

Saint Michael's College – Department of Information Technology

Policy Title: Change Control for IT managed services and systems

Author: Saint Michael's College - Information Technology
Effective Date: 11/07/2004
Applies To: IT Operations
Last Reviewed: 05/12/2008
Description: Change Control for IT managed services and systems

Background: Change Control is the process that organizations use to identify, document and authorize changes to the environment. Saint Michael's College – Information Technology is engaged in a major effort to implement a change control practice to address all the IT managed services and the systems on which they run.

Purpose of Policy: This policy is necessary to safeguard data, equipment, and services that serve the entire college community and the constituencies that we serve. This policy is also necessary to ensure compliance with IT audit findings, Board of Trustee mandate, best practices in Information Technology, and federal, state and other regulatory requirements.

Expected Institutional Outcome: It is expected that this policy and the associated procedure will provide an audit trail of network changes, provide controls for those changes, and minimize impact to the user community.

Change Control Management Procedures

I. Purpose

Our mission is to provide the campuses with accurate and timely information in a reliable and consistent manner. Changes to the operating environment allow opportunities for errors that may disrupt our ability to provide high quality services to our constituents. Managing those changes can help reduce the introduction of errors. As a result, this procedure is a process to manage changes on the network and the potential impact to our users.

Change control also provides a means by which an audit trail of changes made to systems can be kept. This becomes valuable when the relationships between system failures and/or performance problems must be correlated and analyzed.

The change management procedures are meant to:

1. Document the reason for change – why is the change needed?
2. Identify who is responsible for the change
3. Document the steps required to make the change
4. Document back out procedures should the need arise
5. Assess the risk of failure and impact of the change

Saint Michael's College – Department of Information Technology

Policy Title: Change Control for IT managed services and systems

6. Aid in communicating with those affected by the change
7. Identify conflicts between multiple changes
8. Enhance awareness of all of the above.

II. Scope

This change control procedure applies to the following:

- Hardware
- System Software
- Database changes
- Application Software
- 3rd Party Tools
- Telecommunications
- Firewalls
- Network (LAN, WAN, routers, servers, software delivery, etc)
- Facilities Environment (UPS, electrical, etc.)
- External Factors

III. Steps

1. Request – the IT staff member(s) and/or the vendor responsible for implementing the change will complete the Change Control Event form. When preparing the form also consider these factors:
 - a. Risk
 - b. Impact
 - c. Communication requirements
 - d. Install time
 - e. Documentation requirements
 - f. Education/training needs
2. Change control forms will be reviewed by the IT staff. When a change requires a service interruption, the initiator of the change will work closely with User Services to create the appropriate communication.
3. Implementation – Changes will be made according to the submitted plan and in a manner that allows the change to be removed (back out plan) if necessary.
4. Review – the IT staff member responsible for the change event will review and document the implementation by completing the change event review form. Review allows IT staff and the change request author to verify that the change procedure was followed, the change procedure fulfilled its objectives, and implementation and back out procedures were adequate. Review also guarantees that problems are discussed for future planning and organizational learning. Changes are assigned a status of completed, not completed (either partially complete or not at all), failed & backed out, or canceled.

IV. Criteria for reviewing change requests

Saint Michael's College – Department of Information Technology

Policy Title: Change Control for IT managed services and systems

State of the network environment: Before determining if a change should be approved, the IT staff should consider the performance and availability of the network environment during the past week. In general, if performance and availability have been high (95% or better) the Leaders should be more inclined to approve changes that provide new functionality or changes that might have a high risk of failure. Conversely, if performance and availability has been poor, the Leaders should be more inclined to approve only those changes designed to correct problems.

Change level: As part of the approval process, the associated risk and impact of the change must be considered. Particularly important are the comments provided by the change author indicating the reasons for the assigned change level.

Aggregate effect of all proposed changes: When all proposed changes for a particular week are considered as a group, the combined effect may result in too much change activity or too much risk. When the staff reaches this conclusion, their responsibility is to prioritize the various changes, approve the most significant ones, and recommend that the others be re-scheduled.

Resource availability: Consideration must be given to availability of people, time, and system resources when considering the scheduling/approval of changes.

Criticality: There are issues that may alter the impact of the change as viewed by the author. For example, the change author may feel that the impact is relatively low because the change affects a small percentage of the community. However, the group may judge the criticality to be high because that small percentage includes a particular user that it feels has a critical need.

V. Emergency changes

All Emergency changes require review prior to implementation of the change. It is the responsibility of the requestor to escalate and procure all required approvals in an effort to implement the change as expeditiously as possible. All Emergency changes must be fully documented; due to the nature of an emergency request this will often occur after the fact.