EXAMPLE
IT Services Policy and Procedures

Change Management

Approved:  
Next scheduled review: April 27, 2015

Overview

EXAMPLE CHANGE MANAGEMENT DOCUMENT

The purpose of Change Management is to ensure that the negative impact of changes to a systems or organization’s Information Technology system is minimized by using a standardized process of governance.

Definitions

System Change Management – Process for determining the need for a system change. The definition of the proposed change. Subsequent implementation of proposed change. Review of results after implementation to verify that

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

ITRM - Information Technology Risk Management (ITRM) in the IT Network & Information Security (NIS) group.

Information Resource Owner - an entity responsible for:

- A business function; and,
- determining controls and access to information resources supporting that business function.

PROCEEDURES

1. PROCESS

a. Formally request a change – All requests for change within the will be documented by creating a new change request. The change request will be completed by the change requestor with assistance from a member of the Department administrative staff or IT staff.

b. Analyze and Justify Change – The change requestor and the IT Administration will work to develop a specific justification for the change and identify the impact on infrastructure, business operations and budget, identify business as well as technical risks, develop technical requirements, and review specific implementation steps. The change requestor with assistance from IT Administration will be required to submit a functional test plan that is sufficiently detailed to provide assurance that the change will have the desired result.

c. Approve and Schedule the Change – The Project Manager will chair a Change Management team consisting of – at a minimum -representative IS members from Network
Engineering, Server Administration, Operations, Applications Support, Security Administration, Database Administration, Desktop Support, and with appropriate members of the affected end-user community. The group will assess the urgency and impact of the change on the infrastructure, end user productivity and budget. In the event of a major or significant change the change request must be approved by the IT Director and, where appropriate as determined by the IT Director or on recommendation by the Change Management team, members of end-user management.

d. **Plan and Complete the Change** – The Change Management Team will assign specific IS members and identify appropriate end-user members to complete the change in a manner that will minimize impact on the infrastructure and end users. In the event that the change does not perform as expected or causes issues to one or more areas of the production environment, the team will determine if the change should be removed and the production environment returned to its prior stable state.

e. **Post Implementation Review** – A review will be conducted by the Change Management team to formally ensure the change has achieved the desired goals. Post implementation actions may include acceptance, modification, or backing-out of the change. The team formally documents the final disposition of the change as part of the Change Request documentation.

2. **ADDITIONAL RESOURCES**

   a. **Change Tracking Applications**
      
      i. A number of Change management or Change tracking application are available for purchase or in Open Source.
      
      ii. Change Tracking applications will monitor all changes in a system and maintain an active log of when and what changes are made and identify the user account initiating the change.

      iii. Such audit trails are essential to security audit or compliance issues.

   b. **Change Logging**
      
      i. A simple alternative is to ensure that a change log is in use and updated every time a change is made to a system.

      ii. Be aware that validity of a simple Change Log may come it to question as there is no inherent security involved