COLLEGE POLICY: 473

INFORMATION TECHNOLOGY CHANGE MANGEMENT

PURPOSE

The purpose of this change management procedure is to establish a structured, controlled, and auditable process for managing changes to information systems, applications, infrastructure, and business-critical processes.

SCOPE

This process will be used by all parties requesting changes to/within the UA Cossatot production environment including (but not limited to) changes such as:

- All organizational information systems, networks, applications, and cloud services
- All employees, contractors, vendors, and third parties who implement, request, or approve changes
- All changes that may affect system security, availability, integrity, performance, or compliance, including:
- Configuration changes
- Software updates and patches
- Network changes
- Infrastructure modifications
- Security control adjustments
- Business process changes affecting IT systems
- Planned/scheduled outages
- Emergency changes

REPONSIBILITY AND AUTHORITY

The Director of Information Technology will ensure the change management process is established, implemented, and maintained. Information Technology staff will continuously monitor, and update procedural controls as needed.

OBJECTIVES

- Implement a common approach for requesting/documenting change requests/requirements.
- Ensure proper controls and authorizations for all change requests.

- Provide an audit trail within our IT ticketing system of all information technology requested and implemented changes.
- Ensure proper communication of changes with end users.
- Create faster, more predictable change implementation.
- Reduce risk while implementing new technologies.
- Increase visibility into the change process.
- Improve service levels, including reduced downtime across the IT infrastructure.

DEFINITIONS

- **Change** is defined as – Any modification to the production environment as defined in the procedure scope.
- **Routine Change**: A change that will have minimal or no impact to the user community.
- **Comprehensive Change**: A change that impacts a significant number of users or a critical system.
- **Emergency Change**: An urgent request to correct a problem or restore service in the production environment.
- **Change Advisory Board (CAB)**: Structure for review and approval of all comprehensive changes. It consists of all IT team members.
- **Change Manager**: Director of Information Technology Services or his/her designee.
- **Change Implementer**: IT staff member requesting and in charge of implementing the change.
- **Lead Time**: Time required to obtain necessary approvals, plan and communicate upcoming changes to the campus community.
- **Staging Tests**: Application system and network tests to validate planned changes will perform as expected.
- **UAC IT Infrastructure**: All hardware, network and software components for the common infrastructure environment.

POLICY

UA Cossatot maintains a formal change management process to ensure all modifications to systems, applications, infrastructure, and business-critical operations are introduced in a secure, controlled, and predictable manner. All changes must be documented, assessed for operational and security impact, and approved by designated authorities before implementation. Testing and validation are required to confirm changes function as

intended and do not introduce new risks. Emergency changes may be expedited but must still be documented and reviewed afterward. A post-implementation review is conducted for all changes to verify success, capture lessons learned, and update configuration baselines. This policy supports operational stability, security, compliance, and alignment with NIST change management controls.

1. Requesting a Change

    a. All change requests must be entered into the IT ticketing system change management section.
    b. The change request will include a description of the change, detailed instructions for the change, testing instructions for the change, and back out instructions if problems are encountered.
    c. The change request is sent to the CAB for approval.
    d. No routine or comprehensive change can be made until the change has been processed through the approval process detailed below. Emergency changes are an exception and are shown below.
    e. The lead time for routine changes requires that the requestor must initiate the change approval process by end of day on Wednesday prior to the change for the Friday/Saturday change window.

2. Routing Change Process and Approval

    All routine changes follow the change request procedure above. These changes are automatically sent to the supervisor of the Change Implementer. Once approved by the supervisor, the change request can be scheduled for an upcoming maintenance window. If no downtime is required, the change can be implemented immediately. Changes that require downtime or disruptions in service must be scheduled during available maintenance windows.

3. Emergency Change Process and Approval

    Emergency/critical changes may be required to quickly address production issues/outages. Emergencies usually occur because of problems and enter the change management process by a request from the service desk or as the result of an incident or security event.

    In the case of emergency changes, a streamlined process is used to allow the fastest possible response while still maintaining the proper levels of approval, logging, monitoring, communication and closure of all change related activities.

a. If time and circumstances permit, the change request is entered into the IT ticketing system with a type set to “Emergency”. If time does not permit the change to be entered into the IT ticketing systems immediately, the Change Manager should be contacted by phone or email to give oral approval to proceed.

b. The Change Manager evaluates how the change impacts the infrastructure and may elect to involve other members of the Infrastructure Group or the wider CAB if the change is evaluated as major Impact (multiple systems, etc.).

c. The Change Implementer completes the change and enters updates into the IT ticketing system as time permits to provide information to the Change Manager and to update and close out the Change Management documentation.

4. Notification Process

   Timely and transparent notifications will be made to the campus community regarding changes that may affect academic operations, technology services, security practices, or access to institutional resources. Communications must be issued through established channels—such as campus email, official websites, and other approved messaging platforms—and include a clear description of the change, its purpose, expected impact, and any required actions from students, faculty, or staff.

5. Maintenance Window

   A maintenance window is a regularly scheduled preset time and day when planned changes, upgrades and other maintenance tasks can be performed on hardware and software systems. Users will be made aware that the systems may not be available during the preset timeframe and will be able to plan accordingly.

   Maintenance windows will be scheduled outside of normal campus operating hours to limit disruptions. These windows are on Friday and Saturday from 9:00 PM to 7:00 AM. In situations when the change can be made earlier due to the schedule maintained in the specific location, an exception to the time frame can be obtained by contacting the Director of Information Technology Services for approval.

   Third-party and cloud hosted solutions often perform maintenance outside of scheduled maintenance windows. These include, but are not limited to, Microsoft 365, Blackboard, Workday, etc. Typically, these maintenance windows are determined by the service provider and communicated to the IT department prior to implementation. IT staff will provide notifications to the campus community regarding significant updates to these systems, including any scheduled downtime or service disruptions.

6. Documentation

   All changes must be fully documented including:

   1. Requests and Approvals
   2. Testing Results
   3. Implementation notes
   4. Rollback actions (if used)
   5. Post-implementation review findings

7. Compliance and Audit

   Change requests and logs will be retained for documentation and audit purposes. This process will be reviewed annually or after major system or organizational changes.

Policy History:
November 2, 2026
