PURPOSE

Change management refers to a formal process for making changes to Information and Technology related services. The goal of change management is to increase awareness and understanding of proposed changes across an organization, standardize the process and ensure that all changes are made in a thoughtful way that minimize negative impact to services and departmental customers.

POLICY

This policy applies to all mission critical, IT-supported productions systems (hardware, software, application, network) which Prescott College relies upon to perform IT normal business activities. All changes to IT systems, equipment, and services (both new and existing) must follow a standardized process to ensure that appropriate planning and execution result.

Changes will be categorized as either a Routine, Normal, or an Emergency change. It is the responsibility of the IT division manager to ensure that all areas under their direction have documented processes that meet minimum standards, are reviewed annually, and are communicated to staff.

Note: The IT Director in conjunction with the Director of the impacted department(s) are ultimately responsible for ensuring that changes are categorized appropriately and are in alignment with this policy to minimize the impact on Prescott College operations.

In Scope

- The intended scope of the Change Management Process is to cover all of Prescott College's Information Technology systems and platforms. The primary functional components covered in the Change Management process include:
- Hardware: Installation, modification, removal, or relocation of computing equipment.
- Software/Database: Installation, patching, upgrade, or removal of software products (to demonstrate non-continued-use), commercial off-the-shelf (COTS) software packages, internally developed packages, and utilities. Changes to system configuration, databases, or files such as additions, and major maintenance.
- Application: Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- Schedule Changes: Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the County's IT organization.
- Telephony: Installation, modification, de-installation, or relocation of telecom equipment and services.
- Desktop Services: Any modification or relocation of two (2) or more IT Desktop Services supported devices and services. Includes: PCs, laptop/tablets, network, or USB attached mobile devices, printers, scanners, copiers.

Out of Scope

There are many IT tasks performed, either by IT or by departmental customers that do not fall under the policies and procedures of Change Management. Tasks that require an operational process, but are outside the initial scope of the County's Change Management process include:

- Break-fix (not including programmatic changes)
- System reboots or restarting of services (notification of change is still required)
- Changes made within the daily administrative process:
  - Password resets
  - User adds/deletes
  - User modifications
  - Adding, deleting, or revising security groups
  - File permission changes
  - Routine telephone moves, adds or changes

Note: The above items shall be documented in a normal HelpDesk ticket.

MINIMUM STANDARDS

All changes must follow a process of planning, evaluation, review, approval, and documentation.

IT Director's and impacted Director's approval, or designee, prior to the execution of a significant change.

BUSINESS DAY

Monday through Friday (8:00 AM – 5:00 PM) Arizona Time

TYPES OF CHANGES

There are four types of changes based on approvals needed through the change management process. These changes regardless of type, must be documented and authorized in the Change Management system.

Routine Change - Is a relatively low-risk change with well-understood outcomes that is regularly made during the published maintenance window. A routine change follows pre-determined processes, is pre-approved by change management processes, is regularly scheduled and may be made at the discretion of the Change Authority, provided it has been defined as routine per the change management assessment process. All Routine changes typically occur within a scheduled maintenance window.

- Examples: Security/System patches, Microsoft Updates,
- Required Notification - Initial: 3 Business Days Prior to Change. Upon Completion: Immediately Required Steps:

- Use established maintenance window.
- Send notification to all IT staff and impacted departments/customers

Standard Change - A standard change is one that has medium to high risk, involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream services, any proposed standard change must be reviewed by the IT Director in collaboration with the impacted department(s) and authorized by both with appropriate notification. These notifications may be system dependent.

- Required Change Submission - Initial: Minimum 10 Business Days Prior to Change Required Steps:
  - Departmental(s) approval of proposed date/time
  - IT Director/Impacted Director(s) review and approval (< 3 business days)
  - Change notification sent (Immediately upon approval)
  - Reminder notification sent (2 business day prior to the scheduled change)
  - Change Window begins on agreed upon date.
    - Notification required upon completion
    - If Change Window has multiple completion phases, send notification upon each of the phase's completion date.

