Version 1.0

Version Date: 08/08/2023

ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Hardware Sanitization Policy

Contents

Document

Document	**Hardware Sanitization**
References	
Control	
Last Approved	
Next Review	

Annual Review and Revision Tracking

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

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.

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Hardware Sanitization 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

The purpose of the Hardware Sanitization policy is 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.

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 instances immediately to senior authorities.

Policy

ASU is to ensure that all applicable 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:

- Data Removal: Clearly outline the process for securely erasing all data from the hardware before it leaves the university's possession. This includes not only storage devices like hard drives but also any other components that might contain data, such as memory modules.
- Authorized Personnel: Specify who is authorized to perform hardware sanitization procedures. This could be a dedicated IT team or specific individuals responsible for data security.
- Data Destruction Methods: Detail the approved methods for data destruction. Common 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 certificates of data destruction or sanitization. This documentation can serve as proof 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 steps for properly disposing 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 keeping track of hardware throughout its lifecycle, from acquisition to disposal, to ensure all hardware is accounted for.
- Employee Training: Provide training to employees involved in the hardware sanitization process. This ensures that 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 to ensure policy compliance and identify 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.

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**

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