

Effective: February 21, 2017

Information Technology Policy CHANGE MANAGEMENT

Approved: February 21, 2017
President's Cabinet

Introduction

Change management ensures that proposed changes to Millersville University's IT networks, systems, and services are completed in an orderly and controlled manner; ensuring effective delivery of IT services while reducing risk. This policy is intended to meet the foundation requirements for industry best practices as detailed within the Information Technology Infrastructure Library (ITIL) directly relating to IT change management.

All Millersville University IT staff are responsible for following these Change Management guidelines when introducing changes to the Millersville University's IT environment.

Purpose

The purpose of change management is to implement changes in Millersville University's production environments in a logical and methodical way which mitigates risk and maintains a stable environment.

Out of Scope

There are many IT services and tasks performed by the Millersville University IT department that do not fall under the Change Management policy. Services and tasks that are outside the initial scope of Millersville University's Change Management process include:

1. Contingency/Continuity/Disaster Recovery
2. Changes to non-production elements or resources
3. Changes made within the daily administrative process. Examples of daily administrative tasks include, but are not limited to:
 - A. Password resets
 - B. User adds/deletes
 - C. User modifications
 - D. Adding, deleting or revising security groups
 - E. Rebooting machines when there is no change to the configuration of the system

F. File permission changes

Definitions

Back out Strategy – Describes how a change will be reversed, or how the affected system will be placed back to its original state should a change fail.

Change – The addition, modification, or removal of approved, supported, or baselined hardware, network, software, application, or system components.

Change Authority – The individual who is responsible for authorizing a change request.

Change Implementation Plan – Describes in detail how a change is going to be successfully completed.

Change Management Team – Consists of IT personnel whose function is to review all Change Requests and ensure that all foreseeable risks have been identified and mitigated, and that plans are in place for any problems that may arise.

Change Test Plan – Describes in detail how the change will be tested to determine if the change can accomplish the desired outcome.

Requester – The individual requesting a change

Risk Assessment – describes the risk to the device, system, or network if the proposed change is not completed, the risks involved with implementing the change, and any service disruptions that may occur.

Policy

1. Changes will be categorized As Standard, Significant, or Emergency:

A. Standard – a low-risk change with well-understood outcomes that is regularly made during the course of business. A Standard change follows pre-determined processes that have been pre-approved by the Change Management Team and thus do not need to follow the Change Management process once defined as Standard.

a. New changes, expecting to be classified as Standard, must follow the Change Management process for initial approval to obtain pre-authorization.

B. Significant – A change that has a medium to high risk for critical services, involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Due to the ability to affect downstream or upstream services, any proposed Significant change must be reviewed by the Change Management Team and be authorized by the Change Authority.

C. Emergency – A change that must be executed with the utmost urgency in order to prevent any catastrophic events that are likely to occur and/or to recover services from such an event. These are changes that, if not implemented immediately, may leave Millersville University open to significant risk, or negatively impact the University's ability to conduct business. Emergency changes are not required to be reviewed by the Change Management Team, but must be authorized by the Change Authority.

- a. If services are down, the issue should be handled as an Incident and is not under the scope of the Change Management Policy
2. Documentation of Significant or Emergency changes must be made in a Process Log that is stored in a common location so that coordination of changes across IT teams can be managed appropriately.
3. Documentation of Standard changes must be done in a Change Log that can be reviewed for process improvement and root cause diagnosis.

Request for Change (RFC)

1. The Change Management process is initiated by the creation of a Change Request submitted through Millersville University's online ticketing system.
 - A. All documentation, advisory notes, and reviews for a specific Change Request will be attached to the request ticket.
2. All proposed Change Requests must include:
 - A. An implementation plan
 - B. A test plan
 - C. A back out strategy
 - D. A risk assessment
3. Significant Changes will be submitted to the Change Management Team at least 10 days prior to the planned change date.
4. Standard Changes that have not yet been pre-authorized must be submitted to the Change Management Team at least 7 days prior to the planned change date.
5. All Change Requests will be reviewed by the Change Management Team, and once approved, will be authorized by the Change Authority.
6. After a Significant or Emergency Change has been completed, the requestor must verify the change and complete a post-change review outlining whether or not the change resulted in the desired outcome.
 - A. Post-change reviews should be submitted to the Change Management Team

Roles and Responsibilities

1. Requester

- A. The individual requesting the change is responsible for:
 - a. Completing the Change Request ticket in full detail
 - b. Understanding the impact of the proposed change
 - c. Ensuring that the appropriate testing has been completed and documented
 - d. Ensuring that key stake holders have been informed and in are in agreement as to strategy
 - e. Creating an appropriate back out strategy
 - f. Ensuring that the necessary resources are available on requested implementation date
 - g. Verifying and documenting that the change was successful, or if it did not work, employing the back out strategy

2. Change Management Team

- A. The Change Management team consists of the following people:
 - a. Chief Information Officer
 - b. Director of Network and Systems
 - c. Director of Technology Support Services
 - d. Director of Information Systems Services
- B. The Change Management Team is responsible for:
 - a. Thoroughly reviewing and approving Change Requests; ensuring that all requests:
 - i. Have undergone proper planning and testing
 - ii. Have a sound back out strategy in place
 - iii. Have the lowest possible risk to affected services
 - iv. Are coordinated so changes do not impact each other, or occur during times of high impact for affected users
 - b. Providing advice regarding any additional measures that should be considered prior to the change.
 - c. Providing an advisory review that outlines the Change Management Team's rationale if a Change Request is denied

3. Change Authority

- A. The Change Authority for Millersville University is the CIO
- B. The Change Authority is responsible for:
 - a. Reviewing advisory input from the Change Management Team

- b. Reviewing and authorizing Change Requests after they have been approved by the Change Management Team

Governance of Change Management

1. Change Management Meetings

- A. These meetings may be held weekly, or as needed. Additional members not on the Change Management Team may be invited to these meetings as necessary.
- B. The purpose of these meetings is to:
 - a. Bring all required parties together to assess the feasibility of implementing the Change Request
 - b. To review the status of all open Change Requests and schedule changes for the current and upcoming weeks
 - c. Approve or disapprove proposed Change Requests
- C. Any Change Requestor whose request is scheduled for review is required to attend the Change Management meeting, or send a proxy

2. Approving Change Requests

- A. A majority of the Change Management Team must be present and approve a change for the request to move forward. If a majority of the Change Management Team is not present, the change will be held until such time as a majority has met and approved the change.
- B. Any member of the Change Management Team can hold a Change Request if a significant concern is expressed.
- C. A Change Request may be denied by the Change Management Team for a number of reasons, such as, but not limited to:
 - a. Resources are unavailable to execute the proposed change
 - b. Insufficient planning and documentation
 - c. Scheduling considerations
 - d. Risk is too high

Campus Communications

If a proposed change has a broad University wide impact, communications will be sent out to the University community and/or appropriate parties by email and/or web posting. Communications will be coordinated through the Change Management Team and must be approved by the Change Authority.