Emergency Change - An emergency change is high-risk and one that must be executed with utmost urgency. It is a system(s) that is severely degraded, non-functioning (system down) or poses a greater security threat to the County and must be addressed immediately. This type of change must still be authorized by the Change Authority and approved by the IT Director or his/her designee. Notification to impacted users is required prior to making an emergency change.

Required Change Submission - Initial: Immediate/Same Day. Upon Completion: Immediately

Required Steps:

- IT Director or designee approval
- Notification sent immediately by appropriate Gmail Group manager or IT.
- If situation persists, status notification updates should be sent out routinely or as conditions change.

Documentation Required

All changes will have the following documentation included in the Change Management Packet. The scope of this packet with grow or shrink depending upon the scope and nature of the proposed change. See Appendix – A for guidelines. In general, the scope is dependent on the number of impacted users. The more impacted the greater the scope. While the nature of the change refers to the type of system and the degree that of risk to the College. For example, any change to the financial system is significant as is any change to the student information system.

Change Management Packet:

- Date/time
- Impacted systems and software
- Impacted departmental customers and notification(s)
- Test Plan
- Contingency/Roll Back Plan
- Update related documentation (post change)
- See Appendix B for more information

APPENDIX A -CHANGE SCOPE/NATURE EVALUATION GUIDELINES

Low – For routine categories, the technical impact default is low. If the evaluation of the technical impact corresponds with the criteria below, the technical impact will be designated as “low.” The technical impact criteria include:

- Involves minimal IT resources
- One or more College departments are involved; however, there is no anticipated disruption of service(s).
- Low complexity
- No technical coordination required
- Low risk to system availability (system/service outage affecting clients during Non-Prime Time)
- Easy implementation and back-out
- No impacts to service level agreements
- Results in a smaller scope

Medium – The components of a medium impact include:

- Involves 2 or more IT resources
- Impacts 2 or more College Departments.
- Technical coordination required from one or more functional parties.
- Moderate risk to system availability (system/service outage exposure during Prime/Peak Times, outage primarily expected during Non-Prime Time)
- Some complexity to implementation and back-out plans, back-out not expected to extend the window timeframe – Affects application, data or server security

High – A impact is considered to be classified as high if the following criteria apply to the change:

- Involves most of IT’s resources.
- Will impact a majority of the College divisions.
- High complexity – complex technical coordination required with one or more functional groups.
- High risk to system availability (system/service outage expected during Prime/Peak Times)
- Complex implementation and back-out plans, back-out likely to extend the window timeframe).
- Any change that has an impact on the security of data or on the security of the IT infrastructure.
- Outside vendor support is typically required.
- Any major change to the College’s network.
- Any major change to the College’s Student Information System, Learning Management System, or Financial Systems.

APPENDIX B – CHANGE MANAGEMENT PACKET DOCUMENTATION

All Normal and Emergency changes, evaluations and approvals will be documented to allow departmental customers and IT Staff the ability to understand what was changed, the reason why it was done and the process that was used to make a change. The following details the information that will be logged for each change and where it will be logged.

All Routine, Standard, Escalated and Emergency changes are logged using the Change Management System Form. (See Appendix C)

APPENDIX C - CHANGE MANAGEMENT SYSTEM FORM

Change Ticket Number: _____________

What System / App / Device(s) or software are being changed?_________________

Type of change? ____

Who are the impacted departmental customers? ____________________________

Who is making the change? ____

When will the change be made / duration? __________________________________

Why the change was made (Reason/Comment)?______________________________

____

Test Plan and testing results (Summary): _____________________________________

____

Communication Plan (notification of internal and external customers) ______________

____

Deployment Plan, including back-out contingencies: ______________________________

____

Peer review documentation (whether a review was conducted, what was reviewed and how):

____

Indication of approval by manager or director; impacted customer(s) Updated?_______

____

Reference to the related Change Log information (who/what/when/why)____________

____

Post Change summary including successful or unsuccessful determination, related incidents, rollbacks, and business impacts.____

____