Change Management Policy

Date: 05/04/07	**Policy ID:** UVAW – 17	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: All UVa-Wise Employees

Reason for Policy: prevent unauthorized changes and maintain a record of software and hardware changes.

Definitions:

Change

- A substantial change in the capabilities, operation, or way systems interface (something that would change how a system operates).
- Involve development effort by a programmer or engineer
- Involves risk of failure or unintentional consequences requiring mitigation
- Controls are designed to mitigate risk

System maintenance

- Updates to the operating system
- Installation of updates to applications provided by the vendor
- Backups
- Security work, system account maintenance, etc.
- Such events need to be scheduled, notification to end users provided as needed and completion of the maintenance action noted in system change log (aka HelpSpot ticketing system.).
- Maintenance actions do not require more stringent change management since risk is mitigated by vendor testing and procedural safeguards.

Policy Statement: The Change Management Policy exists to provide a method of monitoring changes and the systems affected, mitigation in the event that errors occur, and to ensure consistency in the maintenance and communication of changes that take place in the computing systems campus-wide.

Change Control Team: The Change Control Team will consist of the CIO and IT Managers and/or Staff impacted. Other resource people may be brought into discussions as needed but the CIO will retain the decision-making responsibility. Since the CIO has ultimate responsibility for IT operations, the CIO will have the final approval of all decisions and recommendations coming from the Change Control Team.

Change categories:

Production systems: Systems that are used in daily business activities.

Cat 1: Major changes to systems with high impact on daily business processes. Such changes include (but are not limited to) system reimplementation with a different functional design, changes to the operation that affects the interoperability with other systems, and system changes that have little or no way to return to the previous operational configuration.

Cat 2: Significant changes to systems with high impact on daily business processes. Changes in this category lack the level of risk associated with Cat 1 changes but do require preparatory work to ensure changes can be rolled back and / or coordinated work on other systems is required to ensure normal operations can be maintained.

Cat 3: Changes that only affect one system and do not pose a high risk to daily operations. All required work is within the control of one administrative group and impact of failure would not impact other systems.

Non-Production systems: Systems that are not in operational use do not come under change management. System developers should maintain adequate records on the development effort that other qualified technical staff members could pick up the work if needed.

System Maintenance: Routine activities that do not come under the formal change management process since risk is mitigated by vendor testing and procedural safeguards. These activities should be logged in the the HelpSpot ticketing system.. Discussion of planned activities at IT Managers meetings is recommended for coordination and department wide awareness in case unexpected results should arise. Examples of system maintenance include:

- Updates to the operating system
- Installation of updates to applications provided by the vendor
- Backups
- Security work, account maintenance, etc.
- These need to be scheduled, notification provided and noted in system change log.

Application: Systems identified in Appendix A: Critical Systems will be closely monitored by this formal change management system. All other systems are designated as non-critical and do not normally come under formal change management since failures in these systems do not have significant or far reaching impact on daily business. All system changes should be discussed at IT Managers meetings along with system maintenance actions that have impact on daily business to allow coordination, customer notification and review for any change management issues that may arise.

Process:

1. Proposed changes will be brought before the CIO and IT Managers and/or Staff impacted. The CIO will review the change for scope, risk, interface issues with other systems, and alignment with college goals and priorities.
2. If it is determined that the change has sufficient merit to warrant further development, the CIO will assign an appropriate category to the change and approve further development on the

change including appropriate documentation of what will be done. (proposed changes that do not need the formal process will be handled under system maintenance guidelines)

3. Requestor will research change and document findings and requirements on Change management form for all Cat 1 changes and any others the CIO and IT Managers and/or Staff impacted determines that more formal controls are appropriate.
4. CIO will review submitted change management form sections on testing, change documentation and rollback plan. If planning is satisfactory and resources are available for the change, the CIO will approve the implementation of the change. If these things are not completely ready, CIO will withhold approval pending correction of deficiencies.
5. Upon completion of approved changes, the date of implementation will be recorded on the form.
6. Approved change requests can be withdrawn prior to implementation if the need arises to do so. Documentation of the withdrawal including date, reason for withdrawal and CIO approval of the withdrawal shall be filed with the original request and the status of the request listed as “closed” on the master list of changes.

Documentation: Change management forms will be serialized and maintained in the OIT central files. A master list of all changes will be maintained that includes the serial number of the change, a descriptive title for the change, and current status for all changes the CIO determines should come under the formal change management program.

Status may include:

Submitted changes that have received an initial Change Control Team review and approved for further research and development.

Approved changes that have completed research stage and have been approved by the CIO for **implementation**.

Completed implemented changes.

Withdrawn changes withdrawn from the program without implementation

Review: An updated listing will be provided to the IT managers for review at the first meeting of each month. Managers will review status and follow up as needed on open changes. The purpose of the review is to ensure changes are completed within the constraints of available resources and overall departmental priorities.

Background:

Challenges:

- Lack of a equipment / systems to develop and test in a non production environment
- Thin staffing means most functions have one specialist with only casual backup
- Staffing levels virtually eliminate creator / installer separation
- Work load to maintain and install systems exceeds resources without the overhead of change management requirements

Conclusions:

- Critical systems / changes will be characterized by those things that have a significant impact on daily business processes. (assumes the college is open for business)
- System maintenance activities should be logged in the HelpSpot ticketing system.
- Focus more rigorous change management requirements on true changes that are developed in house.
- Added effort should equate to higher risk activities
- Lower risk activities should have minimized requirements
- All changes must be discussed with managers team prior to implementation. Level of risk and scope of impact will be considered and change will be assigned a change category which will determine the extent of controls that are appropriate.

Change Management Form

ID #: CM – ____________________ Date: ____________________

Requested by: ____

Proposed change(s):____

____

____

____

____

____

Reviewed by the Change Control Team:

Date: ____________________ Approved __________ Denied ____________

Assigned to Administrator (Name): ______________________________

Testing Procedures and Verification: ______________________________

____

____

____

Fully document change(s): ____

____

____

____

____

____

Roll Back Plan: ____

____

____

Implementation reviewed and recommended by the Change Control Team: Yes ________ No ____________

Date Recommended: ________________

Implementation Approval by CIO: Yes __________ No ____________ Date: _____________

Change(s) moved to production Date: ______________________________