Change Management

ROWAN UNIVERSITY POLICY

Title: Change Management Policy
Subject: Information Security
Policy No: ISO:2013:09
Applies: University-Wide
Issuing Authority: Senior Vice President of Information Resources and Technology and Chief Information Officer
Responsible Officer: Director of Device Management
Date Adopted: 07/01/2013
Last Revision: 08/11/2023
Last Review: 08/11/2023

I. PURPOSE

The purpose of this policy is to manage changes in a well-communicated, planned and predictable manner that minimizes unplanned outages and unforeseen system issues. Effective change management requires planning, testing, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the user community.

II. ACCOUNTABILITY

Under the direction of the President and Provost, the Chief Information Officer and the Information Security Officer shall ensure compliance with this policy. The Vice Presidents, Deans, and other members of management shall implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan Community who manage, change or control the University's electronic information and information systems.

IV. DEFINITIONS

Refer to Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy

V. POLICY

1. All changes to an information system or an information technology environment must follow appropriate change management procedures.
2. Change management procedures support the goal of increasing awareness and understanding of proposed changes across an organization and ensure that all changes are made in a way that minimizes negative impact to services and customers. Change management procedures must include the following steps:
    a. Categorized into separate levels, each with different approval and notification requirements that are outlined in the Change Classification Matrix.
    b. Assigned a priority based on the definitions outlined in the Change Priority Description.

    a. Planning and Submission: This phase consists of the steps to move a change from request to the eventual release into the production environment. These steps include the design, test, backup, rollback, and documentation of this request. Change requests are:
    b. Evaluation: This phase consists of reviewing the impact of the change in order to validate the change priority description, change category, schedule, risk and business impact, as well as defining the appropriate change process.
    c. Approval: This phase consists of reviewing the change plan with peers and/or Change Advisory Board (CAB) as appropriate to the change type and obtaining approval of the change plan by management as needed.
    d. Communication: This phase consists of communicating the change and any announcements for planned downtime to all affected stakeholders.
    e. Implementation: This phase consists of implementing the change by the change assignee or release team.
    f. Post Implementation Review and Closure: This phase of closing the change request and reviewing the lessons learned from successful or failed changes with the goal of learning from the experience, documenting them for future reference.
3. Change requests must adhere to the following:
    a. A change request must be submitted for all changes in accordance with change management procedures.
    b. All change requests must adhere to the time requirements set forth in the change management procedures to enable adequate review of each change type including but not limited to normal, em ergency, or standard changes.
    c. All change requests must go through the approval process in accordance with the change management procedures before proceeding with the change implementation.
    d. Any change request not meeting the criteria established in the change management procedures will be denied.
    e. All change requests must include the items and necessary documentation, test plans and information outlined in change request requirements
4. Approvals, Pre-Approvals or Change Exemptions:
    a. All changes are subject to the approval process outlined in the procedures for the Change Management Process, Normal Change Process, Emergency Change Process or Standard Change Process.
    b. CAB meetings should occur on a bi-weekly schedule but no less than weekly to support the review and approval of change requests.
    c. In coordination with the Information Security Office (ISO), the CAB chair may define criteria under which a change may be considered pre-approved or exempt from change control.
    d. Pre-approved criteria must be documented and made available for all CAB members.
5. Change Communication:
    a. All changes are subject to the communication processes outlined in the planned maintenance communication.
    b. The change requestor is responsible to ensure that communication flows to the stakeholders impacted by the change. The CAB has the authority to designate the flow of specific communication.
    c. All change must be communicated to the corresponding stakeholders including data owners, data stewards, and where appropriate the general university community
6. Change Control Process Documentation:
    a. Documentation supporting the change control process must be maintained and reviewed periodically as needed.
7. Testing and Validation:
    a. Test environments are recommended for information technology systems or environments creating, processing, storing or transmitting data classified as confidential.
    b. For changes impacting confidential data, testing and validation must be completed to ensure the isolation of the change, minimize the unnecessary impact on relevant business process(es), and ensure a successful change implementation
8. Roles and Responsibilities:

a. The change management process is supported by the following stakeholder roles and associated responsibilities:

Roles	Description/Responsibilities
SVP and Chief Information Officer (CIO)	The SVP and Chief Information Officer designates and appoints the CAB Chair.
Information Security Officer	The Information Security Officer may provide staff with security expertise to serve on the CAB and/or to conduct security impact analysis prior to approval of a change. The Information Security Officer or designated staff has the authority to reject a change if deemed the change would cause harm to the university.
Chief Technology Officer (CTO)	The CTO must provide staff with infrastructure expertise to serve on the CAB and/or to conduct technology impact analysis prior to approval of a change. The CTO or designated staff has the authority to reject a change if deemed the change would cause harm to the university.
Directors of Software Development & Systems Services and Business Intelligence & Analytics	The Directors of Software Development & Systems Services and Business Intelligence & Analytics must provide staff with application and analytics expertise to serve on the CAB and/or to conduct technology impact analysis prior to approval of a change. The Directors of Software Development & Systems Services and Business Intelligence & Analytics or designated staff have the authority to reject a change if deemed the change would cause harm to the university.
Change Advisory Board (CAB) Chair	The Change Advisory Board (CAB) Chair functions as the chairperson for the CAB. The CAB chair is responsible for managing the implementation and maintenance of the change management program. Responsibilities and authority of the CAB chair includes but are not limited to: • Ensuring all steps of the change management procedures are followed in accordance with section V.2 of this policy. • Management of CAB membership including appointment of new members and offboarding of old members • Ensuring CAB members have access to CAB resources including system tools, procedures, and training. • Ensuring change management program documentation is maintained. • Designation of a backup to handle change coordinator and change meeting responsibilities. • Cancellation of CAB meetings when no changes are due for review • Discretionary authority to override any deviation from the change request procedures. Any deviation must be recorded in the change management system.

Change Coordinator	The CAB chair acts as the routine change coordinator. The change coordinator functions as the individual responsible for overseeing the change management meetings. The CAB chair can designate another individual to act as the coordinator in their absence. The change coordinator hosts weekly change management meetings and coordinates the flow of change requests on the agenda.
Change Advisory Board (CAB)	The Change Advisory Board (CAB) is a group of individuals that have the collective responsibility and authority to review and approve changes. The group is chosen to evaluate changes from various perspectives within the organization and approve changes based on their domain expertise. The CAB is a check and balance on change activity, assuring that changes are held to the defined criteria before being implemented. Responsibilities and authority of the CAB includes but are not limited to: • Acting in an advisory capacity to the change manager for all changes. • The CAB is required to participate in the change management meetings facilitated by the change coordinator • The CAB may invite guests to the change management meeting as needed to provide additional perspective from the business or user community.
Change Advisory Board (CAB) Guests	Change Advisory Board (CAB) Guests are individuals with subject matter expertise who may be asked to participate in meetings to discuss specific changes that impact their areas (e.g. individuals from business or user groups)
Change Requestor	The Change Requestor is the individual requesting the change to be reviewed and considered for implementation. This request for a change may originate from any number of sources including the end user of the system, the support desk, or from management. Proposed changes may also originate from vendor-supplied patches, application updates, security alerts, system scans, etc
Change Manager	The role of the change manager in the change process is to authorize /approve all changes. The change manager also ensures that all activities to implement the change are undertaken in an appropriate manner and are documented and reviewed when completed.
Change Implementer	The change implementer will usually be the technology subject matter expert who is responsible for implementing the change into production.

VI. POLICY COMPLIANCE

Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment or dismissal from school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. Unscheduled or unauthorized changes that occur outside this Change Management Policy will be considered violations. Sanctions shall be applied consistently to all violators identified in ***Section III Applicability*** regardless of job titles or level in the organization per the Acceptable Use Policy.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer