Version Date: 10/24/2024

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Policies

Contents

Document

Document	**Privacy Policy**
References	**HIPPA, FERPA**
Control	
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

Roles and Responsibilities

Implementing and adhering to the University's policies and procedures is a collaborative effort that requires a steadfast commitment from all personnel, including administrators, 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 concerning ASU information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's growing cybersecurity challenges.

- **Administration 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 must regularly report to the President regarding all aspects of the University's information systems posture.

- **Personnel:** Responsibilities include adhering to the University's information security policies, procedures, and 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 the Office of Technology Services, specifically those by other users. While undertaking day-to-day operations, end users may also notice issues that could impede the safety and security of ASU information systems and are to report such instances immediately to senior authorities.

Scope

These policies and supporting procedures encompass all information systems owned, operated, maintained, and controlled by ASU and all other internal and external information systems that interact with them.

- Internal information systems are those owned, operated, maintained, and controlled by ASU and include all network devices (firewalls, routers, switches, load balancers, and 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 description above of "Internal information systems."

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

Policies

Acceptable Use Policy

Overview

This acceptable use policy (AUP) outlines the rules and guidelines for using a particular system, network, service, or technology responsibly and ethically. It is designed to promote safe, legal, and appropriate use of technology while preventing misuse or abuse. This policy will be evaluated annually to ensure its adequacy and relevancy to ASU's needs and goals.

Purpose

The policy must always be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

All applicable users must adhere to the following policies to comply with the mandated University security requirements set forth and approved by the board. Acceptable usage guidelines cover the following items:

- Computer and information system usage
- Software and data usage
- Internet and e-mail usage
- Telephone usage
- Office equipment & materials usage
- Social media

As a requirement of information system access and a component of security awareness training, all information system users, whether employees or third-party personnel, will be required to provide signed acceptance of the acceptable usage guidelines. A copy of the signed document will be provided to the individual, and the Human Resources department will retain the original.

Access Control Policy

Overview

A critical component of any successful institution is the ability to properly provision, manage, monitor, and off-board | de-provision all users 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 component, application, data source, or any other type of business resource identified by a company for which users can access through a process generally known as authentication and authorization.

The growing surge of regulatory compliance requirements and 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)

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, typically a username. Users thus use their respective username with a password, passphrase, or some other commonly used method of "authentication" to authenticate to that 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 correctly identified and authenticated themselves, they are then "authorized" to perform certain functions within those information systems based on their access rights. Finally, "accountability" (i.e., effectively auditing and monitoring this 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 and traditional methods are successfully used to ensure 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 has 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 information systems are never assigned based on a specific employee’s demands, requests, or preferences. Additionally, mandatory access control (MAC) is another concept for access control. It is generally used for very secure environments whereby users can only access system resources 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 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 resigned, revoking all access rights to information systems.

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 access control lifecycle: *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 adequate 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, and flexibility, along with the continued adoption of emerging technologies to meet its needs.*

Per 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 will be evaluated annually to ensure 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 to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

ASU is to ensure that all applicable community users adhere to the following policies to comply 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 authorized users can execute.
- Control the flow of Controlled Unclassified Information (CUI) following 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 tasks in audit logs.
- Limit unsuccessful login 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 access to the University's information.
- Authorize wireless access before 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 the use of portable storage devices on external systems.
- Control CUI posted or processed on publicly accessible systems.

Compliance Mapping Matrix

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	

Audit and Accountability Policy

Overview

In today's world of regulatory compliance – and for information security best practices – it's essential for universities to configure information systems for baseline auditable events and to capture and store such events for further analysis as necessary. Information systems – network devices, servers (virtual and physical stand-alone servers), and the underlying operating systems and applications residing on such servers should capture essential baseline information for auditing purposes.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Audit and Accountability (AU) policy. This policy will be evaluated annually to ensure its adequacy and relevancy regarding ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Audit and Accountability (AU) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of the ASU information systems.

