Purpose

This document establishes the standard for Information Technology (IT) change management across the Arizona State University (ASU) IT environment.

The goal of the Enterprise System Change Management standard is to establish uniform guidance and prescribe a framework for managing change within the ASU IT environment. Change Management refers to the formal process for making changes to IT resources that directly support an ASU Business Service. The goal of Change Management is to increase awareness and understanding of proposed changes to IT Applications and Infrastructure and ensure that those changes are made in a thoughtful manner that minimizes impact to Services. Specifically, this standard:

- Establishes the requirement for a formal ASU Change Process
- Establishes a framework for evaluating, reviewing, approving, scheduling, communicating, implementing and documenting changes to ASU's technology systems
- Governs the management of IT baseline configurations and changes for all University Technology Office (UTO)-operated and managed devices including those managed for UTO by 3rd party vendors
- Ensures all changes have been properly assessed for their potential impacts to the ASU IT environment and ASU services
- Applies a risk/impact-based approval process to all changes prior to their implementation
- Clarifies specific roles, responsibilities and timelines for Information Security Office (ISO) change management

Applicability

This standard applies to all Users of ASU's computing, internet, and communications resources, including all, faculty, staff (including student employees), contractors, vendors, consultants, temporary and other workers for ASU and its Component Units (Users) that operate or manage the configuration of UTO technology resources, including hardware, software, applications, and network resources that support an ASU Service in the production environment. Changes made to non-production UTO managed resources such as systems/applications not yet in production or Development/QA environments are outside the scope of this standard.

Standard

Types of Changes

Changes to ASU technology systems are classified into four types based on the magnitude of risk and impact that they present to system operation – Standard, Normal, Urgent or Emergency. The Change Type, (along with its associated risk) dictates the timeline for the change, required approvals, requirements, and level of scrutiny that will be given to a specific Change Request.

Standard Change

Standard changes are conducted as a matter of course, are repetitive in nature, and have a low likelihood of disrupting operations or significantly impacting the user experience. A Standard Change is, effectively, a pre-approved change that is low risk, relatively common and follows a documented procedure or work instructions. Examples of Standard Changes include Web application migrations, periodic updates to security device resource files, and other regularly occurring maintenance changes required to manage and maintain applications and devices. Due to the nature of Standard Changes, Planning details (Change Plan, Backout Plan, and Test Plan) are not required in the Change ticket.

Any request to have a given Change designated as Standard must be presented to the Change Advisory Board (CAB) who will review the request against above mentioned characteristics. Only the CAB can grant this status.

Normal Change

Normal Changes pose a medium to high risk and/or impact to an ASU service supported by the UTO. Normal changes may involve less understood risks or impacts or may be a change that is not regularly made during the normal course of business. They may be more extensive in scope than Standard changes or affect critical systems in new ways. Such changes require a greater level of oversight and as such must be subject to a greater level of communication and discussion. Normal changes must be approved by the CAB on a case-by case basis via the normal change management process. Due to the nature of Normal Changes, they require extra scrutiny. All Normal Changes must include planning details (Change Plan, Backout Plan, and Test Plan) in the Planning tab on the Change ticket.

Urgent Change

Urgent Changes are Changes that are submitted for approval after the weekly CAB meeting and are not an immediate emergency, but cannot wait until the next CAB meeting.

- An example of this might be an application running on a server that is low on memory and generating messages. The server, hosting a business application, needs to be re-booted/cycled as soon as possible to recapture memory (or install more memory), during non-business hours for the application, to avoid an outage during business hours.
- Urgent changes require eCAB approval. The eCAB consists of 3 CAB members that can quickly assess the situation and apply eCAB approval any time. Two of the three eCAB members must supply their approval before the Change can occur at the Planned Start time.

