Cochise College
Administrative Policy

Category: Technology
Policy Number: 6061
Title: Change Management

This policy is established to ensure that changes at Cochise College to production information technology applications, hardware and services are introduced following a process with the following objectives:

- Manages changes in a controlled and coordinated manner
- Minimizes the risk of errors, unanticipated services outages, instability or security threats
- Reduces the impact of changes on other tasks or projects
- Promotes communication and collaboration regarding change items
- Shares knowledge with those who may be impacted by planned modifications, including user community, stakeholders and technology support resources
- Avoids critical time periods which may negatively impact a key business process, e.g. term startup, year-end accounting
- Maintains compliance with applicable regulations

Changes require serious forethought, adequate testing, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value and effectiveness of information resources.

Procedure: 6061.1
Scope

This policy, associated standards and defined processes apply to all technology-related changes that may be deployed or applied to a production environment of the college that may affect staff, students, alumni, guests, service providers or contractors. Production technology environments can include applications, network infrastructure (components, cabling and services), servers, storage, databases, and cloud, hosted or other solutions architectures.

Procedure: 6061.2
Roles and Responsibilities

Application or Systems Owners: Change Management responsibilities for Application or System Owners or managers include the following tasks:

- Review and approve timing and feasibility of Request for Change requests (RFCs)
- Review and approve RFCs when authorized by Change Authority

- Communicate changes to impacted users
- Ensure that Change Requestors fill out RFCs accurately and completely
- Ensure staff availability to successfully complete the RFC

Change Advisory Board (CAB): Responsible for providing a due diligence readiness assessment and advice about timing for any Request for Change (RFC) that is referred for review. This assessment ensures that all changes to the Technology Services environment are carefully considered to minimize the impact on campus users and existing services. CAB responsibilities include:

- Thoroughly reviewing all change requests
- Raising any potential concerns about the impact or timing of those requests
- Ensuring the changes requested
  - Have undergone proper planning and testing
  - Are planned to ensure the lowest possible risk to services
  - Are coordinated so changes do not impact each other
  - Are coordinated with the campus calendar to avoid times of high impact for affected services
- Providing advice regarding any additional measures that should be considered prior to the change
- Report annually on change management metrics, identifying patterns and making recommendations as needed
- Any decision to move forward with a RFC should include an advisory review by the CAB in advance for Normal changes and after the fact for Emergency changes

Change Authority: The Change Management responsibilities for the Change Authority include the following tasks:

- Provide advisory input to the Requestor on any needed changes to the RFC prior to approval, including any follow up communication necessary for clarification during the change process
- Review and approve RFCs when needed
- Review change outcomes and make process changes appropriate to increase service availability and service quality

Change Requesters: The Change Management responsibilities for Change Requestors include the following tasks:

- Ensure that additional resources are available in case of problems
- Prepare the request for change (RFC) and submit to the appropriate Change Authority

- Incorporate feedback from the Change Authority into the RFC
- Document the outcome of the change

Information Security Team (IST): Responsible to monitor that change control policies and procedures are followed according with this policy.

Technology Services Staff: Responsible to follow this policy and maintain a log with the change documentation.

Procedure: 6061.3
General Policy Statement

All changes to production information technology applications, hardware and services must follow a structured process to ensure appropriate planning and execution. This change management process is initiated by the creation of a Request for Change (RFC) by a Change Requester (see Procedure 6061.1 in the Procedures for Change Management document, for RFC form requirements). Depending on the potential impact and urgency of the change requested, the process for planning, review, approval, communication, implementation, and documentation may be different. The Procedures that follow provide further details on the organization, requirements and standards that have been established to support the change management process at the college.

Procedure: 6061.4
Change Advisory Board

A Change Advisory Board (CAB) or Committee shall be established by CTO to review change requests and determine whether or not they should be made. In addition, the CAB may determine that certain changes to the proposed plan for implementing the change must be made in order for it to be acceptable.

