Version 1.0

Version Date: 05/08/2023

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Identification And Authentication Policy

Contents

Document

Document	**Identification and Authentication**
References	**NIST 800-171 Rev2 / CMMC Rev2 Level II**
Control	**Identification And Authentication (IA-1)**
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

Overview

The concepts of Identification, Authentication, Authorization, and Accounting (i.e., audit) are generally known as IAAA or simply AAA. In short, one assigns users an appropriate and acceptable "identification" phrase, which is generally a username. Users will use their respective username with a password, passphrase or some other type of commonly used method of "authentication" to actually authenticate to that very system resource.

The three (3) factors are generally seen as the following: (1). something you know. (2). something you have. (3). something you are. Once users have properly identified and authenticated themselves, they then are "authorized" to perform certain functions within those information systems based on the access rights afforded to them. And finally, the concept of "accounting" (i.e., effectively auditing and monitoring this type of environment) includes removing aged and dormant accounts, validating access rights for privileged accounts, reviewing log reports for access rights violations, and other essential activities. Lastly, a wide variety of tools along with traditional methods are successfully used for ensuring these measures are being initiated.

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Identification and Authentication (IA) 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 Identification and Authentication (IA) 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 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:

- Identify system users, processes acting on behalf of users, and devices.

- Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to University's systems.
- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- Prevent the reuse of identifiers for a defined period and disable after the defined period.
- Enforce a minimum password complexity and change of characters when new passwords are created.
- Prohibit password reuse for a specified number of generations.
- Allow temporary password use for system logons with an immediate change to a permanent password.
- Store and transmit only cryptographically protected passwords.
- Obscure feedback of authentication information.

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 3.5.4	**Replay-Resistant Authentication**	
NIST SP 800-171 Rev2 3.5.5	**Identifier Reuse**	
NIST SP 800-171 Rev2 3.5.6	**Identifier Handling**	
NIST SP 800-171 Rev2 3.5.7	**Password Complexity**	
NIST SP 800-171 Rev2 3.5.8	**Password Reuse**	
NIST SP 800-171 Rev2 3.5.9	**Temporary Passwords**	
NIST SP 800-171 Rev2 3.5.10	**Cryptographically-Protected Passwords**	
NIST SP 800-171 Rev2 3.5.11	**Obscure Feedback**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Access Control	
Personnel Security	

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