Policy Title: IT Change Control	**Effective Date: 6/9/2009**
Policy ID: IT-PO-5201	**Date of Last Review: 06/26/2026**
Oversight Department: Information Technology Services	**Next Review Date: 06/26/2027**

1. Purpose

Radford University is committed to maintaining reliable and secure technology infrastructure. The purpose of the Change Control policy is to manage change in such a manner that staff and customers can plan accordingly and to manage and minimize risk. Change to the IT environment requires forethought, careful monitoring, and follow up evaluation to eliminate or reduce any negative impact to the user community, and to increase the value of IT resources and services. To accomplish this, it is important that all changes be documented, providing a record of what changes are made, when they are made, who made them and why they are made. Communication of changes with customers and Information Technology Services (ITS) staff is also a key component of change control.

2. Policy

All system changes must be documented according to requirements for the type of change being implemented (Routine, Minor, Major, or Emergency).

2.1 Major Changes

Major changes (see Section 4: Definitions below) must be appropriately requested, documented, and approved in advance. All Major changes should be scheduled during maintenance windows where possible. Changes will be documented and maintained in the department's repository according to department procedures.

- Requests for Major changes must include the following at a minimum:
  - Person requesting the change
  - Category
  - Business Service
  - Short title for the change
  - Description of change
  - Type (Major)
  - Assignment Group
  - Assigned To
  - Planned Start Date and Time
  - Planned End Date and Time
  - Change Plan
  - Back out/recovery plan
  - Test plan
  - Communication plan

- Change Approval
  - Supervisor/Manager
  - CISO (if Security or Firewall related)
  - System Owner
  - Managers Meeting – Review Only

  - Directors Meeting – Review Only
  - CIO

- Communicating a Change
  - All Major changes that will have a noticeable impact, or potential for a noticeable impact, on the campus community will be communicated to the campus community as defined by the Communication Plan.

- Testing
  - Appropriate testing must be performed in a testing environment and verified by the System Owner or Data Owner before changes are executed in a production environment. If a test environment is not available, risk mitigation procedures must be documented and approved by the System Owner.

- Completion of Change
  - Once a change is completed, the appropriate System Owner or Data Owner will be notified that the change has been completed successfully and any follow-up details of the change provided.

2.2 Minor Changes

Minor changes (see Section 4: Definitions below) must be appropriately requested, documented, and approved in advance. Minor changes should be scheduled during maintenance windows where possible. Changes will be documented and maintained in the department's repository according to department procedures.

- Requests for Minor changes must include the following at a minimum:
  - Person requesting the change
  - Category
  - Business Service
  - Short title for the change
  - Description of change
  - Type (Minor)
  - Assignment Group
  - Assigned To
  - Planned Start Date and Time
  - Planned End Date and Time

- Change Approval
  - Supervisor/Manager
  - CISO (if Security or Firewall related)
  - System Owner

- Testing
  - Appropriate testing must be performed in a testing environment and verified by the System Owner or Data Owner before changes are executed in a production environment. If a test environment is not available, risk mitigation procedures must be documented and approved by the System Owner.

- Completion of Change

- Once a change is completed, the appropriate System Owner or Data Owner will be notified that the change has been completed successfully and any follow-up details of the change provided.

2.3 Emergency Changes

Emergency changes (see Section 4: Definitions below) require that the System Owner and Data Owner be notified, and all required documentation for the type of change (Routine, Minor, Major) be completed as soon as possible after the change.

The CISO has the authority to direct ITS staff to apply Emergency changes to protect Radford University infrastructure and data from compromise.

2.4 Routine Changes

Routine Changes (see Section 4: Definitions below) should be documented and entered in advance. Changes will be documented and maintained in the department's repository according to department procedures.

- Requests for Routine changes must include the following at a minimum:
  - Person requesting the change
  - Business Service
  - Short title for the change
  - Description of change
  - Type (Routine)
  - Assignment Group
  - Assigned To
  - Planned Start Date and Time

Routine Changes do not require prior approval.

3. Procedures

Refer to standards and procedures for IT Change Control.

4. Definitions

Emergency Change – Changes that need to take place immediately due to a performance problem, a critical system being unavailable, or a critical security problem.

Major Change – Changes that impact multiple systems or departments and/or require a significant service outage.

Minor Change - Changes that are required for the operation of the system but have low risk, do not require an outage outside the established maintenance window, and will not impact the user community.

Maintenance Window – A defined time when system changes, including minimal downtime, are acceptable.

Routine Change – Changes that are low risk, frequently occurring and follow an established, repeatable procedure.

5. Related Information

Minimum System Configuration Standard – IT-5214s

6. Policy Background

7. Approvals and Revisions

Approved: July 1, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: September 24, 2008
Minor changes for clarification
Approved: September 24, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: December 18, 2008
Policy renumbered to Information Technology Policy 5201 from former Information Technology Policy 111
Approved: December 18, 2008 by Vice President for Information Technology & CIO, Danny Kemp

Revised: June 29, 2009
Policy updated to provide coverage for all DoIT changes rather than just IT Infrastructure and procedures separated into standards and guidelines.
Approved: June 29, 2009 by Vice President for Information Technology & CIO, Danny Kemp

Revised: May 16, 2011
Minor changes to provide clarification to the purpose and definitions.
Approved: May 16, 2011 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: July 1, 2012
No changes.
Approved: July 1, 2012 by Vice President for Information Technology & CIO, Danny Kemp

Revised: February 3, 2016
Policy updated to reflect use of ServiceNow for Change Control tracking and acceptance of four change types and workflows (Routine, Minor, Major, Emergency) for the division.
Approved: February 3, 2016 by Vice President for Information Technology & CIO, Danny Kemp

Revised: February 28, 2019
No changes.
Approved: February 28, 2019 by Vice President for Information Technology & CIO, Danny Kemp
Reviewed: 2/28/2022
Policy reviewed during security standard review with minor wording changes for clarification. Revised with updated template.
Approved: March 08, 2022 by Associate Vice President for Information Technology & CIO, Ed Oakes

Reviewed: 8/6/2024
Minor wording changes

Radford University | Information Technology Services

Reviewed: 06/26/2026
Minor wording changes, added reference to IT-5214s.
Approved: June 26, 2026 by CISO Bob Burton.