**Version 1.0**

**Version Date: 05/08/2023**

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

# Configuration Management Policy

# Contents

## Document

| | |
|---|---|
| **Document** | **Configuration Management** |
| **References** | **NIST 800-171 Rev2 / CMMC Rev2 Level II** |
| **Control** | **3.4 CONFIGURATION MANAGEMENT** |
| **Last Approved** | |
| **Next Review** | |

## Annual Review and Revision Tracking

| Date | Summary of Changes Made | Changes Made By (Name/title) | Version History |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## Overview

Configuration management is one of the most important practices within information security due to the fact that critical system resources must be securely configured for ensuring their confidentiality, integrity, and availability – which is the widely-known information security CIA triad. But configuration management is a broad-based concept, one that's used in a wide variety of industries and business sectors, ranging from manufacturing to technology – just to name a few. For purposes of information security – however – configuration management is viewed as the following:

*Implementing, establishing, maintaining, recording, and effectively monitoring secure configurations to an organization's overall information system's landscape, including, but not limited to the following system resources: network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms.*

Simply stated, it's about applying baseline security standards for ensuring the confidentiality, integrity, and availability (CIA) of critical system resources, and continuously monitoring and updating these systems as necessary.

Information security configuration management is an important principle – no question about it – one that requires thoughtful attention when designing and implementing such a program, along with all supporting policies and procedures. Though there are a number of helpful software tools and other utilities that effectively administer many functions relating to information security configuration management – they are just that, software – thus still requiring a well-developed, formalized, and comprehensive information security configuration management plan.

In accordance with mandated University security requirements set forth and approved by the Board, has established a formal Configuration Management (CM) policy. This policy is to be implemented immediately. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding ASU's needs and goals.

## Purpose

This policy is designed to provide ASU with a documented and formalized Configuration Management (CM) policy that is to be adhered to and utilized throughout the University at all times. Compliance with the stated policy will ensure the safety and security of ASU information systems.

## Scope

This policy and supporting procedures encompasses all information systems that are owned, operated, maintained, and controlled by ASU and all other information systems, both internally and externally, that interact with these systems.

- Internal information systems are those owned, operated, maintained, and controlled by ASU and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other information systems deemed in scope.

- External information systems are those owned, operated, maintained, and controlled by any entity other than ASU, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal information systems".

  **Note:** While ASU does not have the ability to actually provision, harden, secure, and deploy another organization's information systems, ASU will follow due-diligence and best practices by obtaining all relevant information ensuring that such systems are safe and secure.

## Roles and Responsibilities

Implementing and adhering to the University's policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, students, and users of information systems, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to ASU information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- **Management Commitment:** Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Vice President of Technology Services is to report to other members of Board on a regular basis regarding all aspects of the University's information systems posture.

- **Personnel:** Responsibilities include adhering to the University's information security policies, procedures, practices, and not undertaking any measures to alter such standards on any ASU information systems. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of ASU information systems and are to also report such instance immediately to senior authorities.

## Policy

ASU is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated University security requirements set forth and approved by the board. ASU shall:

- Establish and maintain baseline configurations and inventories of university's systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products deployed in university's systems.
- Track, review, approve/disapprove, and audit changes to university's systems.
- Analyze the security impact of changes prior to implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to university's systems.
- Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
- Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Control and monitor user-installed software.

## Compliance Mapping Matrix

The following Matrix is to be completed for purposes of cross-referencing and effectively mapping the basic and derived security requirements with existing information security policies and procedures for ASU.

| Basic and Derived Security Requirements | Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation | Notes and Comments |
|---|---|---|
| **NIST SP 800-171 Rev 2 3.4.2** | **Security Configuration Enforcement** | |
| **NIST SP 800-171 Rev 2 3.4.3** | **System Change Management** | |
| **NIST SP 800-171 Rev 2 3.4.4** | **Security Impact Analysis** | |
| **NIST SP 800-171 Rev 2 3.4.5** | **Access Restrictions for Change** | |
| **NIST SP 800-171 Rev 2 3.4.6** | **Least Functionality** | |
| **NIST SP 800-171 Rev 2 3.4.7** | **Nonessential Functionality** | |
| **NIST SP 800-171 Rev 2 3.4.8** | **Application Execution Policy** | |
| **NIST SP 800-171 Rev 2 3.4.9** | **User-Installed Software** | |

## References

| Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation | Notes and Comments |
|---|---|
| | |
| | |
| | |

## Responsibility for Policy and Procedures Maintenance

ASU is responsible for ensuring that the aforementioned policy initiatives, and if applicable – the relevant procedures – are kept current as needed for purposes of compliance with mandated University security requirements set forth and approved by the Board.

## Definitions

**Personnel –** All community users of all information systems that are the property of ASU. Specifically, it includes:

- All faculty, staff and student workers, whether employed on a full-time or part-time basis by ASU.
- All contractors and third parties that work on behalf of and are paid directly by ASU.
- All contractors and third parties that work on behalf of ASU but are paid directly by an alternate employer.
- All employees of partners and clients of ASU that access ASU's non-public information systems.
- All volunteers and alumni that serve on behalf of ASU.
- All students attending ASU.

## Violation of Policy

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

1. First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the ASU Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
2. Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the ASU Personnel Handbook.
3. In the case of a student, the breach will also be remanded to the Dean of Students.

## Disclosure

ASU reserves the right to change and modify the aforementioned document at any time and to provide notice to all users in a reasonable and acceptable timeframe and format.

_____ _____

Signature Date
Name
Title