Version 1.0

Version Date: 05/08/2023

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

System and Communication Protection Policy

Contents

Document

Document	System and Communications Protection
References	NIST 800-171 Rev2 / CMMC Rev2 Level II
Control	3.13 SYSTEM AND COMMUNICATIONS PROTECTION
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

Overview

The protection of information systems and the data being stored and transmitted over such systems requires Alabama State University Office of Technology Services (ASU OTS) to implement numerous communications protection initiatives for helping ensure the confidentiality, integrity, and availability of the network. Specifically, having in place documented information security practices relating to security function isolation, denial of service protection, boundary protection, and the confidentiality and integrity of data transmissions are excellent examples of communications protection controls.

In accordance with mandated University security requirements set forth and approved by the Board, ASU OTS has established a formal System and Communications Protection (SC) 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 System and Communication (SC) policy that is to be adhered to and utilized throughout the University at all time. 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 OTS 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 OTS 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 OTS, 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 instances 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 OTS shall:

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by University's systems) at the external boundaries and key internal boundaries of University's systems.
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within University's systems.
- Separate user functionality from system management functionality.
- Prevent unauthorized and unintended information transfer via shared system resources.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- Prevent remote devices from simultaneously establishing non-remote connections with the University's systems and communicating via some other connection to resources in external networks.
- Implement cryptographic mechanisms to prevent unauthorized disclosure of Controlled Unclassified Information (CUI) during transmission unless otherwise protected by alternative physical safeguards.
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- Establish and manage cryptographic keys for cryptography employed in the University's information system.
- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
- Control and monitor the use of mobile code.
- Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
- Protect the authenticity of communications sessions.
- Protect the confidentiality of CUI at rest.

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 3.13.3	Role Separation	
NIST SP 800-171 Rev2 3.13.4	Shared Resource Control	
NIST SP 800-171 Rev2 3.13.5	Public-Access System Separation	
NIST SP 800-171 Rev2 3.13.6	Network Communication by Exception	
NIST SP 800-171 Rev2 3.13.7	Split Tunneling	
NIST SP 800-171 Rev2 3.13.8	Data in Transit	
NIST SP 800-171 Rev2 3.13.9	Connections Termination	
NIST SP 800-171 Rev2 3.13.10	Key Management	
NIST SP 800-171 Rev2 3.13.11	CUI Encryption	
NIST SP 800-171 Rev2 3.13.12	Collaborative Device Control	
NIST SP 800-171 Rev2 3.13.13	Mobile Code	
NIST SP 800-171 Rev2 3.13.14	Voice over Internet Protocol	
NIST SP 800-171 Rev2 3.13.15	Communications Authenticity	

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 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.

Cryptography – process of hiding or coding information so that only the person a message was intended for can read the message.

Cryptography keys – a string of characters used within an encryption algorithm for altering data so that it appears random.

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