ENTERPRISE SYSTEM CHANGE MANAGEMENT

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or the *Data Classification and Handling* policy. Questions regarding these *Information Security Standards* should be directed to Information Security Services.

This Information Security Standard establishes minimum requirements for the administration and management of changes to the University's IT Resource production environment. The goals are to improve University IT production system and application reliability and performance, reduce the negative impact of enterprise system changes on dependent systems (such as disruptions or outages that could lead to production system unavailability), and maintain legal and regulatory compliance.

1. **Change Manager.** The Change Manager facilitates the enterprise system change management process and chairs the Change Advisory Board. The Change Manager shall have ultimate authority in change management decision-making and shall be responsible for ensuring that the change process is managed efficiently, effectively, and consistently.

2. **Change Advisory Board**. Under the leadership of the Change Manager, the Change Advisory Board ("CAB") will serve as the University's central review and evaluation authority. Comprised of representatives from participating central IT divisions, the CAB will meet weekly. Each participating Information Technology Services division will be represented. The standard CAB meeting agenda will include the following three fundamental topics:

    a. Reviewing proposed changes that have been determined to be moderate or high risk.

    b. Reviewing proposed "Standard" change templates (see below for more detail) as candidates for reduced controls.

    c. Post-implementation review of any failed changes, changes that succeeded with issues, or emergency changes to determine root cause and lessons learned.

3. **Change Types.** Changes to University IT Resources shall be classified as one of four types based on the criticality, urgency, and expected impact:

    a. **"Normal,**" which means one-time, non-trivial, changes to a service, configuration item, or service component and/or associated elements. The risk of a Normal change determines the level of the approvals it must receive before being authorized for production.
        i. **"Low Risk"** changes must be assessed and approved by the change owner's supervisor. No other approvals are required in order for the change to be authorized for production.
        ii. **"Moderate Risk"** or **"High Risk"** changes must be assessed and approved by the change owner's supervisor, and then be reviewed and authorized for production by the CAB.

    b. **"Emergency,**" which means changes required to immediately restore services, avoid critical outages, or address a critical security risk when no other workaround or mitigation is available. To this end, Director-level approval of Emergency changes is required, but may occur before the details of the change are recorded in a change request form. Emergency changes should be recorded in a change

request, but this record may be created after the change has been implemented. Each Emergency change request record is reviewed by the Director of its assignment group and the CAB.

c. **"Standard**," which means a low-risk, low-impact change that follows a standardized or operationalized procedure or work instruction, maintains change tracking in a standard repository, and is implemented with some frequency. Risk is reduced as a result of a set of approved standardized implementation tasks. Because the risk and impact are low, and the changes follow a standardized/operationalized procedure. Standard changes are first proposed as a "template". A Standard template must be reviewed by the CAB before it can be used. If the CAB approves a Standard template, users can then generate change requests from that template, as long as the changes they are planning follow the procedure and have the same risk and impact as that described in the template. Changes created from an approved template inherit the approvals of that template, and therefore can be scheduled for production without another review by a supervisor or the CAB. Any modifications to an approved template must be reviewed and approved by the CAB. The change owner regularly reviews Standard changes and can revoke the approvals of templates if the changes spawned from them have been frequently unsuccessful or caused an unreasonable number of incidents.

d. "**Expedited,**" **which means** changes that are of an urgent nature and support pressing needs that cannot wait for the full CAB approval process, but are not required to address a critical outage or security risk. Risk is assumed by the Change Approver (who is the Information Technology Services Director who oversees the group to which the change request has been assigned).

4. **Change Request Submittals**. Change requests shall be submitted via ServiceNow by either a requester, the change owner, or, in some rare situations, a third party such as the change manager. All requests are submitted on behalf of the change owner, who is ultimately responsible for the change request itself. All sections of the written change request must be completed in a thorough manner. The change request must identify the Product and Service that will be changed; a "change owner" who will be responsible for the request; the group responsible for the change; risks and impacts; justification; testing, implementation, and remediation/backout plans; and the planned date of deployment.

5. **Change Request Review**. New change requests shall be reviewed using a risk-based approach. As described above, the "type" of the change item determines the nature of approvals it must receive. For changes that require CAB review, the Change Manager and the CAB shall jointly evaluate each pending item to ensure a full understanding of the change and its dependencies. Requests that are understood and agreed to by all shall be motioned for approval. If a request is incomplete or if CAB members have questions or concerns, every effort shall be made to complete the request and address the questions during the CAB meeting. For this reason, the Change Owner is required to be present or identify a delegate to be present at the CAB meeting where their request is reviewed. If the concerns cannot be adressed during the meeting, the request is returned to the change owner for further elaboration.

6. **Change Request Scheduling**. In order to maintain availability of all services, the Change Manager will specify approved change windows and caution periods. The Change Manager will maintain calendars to reflect caution periods, primary change windows, and scheduled/approved changes. Scheduling of approved change requests will occur during the weekly Change Advisory Board meeting. Exceptions may be approved based on specific business or other relevant drivers.

7. **Change Request Evaluation and Closure**. Change items previously approved and subsequently deployed shall include records of their success or failure. A change owner must include these records in every change request. If an incident occurs because of a change, this will be noted in the change request and any related incident records. The Change Manager will regularly review closed change requests and modify processes and procedures with the goal of increasing the proportion of successful changes and minimizing the amount and severity of incidents caused by changes. The Change Manager will also search for any changes that were implemented without appropriate review and approvals, determine why the required processes were not followed, and modify change management practices in order to maximize adoption/compliance.

8. **Documentation**. All change requests and the resulting approvals, reviews, closures, and related decisions shall be fully documented, stored, and processed in a change management application approved by the Chief Information Officer (at present the ServiceNow Change Management system). Change request

records will specify the Product and Service that will be changed; the person and group responsible for the change; overall risk and impact of making the change; justification for the change; implementation, testing, and remediation plans; and schedule. All approvals, denials, and completion notes will be incorporated into the change record prior to closing the request.