Policy Statement

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

- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
- Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
- Review and update logged events.
- Alert in the event of an audit logging process failure.
- Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
- Provide audit record reduction and report generation to support on-demand analysis and reporting.
- Provide a capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- Protect audit information and logging tools from unauthorized access, modification, and deletion.
- Limit management of audit logging functionality to a subset of privileged users.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.3.2	**User Accountability**	
NIST SP 800-171 Rev2 3.3.3	**Event Review**	
NIST SP 800-171 Rev2 3.3.4	**Audit Failure Alerting**	
NIST SP 800-171 Rev2 3.3.5	**Audit Correlation**	
NIST SP 800-171 Rev2 3.3.6	**Reduction & Reporting**	
NIST SP 800-171 Rev2 3.3.7	**Authoritative Time Source**	
NIST SP 800-171 Rev2 3.3.9	**Audit Management**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Content of Audit Procedure	
Event Logging Procedure	
Protection of Audit Information Procedure	

Audit Record Review, Analysis, and Reporting Procedure	
Audit Record Retention Procedure	
Audit Record Generation Procedure	
Audit Log Storage Capacity Procedure	
Audit Record Reduction and Report Generation Procedure	
Response to Audit Logging Process Failure Procedure	

Awareness and Training Policy

Overview

A quality security awareness training program should provide enterprise-wide training measures and subject matter explicitly relating to the applicable compliance requirement or any other necessary mandate. Ultimately, a sound security awareness program should implement the core components of Awareness, Training, and Education.

"Awareness" means that numerous measures are initiated and implemented to keep all employees knowledgeable about the threats, responses, and solutions to security issues affecting an organization. "Training" in that material is researched, developed, and subsequently utilized to educate employees on all aspects of security awareness. And lastly, "Education, in that adequate measures are undertaken for ensuring continuing education on security awareness is provided to all employees on a routine basis – whatever that may be – quarterly, annually, etc. It must be stressed that security awareness training is dynamic, changing as needed to meet the growing threats facing organizations.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Awareness and Training (AT) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Awareness and Training (AT) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Ensure that managers, systems administrators, and users of the University's systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- Ensure personnel are trained to carry out their assigned information security-related duties and responsibilities.
- Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.2.1	Role-Based Risk Awareness	
NIST SP 800-171 Rev2 3.2.1	Role-Based Training	
NIST SP 800-171 Rev2 3.2.1	Insider Threat Awareness	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Role-Based Training Procedure	
Training and Awareness Procedure	

Clean Desk Policy

Overview

A clean desk policy is essential to ensure that all sensitive/confidential materials are removed from an end user's workspace and locked away when the items are not in use or personnel leave their workstations. It is a critical component to reducing the risk of security breaches. This policy should also increase personnel's awareness about protecting sensitive information. This Clean Desk Policy applies to all ASU data assets. Specifically, it includes:

- Intellectual Property (IP), whether owned by *ASU* or provided by a third party.
- Personally Identifiable Information (PII) for personnel, students, clients, constituents, or third parties.
- Private or Sensitive Information (PI) personnel, students, clients, constituents, or other third parties.
- Financial information for ASU, its employees, students, clients, constituents, or other third parties.
- Other non-public data or information assets deemed the property of ASU.
- Other public data or information assets deemed the property of ASU.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Clean Desk policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Clean Desk policy to be adhered to and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- All Personnel must ensure that all PI, PII, and IP in hardcopy or electronic form are secure.
- PI, PII, and IP may not be left unattended in a manner accessible by unauthorized persons.
- Documents containing PI, PII, and IP, which are no longer required, must be destroyed securely.

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Clear Screen Policy	
Password Policy	
Data Protection Policy	
Security Awareness Training Policy	

Clear Screen Policy

Overview

A Clear Screen Policy, also known as a Screen Lock Policy or Secure Screen Policy, is a set of guidelines and practices within an organization that require employees to lock their computer screens when they are not actively using their devices.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Clear Screen policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

A Clear Screen Policy aims to enhance data security by preventing unauthorized access to sensitive information when employees are away from their desks or workstations. This policy is designed to provide ASU with a documented and formalized policy that can be followed and utilized throughout the university. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Ensure all personnel lock screens when working from home or other remote locations.
- Configure all devices to activate a screen lock after a predefined period of inactivity. The idle timeout should be set to a reasonable duration, considering security needs and user convenience.
- Ensure Employees should log out of their accounts and applications when they have finished using them, this is especially important in shared workspaces and public areas.
- Ensure that computer screens and electronic devices are not visible to unauthorized individuals.

Configuration Management Policy

Overview

Configuration management is one of the most essential practices within information security because critical system resources must be securely configured to ensure their confidentiality, integrity, and availability –the widely-known information security CIA triad. Configuration management is a broad-based concept used in various industries and business sectors, ranging from manufacturing to technology –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 in an organization's overall information system 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 to ensure 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 several helpful software tools and other utilities 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, ASU has established a formal Configuration Management (CM) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

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

Policy Statement

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

- Establish and maintain baseline configurations and inventories of the 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 the university's systems.
- Track, review, approve/disapprove, and audit university system changes.
- Analyze the security impact of changes before implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with university system changes.
- Employ the principle of most minor 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 a deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny all permit-by-exception (whitelisting) policies to allow the execution of authorized software.
- Control and monitor user-installed software.

Compliance Mapping Matrix

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
Access Restrictions for Change Procedure	
Baseline Configuration Procedure	
Configuration Change Control Procedure	
Impact Analysis Procedure	
Least Functionality Procedure	
Software Usage Restrictions Procedure	
User Installed Software Procedure	

Hardware Sanitization Policy

Overview

Hardware Sanitization Policy is a set of guidelines and procedures that a university follows to ensure that electronic devices, such as computers, laptops, servers, and other hardware components, are properly sanitized before being repurposed, recycled, or disposed.

Following the mandated university security requirements set forth and approved by the board, ASU has established a formal hardware sanitation policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

The Hardware Sanitization policy aims to protect sensitive data, maintain security, and comply with privacy regulations during the disposal or reuse of hardware. This policy is designed to provide ASU with a documented and formalized Hardware Sanitization 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.

Policy Statement

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

- Data Removal: Clearly outline the process for securely erasing all data from the hardware before it leaves the university's possession. This includes storage devices like hard drives and other components containing data, such as memory modules.
- Authorized Personnel: Specify who is authorized to perform hardware sanitization procedures. This could be a dedicated IT team or individuals responsible for data security.
- Data Destruction Methods: Detail the approved methods for data destruction. Standard methods include secure data erasure using specialized software, physical destruction of storage media (such as shredding hard drives), or data wiping using approved tools.
- Certification and Documentation: Describe the process of generating and maintaining data destruction or sanitization certificates. This documentation can prove that the university has taken appropriate measures to secure sensitive data.
- Reuse and Recycling: If the hardware is being reused within the university or donated to others, define the process for verifying that all data has been removed before the hardware is repurposed.
- Disposal Procedures: Specify the proper disposal of hardware that can't be reused or repurposed. This might involve partnering with certified recycling companies that adhere to responsible e-waste disposal practices.
- Physical Security: Address the importance of physically securing hardware awaiting sanitization or disposal. This could involve locked storage areas or containers to prevent unauthorized access.
- Inventory Management: Outline procedures for tracking hardware throughout its lifecycle, from acquisition to disposal, to ensure all hardware is accounted for.
- Employee Training: Train employees involved in the hardware sanitization process. This ensures everyone understands the importance of proper data removal and follows the approved procedures.
- Legal and Regulatory Compliance: Emphasize adherence to relevant data protection and privacy regulations, such as GDPR, HIPAA, or industry-specific standards that govern how data should be handled during hardware disposal.
- Auditing and Accountability: Describe how the university will conduct periodic audits or reviews of its hardware sanitization practices, ensuring policy compliance and identifying areas for improvement.
- Communication and Awareness: Highlight the importance of communicating the hardware sanitization policy to all employees and stakeholders, ensuring they understand their roles in maintaining data security.

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	**Notes and Comments**
Hardware Sanitization Procedure	

Identification And Authentication Policy

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 commonly used method of "authentication" to actually authenticate to that system resource.

The three (3) factors are generally considered as (1). something you know. (2). something you have. (3). something you are. Once users have correctly identified and authenticated themselves, they are then "authorized" to perform certain functions within those information systems based on their access rights. Finally, "accounting" (i.e., effectively auditing and monitoring this 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 and traditional methods are successfully used to ensure 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, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Identification and Authentication (IA) policy 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.

Policy Statement

ASU is to ensure that all applicable community users adhere to the following policies to comply 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 the University's systems.
- Use multifactor authentication for local and network access to privileged accounts and 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 specified 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 logins with an immediate change to a permanent password.
- Store and transmit only cryptographically protected passwords.
- Obscure feedback on authentication information.