The CAB may consist of as little as one person, or it may be a group of people, depending on who should be involved in the process. In addition, the membership of the committee might be formally defined, or it might change depending on the nature of the change or the systems involved. Each department must determine the membership in consultation with application and system owners, business area managers, and data owners depending on their needs and the specific resources in question.

For change requests evaluated to be of type Normal Medium, Normal High or Emergency, representation of each core OTS department will be included as part of any formed CAB in order to ensure successful planning, review, approval, communication, implementation, and documentation of change items.

Procedure: 6061.5
Change Types

By Information Technology Infrastructure Library (ITIL) practice definition there are three types of changes:

1. **Standard Change:** A repeatable change that has been pre-authorized by the Change Authority by means of a documented procedure that controls risk and has predictable outcomes.
2. **Normal Change:** Any change that is not an Emergency Change or a Standard Change. Normal changes follow the defined steps of the change management process. The Urgency of the change, Low, Medium, or High, is determined by Application or System Owners or delegates according to the Impact Risk Assessment Matrix included below in Procedure 6061.6. Based on this matrix, the type of change and the appropriate Change Authority determined:
   - Normal Low changes must be reviewed and approved by the System or Application Owner or delegate as Change Authority.
   - Normal Medium changes must be reviewed and approved by the Change Advisory Board as Change Authority.
   - Normal High changes must additionally be reviewed and approved by the IT Leadership Team as Change Authority.
3. **Emergency Change:** A change that must be introduced as soon as possible, e.g. in response or to mitigate a potential Security Incident, system failure or other high impact issue. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps due to the urgent nature of the issue; however, any Emergency Change must still at minimum be authorized by a System or Application Owner and reviewed by the Change Advisory Board retroactively.

Procedure: 6061.6
Impact Risk Assessment Matrix

Impact	Change Type		
	Low Urgency	**Medium Urgency**	**High Urgency**
Organization Change affects more than 1,000 individuals	Normal Medium	Normal High	Emergency
College Change affects approximately 1,000 or fewer individuals	Normal Medium	Normal High	Normal High
Department Change affects approximately 100 or fewer individuals	Normal Medium	Normal Medium	Normal High
User Change affects approximately 10 or fewer individuals	Normal Low	Normal Low	Normal Medium

Table: Risk and Change Type Matrix for Normal and Emergency Changes

To use this matrix, first determine the impact of the change to the service. Next, assess the urgency of the proposed change:

- Low changes can wait until the next scheduled CAB meeting
- Medium cannot wait until the next scheduled CAB meeting
- High needs to be performed as soon as possible

Based on this, the matrix indicates whether the type of change is in turn a Normal Low, Normal Medium, Normal High, or an Emergency change. Note that a Standard change does not need to use this matrix because risk is controlled by means of following a pre-authorized procedure or process. Some examples based on this matrix include:

- A High Urgency change to a service that would impact the organization would be considered an Emergency change
- A Medium Urgency change to a service that would impact a department would be a Normal Medium change
- A Low Urgency change to a service that would impact users would be a Normal Low change

Procedure: 6061.7
Minimum Standards

All changes should follow a process of planning, testing, evaluation, review, approval, and documentation. See Procedure 6061.8 below for Change Control Process Standards. Additionally:

- Information technology applications, infrastructure components and services require maintenance windows for planned upgrades, preventative maintenance or fine-tuning.
- Only authorized staff shall perform changes, with the changes endorsed by the Application or System Owner(s)
- An assessment of the potential impact of any change shall be conducted by the Application or System Administrator
- An audit trail of all changes, configuration changes made, person who performed the change, date of the change, purpose of the change, whether the change was a success or failure and other relevant information shall be retained. See Procedure 6061.11 for Change Log requirements.
- Procedures for testing and approval of changes shall be implemented prior to promoting a change to production
- Procedures identifying responsibilities for aborting, recovering or rolling back from unsuccessful changes shall be implemented
- All potentially impacted users shall be notified regarding how these changes might affect them. If system availability will be affected while the change is being made,

affected individuals will be notified letting them know what to expect, when to expect it, and any potential workarounds, if applicable. They should also know whom to contact in case they experience difficulty as a result of the change.

