Version 1.0

Version Date: 05/08/2023

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Maintenance Policy

Contents

Document

Document	Maintenance
References	NIST 800-171 Rev2 / CMMC Rev2 Level II
Control	3.7 MAINTENANCE
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

Overview

System maintenance is a critical element of any university's overall information systems security framework as the ability to update, enhance, configure, and repair systems as necessary helps for ensuring their safety and security. Additionally, from an information security perspective, system maintenance should include, at a minimum, the following provisions regarding maintenance: (1). Preventative Maintenance. (2). Scheduled Maintenance. (3). Corrective Maintenance.

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Maintenance (MA) 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 Maintenance (MA) 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

3

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 community 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:

- Perform regularly scheduled maintenance on University's systems.
- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- Ensure equipment removed for off-site maintenance is sanitized of any Confidential Uncontrolled Information (CUI).
- Check media containing diagnostic and test programs for malicious code before the media are used in university's systems.
- Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- Supervise the maintenance activities of maintenance personnel without required access authorization.

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 Rev2 3.7.2	System Maintenance Control	
NIST SP 800-171 Rev2 3.7.3	Equipment Sanitization	
NIST SP 800-171 Rev2 3.7.4	Media Inspection	
NIST SP 800-171 Rev2 3.7.5	Nonlocal Maintenance	
NIST SP 800-171 Rev2 3.7.6	Maintenance Personnel	

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