Delaware State University

University Area(s) Responsible: Division of Technology and Information Systems; Office of Finance and Administration

Procedure Number & Name: 8-02: Change Management Process

Approval Date: 7/11/11

Revisions: _____

Related Policies and Procedures: _____

Purpose

The purpose of this set of procedures is to identify, plan, manage and control change within the Division of Technology and Information Systems effectively. Changes will take place and we need to be prepared to manage them before they are implemented. There is a need to record change requests. Change requests need to be reviewed and evaluated before they are approved, deferred or rejected. A request for change should include, whenever possible, a planning and a testing component to assist in the approval and implementation process.

Procedures

Change Management Process

The goal of Change Management is to control and manage approved changes within accepted risk levels, and should allow you to implement a comprehensive change management system that permits you to handle pre-approved changes as well as changes requiring complete individual review and approval.

Change Management Workflow

- Initiate Change Request

- Planning and Testing the Change (whenever possible)
- Change Levels and ITGC (IT Governance Committee)
- Approval from ITGC Members
- Co-ordinate Change Implementation
- Post Implementation Review
- Change History

Initiate Change Request

The change request form needs to have complete details about the reasons for considering the change, and how this change can impact services. The change request form must have following information so that the CIO and ITGC have all the details needed to make informed decisions.

- Impact Analysis - risk involved in either implementing or not implementing the change.
- Rollout Plan - how the plan will be implemented
- Back out Plan - plan to restore things to back to its original state should the plan fail.
- Checklist - List of mandatory items required for the plan to succeed

Planning and Testing the Change (whenever possible)

Once a need for a change has been identified and brought to the attention of the ITGC through a change request, the following questions will assist in planning for a Change:

Determine the following information during the planning process:

- Identify and justify the necessary change.
- Who is responsible for the change?
- What effect(s) will the change have?
- When should the change occur?
- When will the change have the least chance of interfering with operations?
- Will appropriate support staff be available?
- Can the change be made within the standard maintenance window?
- Will there be enough time to review and test the proposed change?
- Why making the change is important?
- How will the change be made?

- Will the change result in any additional security issues or increase the risk to the system?
- What will be the Back-out procedures in case the change is not successful?
- What additional training and documentation will be necessary for both support staff and end users?

Test the Change (whenever possible)

- If a test environment is available, the change should be tested.
- Detailed discussions and tabletop testing should supplement testing in a test environment. They may also be used as an alternative if test equipment is not available.
- Look for unintended consequences that might result in stability or security issues.

Communicate the results of the tests to supervisory staff and the change committee, so that they may be considered in the review and final approval decisions.

Change Levels and ITGC (IT Governance Committee)

Level 1 changes

Level 1 changes require two approvals, the first by the CIO, and second from all the members in attendance at the ITGC meeting.

NOTE: An approved change request requires acceptance by 100% of ITGC members in attendance.

Level 2 changes

Level 2 changes are changes needing only CIO approval, such as changes that are deemed to have either a low impact on the end users or any task defined in a Pre-Approved list of changes.

Note – Tasks added to the Pre-Approved list of changes must be mutually agreed upon by the CIO and ITGC.

Critical Changes (and bypassing the process)

In some cases, events are critical enough that they must be rushed into production, creating an unexpected change. Each situation is different, and even though some steps might be bypassed, as much consideration as possible should be given to the possible consequences of attempting the change. It is still important to obtain sufficient approval for the change. What constitutes "sufficient approval" will vary, and should be defined by the department or business unit requesting the change.

Approval from ITGC Members

The ITGC Members meet (***to be determined)*** to discuss the changes that are submitted for approval. Based on the change control plan and the risk analysis, the ITGC Members in attendance make a decision to **Accept, Defer, or Reject** a Change Request.

Co-ordinate Change Implementation

All Approved Changes have to be implemented with minimal service downtime. Changes need to be prioritized by Urgency, by Incident, and Problem counts within the change level. This helps CIO's to prioritize and schedule changes. Change information will be disseminated via *Trackit* and a change calendar.

- Change Calendar

Based on the changes considered for implementation, the changes are scheduled and published. The Change Calendar keeps everyone informed when a particular service will be down for maintenance and when it will be restored.

Post Implementation Review

The Post Implementation Review helps IT and the CIO to keep track of the rolled out change to

- Capture any issues that occurred during or as a result of the change.
- Measure the effectiveness of the change.
- If necessary, based on results modify the change process.

Keep Track of the Change History:

As Change Management involves key business processes, it is important to maintain clear documentation about the change for both operational, as well as Audit reasons. All documentation should be stored online, in a backed up location.