Compliance Mapping Matrix

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 Procedure	
Personnel Security Procedure	
Authentication Feedback Procedure	
Authentication Management Procedure	
Cryptographic Module Authentication Procedure	
Identification and Authentication (Non ASU-OTS) Procedure	
Identity Proofing Procedure	
Identifier Management Procedure	
Re-Authentication Procedure	

Incident Response Policy

Overview

Data breaches, cyber security threats, and many other malicious exploits are challenging organizations like never before, ultimately requiring comprehensive security measures to help ensure the confidentiality, integrity, and availability of one’s entire information systems landscape. Unfortunately, security breaches do happen - even with the best controls in place - thus, the ability to respond swiftly and effectively is a must for mitigating further damage. It’s the main reason every organization should have a well-defined and in-depth incident response plan in place - one complete with documented policies and procedures, along with essential forms and templates to use as necessary. A structured protocol is critical for incident response initiatives as it achieves the following:

- Responding immediately with best-of-breed information security practices.
- Isolating the affected systems as quickly as possible, helping minimize the threat to other critical system resources.
- Helping minimizes system downtime while restoring critical infrastructure to full operational capabilities as quickly as possible.
- Providing a “lessons learned” approach for every incident, regardless of size, scale, complexity, and severity.

Comprehensive incident response measures require participation and involvement from everyone within ASU, from senior management down to end-users of systems - along with being aware of the following core components of incident response:

1. Preparation
2. Detection
3. Initial Response and Containment

4. Security Analysis | Recovery and Repair
5. Communication
6. Post-Incident Activities and Awareness
7. Monitoring
8. Reporting of Suspected Incidents
9. Training and Testing

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Incident Response (IR) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Incident Response (IR) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Establish an operational incident-handling capability for organizational systems, including adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate officials and/or authorities, both internal and external to the organization.
- Test the organizational incident response capability.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.6.1	**Incident Capability**	
NIST SP 800-171 Rev2 3.6.2	**Incident Reporting**	
NIST SP 800-171 Rev2 3.6.3	**Incident Response Testing**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Incident Response Assistance Procedure	
Incident Response Handling Procedure	
Incident Response Monitoring Procedure	
Incident Response Plan Procedure	
Incident Response Testing Procedure	
Incident Response Training Procedure	
Incident Response Reporting Procedure	

System Maintenance Policy

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 to ensure 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, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Maintenance (MA) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Perform regularly scheduled maintenance on the University's systems.
- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- Ensure that equipment removed for off-site maintenance is sanitized against any Confidential Uncontrolled Information (CUI).
- Check media containing diagnostic and test programs for malicious code before they are used in the university's systems.
- Multifactor authentication is required 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

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
Controlled Maintenance Procedure	

Maintenance Tools Procedure	
Nonlocal Maintenance Procedure	
Timely Maintenance Procedure	

Media Protection Policy

Overview

Media protection is a critical element of any institution's overall information systems security framework, as the ability to access, utilize, modify, store, transport, and sanitize media must only be conducted and initiated by authorized personnel to ensure the confidentiality, integrity, and availability of media. Furthermore, even today's digital world, media must be assessed in terms of digital media and non-digital formats, such as paper, microfilm, and other applicable hardcopy documents and materials.

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Media Protection (MP) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Media Protection (MP) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Protect (i.e., physically control and securely store) system media containing Confidential Uncontrolled Information (CUI), both paper and digital.
- Limit access to CUI on system media to authorized users.
- Sanitize or destroy system media containing CUI before disposal or release for reuse.
- Mark media with necessary CUI markings and distribution limitations.
- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- Control the use of removable media on system components.
- Prohibit portable storage devices when such devices have no identifiable owner.
- Protect the confidentiality of backup CUI at storage locations.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.8.2	**Media Access**	
NIST SP 800-171 Rev2 3.8.4	**Media Markings**	
NIST SP 800-171 Rev2 3.8.5	**Media Accountability**	

NIST SP 800-171 Rev2 3.8.6	**Portable Storage Encryption**	
NIST SP 800-171 Rev2 3.8.7	**Removable Media**	
NIST SP 800-171 Rev2 3.8.8	**Shared Media**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	**Notes and Comments**
Media Access Procedure	
Media Marking Procedure	
Media Storage Procedure	
Shared Media Procedure	

Personnel Security Policy

Overview

Comprehensive personnel security controls regarding user hiring, provisioning, and de-provisioning are ultimately essential in helping ensure the safety and security of organizational assets. Initiatives such as proper background screening and structured processes for removing access to information systems for terminated employees are just a few of the notable requirements for personnel security controls.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Personnel Security (PS) policy. This policy is to be implemented immediately and evaluated annually to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Personnel Security (PS) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Screen individuals before authorizing access to the University’s systems containing Controlled Unclassified Information (CUI).
- Ensure that the University’s CUI systems are protected during and after personnel actions such as terminations and transfers.

