

Policy	Change Management Policy
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	June 4, 2025
Reviewed	June 23, 2025; May 5, 2026; June 24, 2026
Approved by	Provost and Vice President of Academic Affairs
Version	26.1

CHANGE MANAGEMENT POLICY

PURPOSE

Shepherd University's Change Management Policy establishes standards for managing upgrades, additions, or changes to IT infrastructure or systems. The intent of this policy is to reduce operational, security, and availability risks by ensuring changes are communicated, reviewed at an appropriate level, and implemented in a controlled and transparent manner, while remaining proportionate to the size and resources of the University's IT environment.

POLICY

GENERAL IT CHANGE MANAGEMENT

Shepherd University operates with a small IT team, and change management is intentionally risk-based and collaborative. This policy applies to general IT changes, including but not limited to:

- Network configuration changes
- Server and storage changes (physical or virtual)
- Security-related changes
- Infrastructure additions, removals, or reconfiguration

General Change Management Practices

Planned changes are communicated to IT Services staff prior to implementation to promote awareness, coordination, and early identification of potential risks or conflicts. Preparation is proportional to the scope and impact of the change, and may include

- Purpose and scope of the change
- Expected impact or downtime, if any
- Timing of implementation
- Rollback or recovery considerations, when appropriate

The team reaches consensus on the planned change, and this serves as approval. Records of change management are maintained through team chats and change management tickets.

Emergency Changes

- Team managers may implement emergency changes when required to restore services, address critical security vulnerabilities, or prevent significant operational impact.
- Emergency changes may be implemented outside of normal communication processes when time-sensitive conditions exist.
- Emergency changes are communicated to the IT team as soon as reasonably possible after implementation, including a summary of the reason for the change and actions taken.

BANNER SYSTEM CHANGE MANAGEMENT

Updates to the Banner system are coordinated with internal IT Teams and Data Custodians. When a need for an update is identified, the following steps are taken and documented.

1. The update is announced to the Data Custodians and an installation to one of the test databases is scheduled.
2. Internal IT teams are notified, if necessary.
3. The installation takes place, and the Data Custodians begin testing the upgrade/release.
4. When Data Custodians and IT Services agree that testing is complete and successful, a date is scheduled for the production upgrade.
5. Internal IT teams are notified. Estimated production downtimes are announced to internal IT and Data Custodians.
6. The upgrade takes place as scheduled.

If the Banner General Custodian/IT Applications Manager deems the change to be an emergency, the Emergency Change procedures above can be implemented.

This process ensures that changes to enterprise systems are communicated, tested, and implemented in a manner appropriate to institutional risk and impact.

SCOPE OF AFFECTED PARTIES

This policy applies to all users, such as students, faculty, staff, or affiliates of Shepherd University accessing Shepherd University IT resources.

ROLES & RESPONSIBILITIES

CIO/CISO – Information Privacy Officer

- Oversee and administer this policy.
- Provide authorization and direction to IT Services staff in accordance with this policy.
- Ensures change management practices align with institutional risk management.

IT Services Staff

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.

RELATED

Patch Management Policy