change?
- Who authorized the change? If multiple people, please record.
- What new functionality is available as a result of the change.
- What technical elements were affected by the change?
- Was the change tested before implementation?
- If software or firmware upgrades, record version level.

The Change Management Log Report is available for each IT Environment/System and is kept current by the manager and director of each area.

## Responsibilities

| Position or Office | Responsibilities |
|---|---|
| Office of Information Technology (Technical Services, Director of IT) | Update of policy and Change management log report |

# IT Change Management Policy
# TEC 14.0

## Office of Information Technology

Applies to: Information Technology Staff Members

| Position or Office | Responsibilities |
|---|---|
| | |

## Contacts

| Subject | Office | Telephone | E-mail/URL |
|---|---|---|---|
| | Office of Information Technology | 330-823-2854 | IT@mountunion.edu |

## History

This policy was established in 2019 part of GLBA compliancy.
All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued: 12/11/19

Revised: 2/23/2024

Edited by: Tina Stuchell

Reviewed: 2/23/2024