Version 1.0

Version Date: 05/08/2023

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Access Control Policy

Contents

Document

Document	**Access Control**
References	**NIST 800-171 Rev2 / CMMC Rev2 Level II**
Control	**3.1 ACCESS CONTROL**
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

Overview

A critical component of any successful institution is the ability to properly provision, manage, monitor, and off-board | de-provision all users that have been granted access rights to company-wide information systems – a concept universally known as access rights and/or access control. The phrase "information systems" includes any type of component, application, data source, or any other type of business resource identified by a company for which users have the ability to access through a process generally known as authentication and authorization.

The growing surge of regulatory compliance requirements along with the need for incorporating a secure and stable platform regarding access control has propelled institutions to revisit and rethink their entire provisioning, management, and off-boarding | de-provisioning lifecycle for all applicable users. The result has been to incorporate best practices within an access control policy and procedures document which generally include the following activities:

Identification, Authentication, Authorization, and Accounting (AAA)

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 thus 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 "accountability" (i.e., effectively auditing and monitoring this type of information system) 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.

Additional activities encompassed within the AAA framework include the following:

Establishing Access Rights

Known collectively as many concepts, such as that of "least privilege", "least access", "need to know" access, or Role Based Access Control (RBAC), the University have incorporated frameworks regarding access rights for which permissions to perform certain operations are assigned to specific roles, resulting in users acquiring the permissions to perform particular functions on information systems within the institution. Therefore, privileges to these very information systems are never to be assigned based on a specific employee's demands, requests, or preferences. Additionally, Mandatory Access Control (MAC) is also another concept for access control which are generally used for very secure environments whereby users can only access system resource equal to or below their classified rights or permissions.

Off-boarding | De-provisioning

Off-boarding and de-provisioning, a process whereby users are effectively removed from having any type of access rights to University-wide information systems, is a critical component of the access control lifecycle. Moreover, this process generally occurs when users have been terminated or have resigned, resulting in the revocation of all access rights to information systems.

And while there are many components, terms, processes, and procedures associated with user access rights, some of which have been illustrated above, they can be categorically placed under the umbrella of the <u>access control lifecycle</u>: *a lifecycle management process whereby a series of administrative, operational, and technical activities and related procedures are adopted, implemented, and undertaken for creating identities (Identification), authenticating to information systems (authentication), assigning users certain access rights, (authorization), employing effective segregation of duties, while also undertaking various auditing, monitoring, logging and reporting functions (accountability) for a given entities distributed information systems environment. Furthermore, the user identity, provisioning, & access rights lifecycle management process should always strive to advocate security, scalability, flexibility, along with the continued adoption of emerging technologies to meet its needs.*

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Access Control (AC) 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 Access Control (AC) 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 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:

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- Limit system access to the types of transactions and functions that authorized users are permitted to execute.

- Control the flow of Controlled Unclassified Information (CUI) in accordance with approved authorizations.
- Separate the duties of individuals to reduce the risk of malicious activity without collusion.
- Employ the principle of least privilege, including for specific security functions and privileged accounts.
- Use non-privileged accounts or roles when accessing non-security functions.
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
- Limit unsuccessful logon attempts.
- Provide privacy and security notices consistent with applicable CUI rules.
- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
- Terminate (automatically) a user session after a defined condition.
- Monitor and control remote access sessions.
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- Route remote access via managed access control points.
- Authorize remote execution of privileged commands and remote access to University's information.
- Authorize wireless access prior to allowing such connections.
- Protect wireless access using authentication and encryption.
- Control connection of mobile devices.
- Encrypt CUI on mobile devices and mobile computing platforms.
- Verify and control/limit connections to and use of external systems.
- Limit use of portable storage devices on external systems.
- Control CUI posted or processed on publicly accessible systems.

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 3.1.1	**Authorized Access Control**	
NIST SP 800-171 Rev2 3.1.2	**Transaction & Function Control**	
NIST SP 800-171 Rev2 3.1.20	**External Connections**	
NIST SP 800-171 Rev2 3.1.22	**Control Public Information**	
NIST SP 800-171 Rev2 3.1.3	**Control CUI Flow**	
NIST SP 800-171 Rev2 3.1.4	**Separation of Duties**	
NIST SP 800-171 Rev2 3.1.5	**Least Privilege**	
NIST SP 800-171 Rev2 3.1.6	**Non-Privileged Account Use**	
NIST SP 800-171 Rev2 3.1.7	**Privileged Functions**	
NIST SP 800-171 Rev2 3.1.9	**Privacy & Security Notices**	
NIST SP 800-171 Rev2 3.1.10	**Session Lock**	

NIST SP 800-171 Rev2 3.1.11	**Session Termination**	
NIST SP 800-171 Rev2 3.1.12	**Control Remote Access**	
NIST SP 800-171 Rev2 3.1.13	**Remote Access Confidentiality**	
NIST SP 800-171 Rev2 3.1.14	**Remote Access Routing**	
NIST SP 800-171 Rev2 3.1.15	**Privileged Remote Access**	
NIST SP 800-171 Rev2 3.1.16	**Wireless Access Authorization**	
NIST SP 800-171 Rev2 3.1.17	**Wireless Access Protection**	
NIST SP 800-171 Rev2 3.1.18	**Mobile Device Connection**	
NIST SP 800-171 Rev2 3.1.19	**Encrypt CUI on Mobile**	
NIST SP 800-171 Rev2 3.1.21	**Portable Storage Use**	

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