Compliance Mapping Matrix

Basic and Derived Security Requirements	**Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation**	**Notes and Comments**
NIST SP 800-171 Rev2 3.9.2	**Personnel Actions**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	**Notes and Comments**
Personnel Screening Procedure	
Personnel Termination Procedure	
Personnel Transfer Procedure	

Physical Protection Policy

Overview

Physical security elements are safeguards enacted to ensure that only authorized individuals can access various physical locations, such as corporate facilities, data warehouses, computer operation centers, and other critical areas. Physical security also consists of the various measures put in place for protecting institutional assets, ranging from people and property to tangible goods, services, or products.

With many institutions today outsourcing critical functions to data centers, managed services providers, and document storage facilities—to name a few—physical security has become a crucial component of one's risk assessment and risk management framework. Knowing where your assets are and how they are protected is paramount. But it's just as important to have physical security controls at one's corporate office, satellite offices, and other critical locations.

Another vital component of physical security is the supporting environmental security controls. Specifically, environmental security measures protect physical surroundings from damaging elements, such as fire, water, smoke, electrical surges, spikes, outages, and any other hidden dangers. Environmental safeguards are critical in that they, along with physical security, ensure the safety of the employees, company property, and all other pertinent physical elements near the facility.

By implementing the mandated university security requirements set forth and approved by the board, ASU has established a formal Physical Protection (PE) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Physical Protection (PE) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Limit authorized individuals' physical access to the University’s systems, equipment, and operating environments.
- Protect and monitor the physical facility and support infrastructure for the University’s systems.
- Escort visitors and monitor visitor activity.
- Maintain audit logs of physical access.
- Control and manage physical access devices.

- Enforce safeguarding measures for CUI at alternate work sites.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.10.3	**Escort Visitors**	
NIST SP 800-171 Rev2 3.10.4	**Physical Access Logs**	
NIST SP 800-171 Rev2 3.10.5	**Manage Physical Access**	
NIST SP 800-171 Rev2 3.10.6	**Alternative Work Sites**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Visitor Escort Procedure	
Physical Access Logs Procedure	

Privacy Policy

Overview

This Privacy Policy outlines the principles and practices governing the collection, use, disclosure, and protection of personal information under the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA) and Payment Card Industry (PCI) compliance. Following mandated organizational security requirements set forth and approved by management, ASU has established a formal Electronic Payment policy.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Privacy policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This Privacy Policy describes how ASU collects, uses, discloses, and protects the Personal Identifiable Information (PII) of personnel following the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). We are committed to maintaining the privacy and confidentiality of PII entrusted to the University. Additionally, this policy will be evaluated annually to ensure its adequacy and relevancy regarding ASU's needs and goals.

Policy Statement

This Privacy Policy applies to all PII (Personal Identifiable Information) collected, used, disclosed, and maintained by the University while providing healthcare and educational services. ASU is to ensure that all applicable community users adhere to the following policies to comply with the mandated University security requirements set forth and approved by the board. ASU shall:

Health Insurance Portability and Accountability Act Compliance

Comply with HIPAA, which governs the privacy and security of Protected Health Information (PHI). Following HIPAA, ASU shall:

1. Collect and use PHI solely for the purposes permitted under HIPAA, such as treatment, payment, and healthcare operations.
2. Implement appropriate safeguards to protect PHI's confidentiality, integrity, and availability.
3. Disclose PHI only as authorized by law or as necessary to provide healthcare services.

Family Education Rights and Privacy Act Compliance

Comply with FERPA, which safeguards the privacy of student educational records. Following FERPA, ASU shall:

1. Collect and use student educational records only for legitimate academic purposes and in compliance with FERPA.
2. Maintain the confidentiality and security of student educational records to prevent unauthorized access or disclosure.
3. Disclose student educational records in compliance with FERPA, such as for legitimate educational interests, with student consent, or as required by law.

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	**Notes and Comments**
FTC Safeguard Rules Section 314.4	

Risk Assessment Policy

Overview

The concept of risk management, which includes the process of performing a risk assessment, has quickly become one of the most notable topics in today’s growing world of regulatory compliance. Risk assessments are a key part of effective risk management and facilitate decision-making at all three tiers in the risk management hierarchy, including the organization, mission/business process, and information system levels.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Risk Assessment (RA) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Risk Assessment (RA) policy 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.

