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 & Technology and Chief Information Officer
Responsible Officer: Director of Information Security
Date Adopted: 07/01/2013
Last Revision: 07/26/2018
Last Review: 07/26/2018

I. PURPOSE

To ensure a change management process is in place for the University's, Information Technology environment(s) managed both internally or externally. This policy addresses changes involving all critical systems, including, but not limited to changes of operational systems, application systems, network infrastructure, hardware installation, operating procedures and maintenance.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer, Deans, Vice Presidents, shall implement this policy throughout the University, and the Director of Information Security shall ensure compliance.

III. APPLICABILITY

This policy applies to all Departments, Colleges, Business Units, and Vendors who manage IT environments. It includes all changes to the production information technology environment, as defined below.

IV. DEFINITIONS

1. **Change** - The addition, modification or removal of approved, supported or base lined hardware, network, software, application, environment, system, desktop build or associated documentation of the production IT environment.
2. **Production IT environment** - system components used to provide information technology (IT) service to employees, faculty, patients, students, including but not limited to: server hardware and associated operating systems, virtual servers, software applications, virtual applications, networks, data storage, air-conditioning, power supply, server rooms, datacenters, networks, and workstations that are part of the University Environment. This includes IT environments managed by IRT, departments, colleges, and vendors.

V. REFERENCES

1. Change Management Procedures for IRT

VI. POLICY

1. General Principles:
   Change management refers to a formal process for making changes to IT services. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimizes negative impact to services and customers. Change management generally includes the following steps:
   a. **Planning:** Plan the change, including the implementation design, scheduling, communication plan, testing plan and roll-back plan.
   b. **Evaluation:** Evaluate the change, including determining the priority level of the service and the risk of the proposed change; determine the change type and the change process to use.
   c. **Review:** Review Change Plan with peers and/or Change Advisory Board as appropriate to the change type.
   d. **Approval:** Obtain approval of the Change Plan by management as needed.
   e. **Communication:** Communicate about changes with the appropriate parties.
   f. **Implementation:** Implement the change.
   g. **Documentation:** Document the change and any review and approval information.
   h. **Post-change review (if necessary):** Review the change with an eye to future improvement
      i. All changes to IT services must follow a standard process to ensure appropriate planning and execution
      ii. Changes are categorized into four categories, each with different approval and notification requirements that are outlined in the Change Classification Matrix (Appendix A). In addition, all changes are assigned a priority based on the Change Priority definitions (Appendix B).
      iii. It is the responsibility of the CIO, Dean, and/or Vice President of the business unit or college to ensure that all areas under their direction have documented processes that meet minimum standards, are reviewed annually, and are communicated to staff. The CIO, Dean, and/or Vice President serves as Change Manager by default and is ultimately responsible for ensuring that changes are made in a manner appropriate to their impact on university operations.
2. Minimum Standards:
   a. All changes must follow a process of planning, evaluation, review, approval, and documentation as referenced in the Change Management Procedure for IRT.
   b. All changes deemed Normal Major must be presented to a Change Advisory Board (CAB) for input and advice (See Section D – Roles & Responsibilities"). Should a Change Manger (or designee) decide to act contrary to advice from the CAB, a written explanation must be submitted to the CAB and the Vice Provost for Information Services. In addition, before a change can be deemed a Standard Charge it must be presented to the CAB for input and advice.
   c. All changes deemed Emergency must be presented to a Change Advisory Board (CAB) for input and advice unless time constraints require that changes be made prior to submission. In these cases, verbal approval must be given by the Change Manager. Submission to the Change Advisory Board for review must be done by the next scheduled meeting.
   d. Documentation of all changes must be made in a Change Log that is stored in a common location so that coordination of changes across the organization can be managed appropriately
3. Security Review and Approval:
   a. In addition to the requirements above, all security changes must be reviewed and approved by the Information Security Office (ISO).
   b. All firewall, ACL, and GPO changes must include a business justification for each change item
4. Roles & Responsibilities:

Roles	Description/Responsibilities

Change Advisory Board (CAB)	The Change Advisory Board is a group called together by the Change Coordinator to act in an advisory capacity to the Change Manager to all changes that are categorized as major or emergency (after triage). They also authorize changes as Standard Changes, if the qualifications are met. The CAB is made up or individuals within or outside IT who are relevant in the making the decisions on whether a change should be authorized. They are called together as required in order to ensure that changes are progress in a prompt and efficient manner.
Change Advisory Board Members	• Review the list of scheduled changes• Attend a weekly meeting either in-person, by video or telephone conference.• Prepare for the weekly meeting by inviting representatives from business or user groups, technical support staff and vendors as necessary to resolve potential conflicts.• At the meeting, affirm acceptance of planned changes on behalf of the Department or state potential conflicts and work to resolve them. Stated positions will be required and recorded.
Change Coordinator	The Change Coordinator will be the chairperson for the CAB. Responsible for the coordinating the flow of documentation/communication surrounding any changes to the IT production environment.
Change Implementer /Change Implementation Team	The Change Implementer will usually be the technology subject matter expert who is responsible for implementing the change into production. If the change implementation needs external third party or supplier involvement this needs to be documented within the RFC form.
Change Initiator	Anyone can initiate a change within the organization – however, consideration must be given to whether this should include all users. If users are to be allowed to raise changes this should be controlled through the service desk, this will ensure that only relevant and appropriate changes are raised.
Change Owner	The Change Owner is the person who is responsible for the making the change happen, ensuring the change ticket is updated and marked as completed. This includes designing the change.
Change Tester	Wherever possible with all changes the Change Tester should not be the Change Implementer. This is to ensure rigorous and error free testing.
Internal Audit (IA)	Determine the effectiveness of internal controls, adherence with applicable laws and regulations, and reliability of financial reporting
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.