- Backups will be performed as soon as possible prior to any changes
- The CAB, or an Application or System Owner, may deny a scheduled or unscheduled change for reasons including, but not limited to:
  - Inadequate planning;
  - Inadequate rollback or contingency plans;
  - Proposed change timing negatively impacting a key business process, e.g. term startup, year-end accounting, etc.; or
  - Resource availability challenges, e.g. resources may be a problem on weekends, holidays, or during special events.

Procedure: 6061.8
Change Control Process Standards

Step	Standard Change	Normal Change
Plan	• Collect information to make the change • Follow documented procedure • Identify change window	• Create RFC • Collect information to make the change • Perform testing • Review documentation • Identify maintenance window • Determine rollback contingencies
Evaluate	• Access documented procedure to ensure compatibility with the change	• Determine the risk, urgency and Normal Change type • Determine communication plan • Complete RFC
Peer Review	• Conduct internal review as needed in documented procedure	• Conduct internal or external review depending on resources or services impacted
CAB Review	• Not required	• Submit RFC to Change Authority for assessment and advice
Approval	• Pre-approved by Change Authority	• Obtain authorization from Change Authority • Obtain approval from Application or System Owner

Step	Standard Change	Normal Change
Communicate	• Send targeted email to affected customers only as needed in documented procedure	• Send targeted email to affected customers
Implement	• Perform the change	• Perform the change
Document	• Update Change Log	• Update Change Log

Table: Change Process for Standard and Normal Changes

Follow the Change Control process table steps above based on the identified Change type, Standard or Normal.

Procedure: 6061.9
Maintenance Windows

Maintenance windows will be defined by OTS to establish periods of time when maintenance, such as performing needed technology updates, e.g. patching, upgrades, etc. can be performed. At minimum, a weekly window of time outside regular business hours will be established and communicated to the user community as being set aside for conducting preventative maintenance. A regular monthly or scheduled quarterly window of longer duration will also be established for conducting larger scale changes. It should be communicated to the user community that service disruptions should be expected during these windows.

Procedure: 6061.10
Change Log

All Changes, irrespective of type, will be logged. In the case of Normal or Emergency changes, details of the Change Authority review and approval will also be documented to maintain records on what was changed, the reason it was done and the process that was used to make a change.

The following information will be included, where applicable, within the Change Log for each change performed as part of the Change Control process:

- Test Plan and testing results
- Risk assessment documentation
- Communication Plan
- Deployment Plan, including back-out contingencies
- Who made the change
- What was changed
- Why the change was made, e.g. rationale or requirement
- When the change was made

- Results of the change

Procedure: 6061.11
Compliance

This policy is a component of the Cochise College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA and other regulations.

Procedure: 6061.12
Exceptions

The Chief Technology Officer (CTO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the “Request for Policy Exception” form and a copy maintained by the CTO.

Procedure: 6061.13
Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The college reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure: 6061.14
Definitions

Change Advisory Board: A group of individuals who are responsible for the assessment, prioritization, authorization and scheduling of changes.

Change Authority: The person or group authorizing a change.

Change Control: The procedure to ensure that all changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the change.

Change Log: Auditable log of who, what, why, and when for all changes. This may be system specific as certain systems have the ability to automatically log changes in this manner.

Change Management: The process of requesting, developing, approving and implementing a planned or unplanned change within the information technology infrastructure.

ITIL: Formally an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management (ITSM) that focuses on aligning Technology Service with the needs of business.

Production Environment: The information technology infrastructure or service where the real-time staging of programs that run an organization are executed, and includes the personnel, processes, data, hardware and software needed to perform day-to-day operations.

Request for Change (RFC): A form used to record details of a request for a change and is sent as an input to Change Management by the Change Requestor.

Security Incident: Any event that threatens the confidentiality, integrity, or availability of college systems, applications, data or networks.

User: Any college faculty, staff, student or partner who has been authorized to access any college electronic information resource.