Policy Statement

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

- Annually assess the risk to the University’s operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from operating organizational information systems and the associated processing, storage, or transmission of CUI (Controlled Unclassified Information).
- Scan all University systems and applications periodically and when new vulnerabilities affecting them are identified.

- Remediate vulnerabilities following assessments of risk.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.11.2	**Vulnerability Scan**	
NIST SP 800-171 Rev2 3.11.3	**Vulnerability Remediation**	

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
Criticality Analysis Procedures	
Risk Assessment Procedures	
Risk Response Procedures	
Security Categorization Procedures	
Vulnerability Monitoring and Scanning Procedures	

Security Assessment Policy

Overview

Assessing one's control environment related to the security controls within NIST SP 800-171 and/or any other supporting or overlapping family of controls is critical for helping ensure the confidentiality, integrity, and availability of ASU information systems. Assessments are to be performed by qualified personnel—either internal and/or external—who have the necessary knowledge.

Following mandated University security requirements set forth and approved by the Board, ASU has established a formal Security Assessment (CA) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized Security Assessment (SA) policy to be followed and utilized throughout the University. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

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

- Annually assess the security controls in organizational systems to determine if they are effective in their application.
- Develop and implement action plans to correct deficiencies and reduce or eliminate University system vulnerabilities.
- Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.12.2	**Plan of Action**	
NIST SP 800-171 Rev2 3.12.3	**Security Control Monitoring**	
NIST SP 800-171 Rev2 3.12.4	**System Security Plan**	

System and Communication Protection Policy

Overview

The protection of information systems and the data stored and transmitted over such systems requires the Alabama State University Office of Technology Services (ASU OTS) to implement numerous communications protection initiatives to help ensure the network's confidentiality, integrity, and availability. 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, it is to be evaluated on an annual basis to ensure its adequacy and relevance to 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 times. Compliance with the stated policy will ensure the safety and security of ASU information systems.

Policy Statement

ASU is to ensure that all applicable community users adhere to the following policies to comply 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 the University’s systems) at the external and key internal boundaries of the University’s systems.
- Employ architectural designs, software development techniques, and systems engineering principles that promote adequate information security within the 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 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 an indication of devices in use to users present at the device.
- Control and monitor the use of mobile code.
- Control and monitor Voice over Internet Protocol (VoIP) technologies.
- Protect the authenticity of communication sessions.
- Protect the confidentiality of CUI at rest.

Compliance Mapping Matrix

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**	

System and Information Integrity Policy

Overview

The protection of information systems and the data stored and transmitted over such systems requires ASU to implement numerous system and information integrity initiatives to help ensure the confidentiality, integrity, and availability of the network.

In accordance with mandated University security requirements set forth and approved by the Board of Regence, ASU has established a formal System and Information Integrity (SI) policy. This policy is to be implemented immediately. Additionally, it is to be evaluated on an annual basis to ensure its adequacy and relevance to ASU's needs and goals.

Purpose

This policy is designed to provide ASU with a documented and formalized System and Information Integrity (SI) 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.

Policy Statement

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

- Identify, report, and correct system flaws promptly.
- Monitor system security alerts and advisories and take appropriate actions in response.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the University's systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
- Monitor the University's systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- Identify unauthorized use of the University's systems.

Compliance Mapping Matrix

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
NIST SP 800-171 Rev2 3.14.1	**Flaw Remediation**	
NIST SP 800-171 Rev2 3.14.2	**Flaw Remediation**	
NIST SP 800-171 Rev2 3.14.3	**Malicious Code Protection**	
NIST SP 800-171 Rev2 3.14.4	**Update Malicious Code Protection**	
NIST SP 800-171 Rev2 3.14.5	**System & File Scanning**	
NIST SP 800-171 Rev2 3.14.6	**Monitor Communications for Attacks**	
NIST SP 800-171 Rev2 3.14.7	**Identify Unauthorized Use**	

Responsibility for Policy and Procedures Maintenance

ASU is responsible for ensuring that the policy above initiatives, and if applicable – the relevant procedures – are kept current to comply 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 full-time or part-time, are employed by ASU.
- All contractors and third parties who work on behalf of ASU are paid directly.
- 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 who 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. The First Incident of a minor breach will result in a verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy in the ASU Personnel Handbook. If the offender 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 significant 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 document above and notify all users in a reasonable and acceptable timeframe and format.

__________________________ ____________________

Signature Date

Name

Title