Emergency Change

Emergency Changes occur in response to unforeseen conditions and must be attended to immediately, often without broad consultation, due to the urgency of the situation. Nevertheless, such changes must be accurately recorded so that their impact can be properly assessed in hindsight. Emergency changes generally occur as a result of three different situations:

- An unexpected service outage that cannot wait for full CAB approval to take the necessary steps to bring the service back on line. In these cases, the primary objective is to get the service on line as quickly as possible. In these cases, authorized staff who have been predesignated by the CAB may begin work on the change immediately but must obtain approval within 1 business day for any changes required.
- Actions taken to protect the ASU environment as a direct response to remediate an imminent cyber threat, such as an ongoing Distributed Denial of Service (DDoS) attack or malware outbreak that can affect the availability of critical ASU services and resources. In these cases, authorized staff who have been pre-designated by the CAB may begin work on the change immediately but must obtain approval within 1 business day for any changes required.
- Other changes which must be enacted promptly and cannot wait for the next scheduled CAB meeting. Examples may include actions that must be taken to resolve poor systems response times that are materially affecting the quality of service and may require a brief service outage to implement the remediation measures. In these cases, Emergency CAB (ECAB) approval must be granted before work can begin.

The CAB will designate a small group of UTO staff members who can immediately authorize the implementation of emergency changes as part of ongoing service restoration, break/fix or security incident response activities. For Emergency Changes, the requestor and the implementer may be

the same individual. An Emergency Change ticket will be created after the impacted service has been restored as the primary objective is to restore service as quickly as possible. All Emergency Changes must be presented to the ECAB within 1 business day for review and approval.

Security (Firewall) Change

A unique category of change requiring special handling is a Security Change, which most often involves changes to enterprise firewalls, including border firewalls that form the core of ASU's protection against external threats. Security changes can be any type of change (e.g., Normal, Routine or Emergency) that involve a security device requiring additional scrutiny and approval.

In addition to the normal CAB approvals, Security Changes must also be approved by ASU's Chief Information Security Officer (CISO) or designee prior to implementation.

Change Windows

In order to maintain maximum availability of all Services, the ASU Enterprise System Change Management Process will specify Maintenance Windows and Maintenance Blackout Periods. Approved changes will be implemented only during specified Maintenance Windows. These Maintenance Windows ensure that Service impacting changes don't occur during critical ASU business hours.

As an exception, emergency changes may be implemented by CAB-designated personnel as part of a break/fix, outage restoration or security remediation solution outside specified Maintenance Windows, but extreme caution should be used.

Changes will not be implemented during a Maintenance Blackout Period (such as Semester Startup). Exceptions can be granted only with the approval of the Executive Director of Service Operations. If the Executive Director of Service Operations is unavailable, he/she can designate an alternate approver. In all cases, a business justification will be required for any Change to occur during a maintenance blackout period.

In cases where a documented SLA exists between an ASU business unit / department and the UTO which outlines a specific maintenance window for a specified application or service, those changes will occur within that documented maintenance window. Since these are for a specific service or application, any impacts would not be university-wide.

Change Management Process

All changes, unless excluded for a specific Change type, will be implemented using a structured process to avoid unintended consequences. At a minimum, the process will address:

- Planning and testing the details of the change, including roll-back procedures (Links to documents with appropriate detail are acceptable)
- Creating and assigning the change request, including all pertinent information
- Assessing the potential risk exposure
- Obtaining authorization and approvals from technical staff and the CAB
- Scheduling the change in the approved change window, taking into account potential adverse impacts and ongoing activities
- Deploying the change
- Monitoring the progress of the change to look for any signs of adverse impacts
- Verifying the change is completed
- Updating the configuration baseline

Change Advisory Board (CAB)

The ASU Change Advisory Board will serve as the centralized approval authority for all changes, using a risk-based approach to analyze proposed changes as an integral part of ASU's Enterprise System Change Management Process.

To the greatest extent possible, the CAB will automate the change management process within ASU's designated service ticketing system.

Initiation / Recording

Proper recording of changes is essential. Changes will be submitted electronically via ASU's Change Management system (ServiceNow) by the Requestor.

Configuration Management

The Change Management Process will ensure the appropriate configuration records for the systems and/or services affected by the Request for Change (RFC) are updated. This includes the identification of all relevant stakeholders, who will be given the opportunity to assess the RFC. Configuration data will also be updated following the implementation of all RFCs.

