Contents

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

Purpose and Scope

This policy outlines how Alvernia University ("AU") controls the configuration of its network, systems, and applications. It applies to all AU managed infrastructure, but excludes systems provided to AU as a service and hosted by the vendor, rather than on AU's network.

Responsibilities

Title or Role	What They are Responsible For
Chief Information Officer	Maintains and Enforces this policy.
IT Team Members	Responsible for implementing this policy.

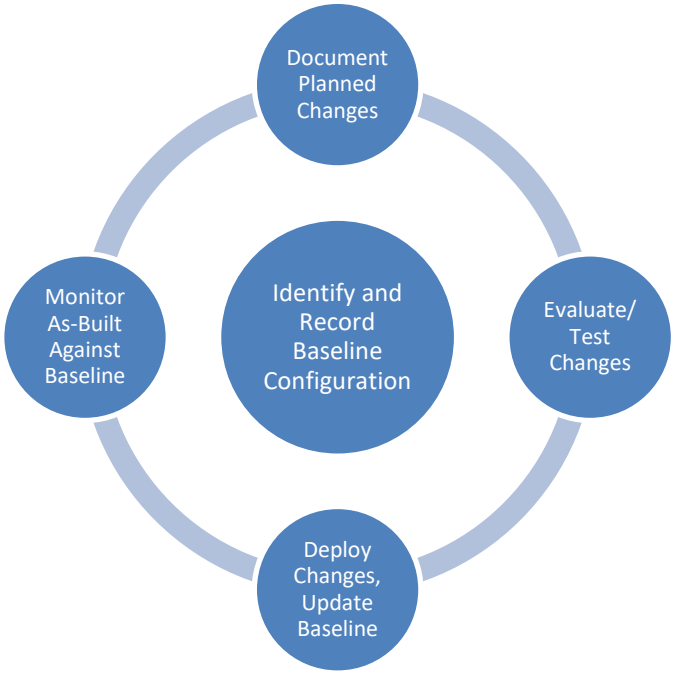
Policy

This policy defines how AU defines and maintains a controlled information technology environment, including how changes to network components, servers and applications are evaluated, tested, and deployed to the production environment, and how AU protects itself from unplanned changes to that environment. Configuration Management is a key part of managing the overall risk to the AU organization.

Below are a few key terms:

- *Configuration Management* (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.
- A *Configuration Item* (CI) is an identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.
- A *Baseline Configuration* is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
- *Configuration Change Control* – process for managing updates to the baseline configurations for the configuration items.
- *Configuration Monitoring* – process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.

The diagram below shows the key elements of the configuration management process. These same steps apply to management of the overall environment, and to individual Configuration Items.



Having a known baseline configuration allows more rapid detection of system compromise, and speeds restoration to a known state in the event of either a security event or a system failure.

The rest of this policy defines expectations for each phase of this process.

Identify and Record Baseline Configuration

There are two key elements to this:

1) Maintaining a configuration database that is an inventory of all hardware components, the software running on them, and their configuration.
2) Defining standardized configurations and images for servers, workstations, and network components that are used as the starting point when building out new systems. When possible, National Institute of Standards and Technology (NIST) hardening guidelines should be followed when creating standardized configurations and images.

This excludes equipment attached to the public wireless network, and equipment brought in by event coordinators and attached to the event network.

AU will maintain a consolidated inventory of all AU owned hardware and the software running on them, leveraging software tools as they are available. This inventory will include all systems either on the AU network or at AU data centers and will also include software as a service (SaaS) systems that are integrated with AU systems. For SaaS systems, the focus will be on the system business purpose its integrations. Details of the SaaS application infrastructure are not required. IT must be involved in the selection, acquisition, and integration of SaaS applications, including any significant changes to the integration, as with any other system change.

AU will define secure baseline configurations for each system type (workstations, network devices, servers, etc.). These baseline configurations, where possible, will be captured as images and will be used as the starting point when building out new components.

Document Planned Changes

9.3400, Change Management Procedure, addresses the process for documenting and approving planned changes. All planned changes must be reviewed and approved prior to execution. Some examples of changes include:

1) Adding new hardware or hardware components to the AU environment
2) Removing hardware from the environment
3) Installing new software
4) Removing software
5) Software or firmware upgrades
6) Patching
7) Network Configuration changes (outside of routine changes required for supporting day-to-day operations). This includes any wireless configuration changes.
8) Other configuration changes (scheduling new automated tasks, changing firewall, router or switch configurations, etc.).

Normal infrastructure updates done in the normal course of business are not considered changes. Examples would include enabling/disabling user accounts. However, changes that affect the infrastructure's configuration or structure (new devices, enabling or disabling services, or changes to firewall or routing rules that affect the function of the infrastructure) are included.

Evaluating and Testing Changes

Each change must be evaluated based on:

a) The risk of disrupting business operations.
b) The potential impact on the security of the AU network and systems.
c) Consultation with Subject Matter Experts (SMEs).
d) The business need for the change.
e) Awareness of the change within the parts of the business affected by it.

The requester and reviewer(s) must address these two key issues. Whenever possible, the change should first be tested in an environment that minimizes the risk of disrupting business operations. This could be a non-production environment or it can be a system that is less mission-critical. Details of the testing performed should be documented as part of the change control, including who did the testing and where it was performed. Once the change has been evaluated and tested, if possible, the reviewer can approve the change for deployment to production.

Deploy Changes, Update Baseline

Once the change has been reviewed, evaluated, tested, and approved, it can be deployed to production in accordance with the timeline outlined in the change control. It is the responsibility of the individual deploying the change to update the configuration database to reflect the change(s) made, and if applicable, to also update baseline configurations and images to reflect the change. The change control shall be updated with the following:

1) Time the change was made
2) Any issues encountered during the deployment
3) Confirmation that the configuration database and baseline configuration were updated.

If there are unanticipated side effects caused by the change (e.g. a disruption in IT services or business operations), the change should be rolled back and the change control updated, including with any follow-on investigation and resolution of the issue. If the issue is subsequently resolved, the old change control should be closed, and a new change control should be created that refers to the old change control to implement the subsequent change. This will ensure that a clear audit trail exists of all changes, including those that are subsequently rolled back.

Monitor As-Built Against Baseline

At least annually, but also as required, the IT team will do a self-audit of the as-built configurations of all servers and network components against the configuration database and investigate and resolve any discrepancies. This monitoring can be accomplished either manually or using software tools specifically for this purpose.

Firewall and router rule sets must be reviewed every 6 months. A procedure must be put in place documenting these reviews.

Note: This addresses PCI requirement 1.1.7.

File Integrity software must be used to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files. The software shall perform critical file comparisons at least weekly.

Critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the IT team.

Note: This addresses PCI requirement 11.5.

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems
2. Payment Card Industry (PCI) Data Security Standard, v3.2

Exhibits

No Exhibits for this policy.