5. Non-Compliance and Sanctions
   Violation of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a college, and may subject the violator to penalties stipulated in applicable state and federal statutes.

VI. ATTACHMENTS

1. Attachment A - Change Classification Matrix
2. Attachment B - Change Priority Description
3. Attachment C - Clarification of Change Management Requirements with Respect to Virtual Environments

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer

ATTACHMENT A
Change Classification Matrix

Change Classification Matrix			
Level	**Description**	**Risk**	**Submittal/Approval Requirements**
Normal Major Change **	Potential to disrupt critical business and/or student activities for many users.	High	Change Request is submitted at least 7 calendar days prior to target implementation date
	Introduces major new technologies on a considerable scale		
	Affects a major part of the business-critical infrastructure		Review and approval by the Change Manager and Change Advisory Board (CAB)
	High probability of service outage with lengthy back out plan (> 1hr)		
	Complex or lengthy implementation		
	Not standard or emergency change		
Normal Minor Change	Change impacts a small user group.	Moderate	Change request is submitted prior to EOB on the day preceding a CAB meeting and target implementation time is scheduled after CAB
	High probability of success		
	Not standard or emergency change		Review and Approval by the Change Manager
	Relatively simple or quick implementation and back-out		
Standard Change**	Pre-authorized change that has a established implementation path, that has been proven successful with minimal business impact and has a documented set of procedures, including a well documented and successfully tested back out procedure.	Low	No minimum submission requirement.
			Initial Review and Approval by Change Manager and CAB, with approval expiration date of 1 year. Subsequent implementations do not require approval, however will be recorded in the work log of the Standard Change.
Emergency Change **	Critical service is down or severely impaired with disruption to business and/or student activities	Critical	Email notification of change to Information Security Office immediately
			Change Request is submitted within 1 business day after the start of the triage
	Change Request is deferred until the issue is resolved or under control.		Change is reviewed at the next Change Advisory Board (CAB) Meeting

** Requires Review/Approval by the Change Advisory Board (CAB)

ATTACHMENT B
Change Priority Description

Priority	**Description**
Immediate	Requires immediate implementation (emergency change process). Causing loss of service or severe usability problems to a larger number of Users, a mission-critical system, or some equally serious problem. Immediate action required. Resources may need to be allocated immediately to build such authorized changes.
High	Requires implementation within 48 hours. Severely affecting some users, or impacting upon a large number of users. To be given highest priority for change building, testing and implementation resources. (Other than emergency).

Medium	Requires implementation within five days. No severe impact, but rectification cannot be deferred until the next scheduled release or upgrade. To be allocated medium priority for resources.
Low	Requires implementation by an indicated date. A change is justified and necessary, but can wait until the next scheduled release or upgrade. To be allocated resources accordingly.

ATTACHMENT C
Clarification of Change Management Requirements with Respect to Virtual Environments

Introduction

When using virtual environment technology, certain changes should be considered changes to the active production environment and should be scheduled in accordance with the IRT Change Management policy. Other changes may be made in such a way as not to impact the production environment, and are therefore exempt from the IRT Change Management policy.

This example applies only to virtual environments, not to systems in general. Exemptions are offered for cases where a change cannot impact the production environment.
Note: Clustered pair server technology is not considered part of a virtual environment. Although service fails over from one server to another, there is a momentary lapse of service in the active production environment, as well as a risk of not restoring full redundancy.

Virtual Servers: VMware

The terms host and guest describe the physical and virtual machines. The physical computer on which we install VMware Workstation software is called the host computer, and its operating system is called the host operating system. The operating system running inside a virtual machine is called a guest operating system.

IRT provides a host server service. If there are changes in interface connectivity or service availability of the host, then IRT will schedule such changes per the IRT Change Management policy. However, routine maintenance, such as operating system patching, is done without impacting interface connectivity or service availability, is not considered part of the active production environment, and is therefore exempt from the IRT Change Management policy. Detailed records of such routine maintenance are stored in the VMWare environment.

IRT also provides guest server service. Changes to guest servers may impact service to the production environment and therefore should be scheduled in accordance with the IRT Change Management policy.

Virtual Applications: Xen Server and Citrix

IRT provides an application service. I f there are changes in interface Connectivity, service availability, the user experience or integration with other applications, then such changes are said to impact the production environment and IRT will schedule such changes per the IRT Change Management policy.