Authorization

RFCs will be reviewed by the CAB during periodic meetings or by special arrangement if the RFC is designated urgent. These reviews will balance the expected benefits of implementation with the business and technical risks identified, the urgency of the change and the predicted impact on clients or university operations.

No unauthorized RFCs will be implemented. The decisions of the CAB can be appealed to the ASU CIO or designee.

Scheduling

Proper scheduling is important to ensure change implementations do not conflict and cause undue impact on the university operations.

The Change Calendar will be published at a secure site accessible to appropriate ASU personnel and will serve as the definitive source of change schedule information.

Scheduling will be the joint responsibility of the Initiator, the Service Owner and the Change Manager.

Implementation

From a change management point of view, the implementation of the change should follow the plans provided as part of the RFC.

Success or failure of the implementation must be promptly reported per the approved Enterprise System Change Management Process.

The Initiator has responsibility for ensuring the implementation follows the approved plan and that back out plans are implemented if required.

Review

All Changes that fall into the following categories will be reviewed:

- Failed changes
- Changes that exceeded the specified outage window

- Emergency or urgent changes
- Changes causing unexpected or unreasonable incident volumes

Changes falling into these categories will be passed to the Change Manager, who will ensure appropriate investigations take place and facilitate discussion to ensure any improvements to the process or to the implementation can be identified and actions are taken towards resolution.

CAB members will be responsible for appropriate review of changes and identification of improvements or additional safeguards to ensure future successful change implementation.

Change Process Metrics

The ASU Change Management Process will include requirements for associated metrics that allow the process quality to be monitored and improvements to be identified.

CAB Meetings

The CAB will meet weekly, and on an ad-hoc basis as needed, to perform authorization and review of pending RFCs or as needed to ensure timely response to urgent issues.

The CAB meeting time and location will be published at a secure site accessible to appropriate ASU personnel.

Weekly CAB Meetings

The weekly CAB meeting will be chaired by either the Change Manager or a CAB member and will follow a standard agenda as prescribed by the ASU Enterprise System Change Management Process.

Ad-Hoc Meetings

An ad-hoc CAB meeting may be called when required for urgent changes. This may be conducted via email or Slack if required.

Quorum

For IT infrastructure changes, a quorum of the CAB must be present in order to authorize any RFC. In the absence of a quorum, all changes may be deferred or referred to the ASU CIO or designee.

Change Requestor

The change requester should attend the CAB meeting (either virtually or physically) in order for that sponsor's change to be considered/approved. If the CAB has questions or requires further information concerning the change and the Change Sponsor is not available to assist the CAB, then the change may not be approved.

Authorization

RFC authorization will require consensus of the CAB members. If consensus cannot be reached, the RFC is sent back to the Requester for further clarification. If the CAB is still unable to reach a consensus regarding the approval of a proposed change, an RFC may be referred to the University Technology Officer or designee for a final decision.

CAB Notification and Review

As part of the ASU Change Management process, the CAB will ensure that the proper notification procedures for each class of Change are followed. The CAB will monitor comments, responses, and reviews of proposed High Impact Changes to ensure that the proposed Change can accommodate the expressed concerns of ASU faculty or staff leadership.

Security (e.g., Firewall) Changes

Because of the potential for widespread impacts resulting from a security change, especially with enterprise firewalls, including border firewalls which form the core of ASU's protection against external threats, ASU's Change Management Process will incorporate extra precautions for all Security Changes:

- An additional level of approval by CISO or designee will be required for all Security Changes
- Additional change implementation monitoring will be enacted to enable ASU to immediately detect and react to any unforeseen issues associated with Security Changes
- A rule tracking mechanism that provides for change logging will be used in order to audit all modifications to enterprise firewalls. The audit logs will be stored securely with access limited to authorized individuals only.

Violations and Enforcement

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU's computing, Internet and communication resources, until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

In a circumstance where compliance may not be immediately possible, the ASU academic or business units must confer with the Information Security Office to develop a plan for moving into compliance within a reasonable amount of time.

Resources

ASU Enterprise System Change Management Process

Standard Revision

This standard is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at infosec@asu.edu.