Augusta University
Policy Library

Encryption Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

This policy applies to all employees and staff of Augusta University (AU), hereinafter referred to as "AU". This policy applies to all duties of AU employees and staff performed within the scope of their employment at any site of the AU. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), and/or other sensitive information (SI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to PHI, ePHI, PII, PCI DSS, or SI.

It is the policy of AU to provide guidance for the use of encryption to protect electronic protected health information (ePHI), protected cardholder data, and student education records (and other confidential and proprietary electronic information) and to provide guidance for the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal and State regulations are followed.

This policy addresses the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations (as well as changes made through the Health Information Technology of Economic and Clinical Health Act (HITECH), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach Bliley Act (GLBA) and other applicable federal, state, or local laws and regulations that may relate to the protection and security of sensitive information through the use of encryption technologies to render this information unreadable while at rest and in motion.

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☐ Graduate Students ☒ Health Professional Students
☒ Staff ☐ Undergraduate Students ☐ Vendors/Contractors ☐ Visitors
☐ Other:

DEFINITIONS

Cloud: A computing infrastructure of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Device: Any media, material, or type of equipment that records, stores, transmits, distributes, or uses electronic information. This includes, but is not limited to, computers (hard drives), any removable/transferrable digital memory, disks, memory cards, cloud storage, internet, extranet or any other device which involves the access, storage, or creation of sensitive information.

Mobile Devices: are a subset of devices that reside outside of a traditional data center and can be removed or transported by one person, (e.g., laptops, tablets, smartphones, memory sticks, removable hard drives, biomedical equipment).

Encryption: Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

Electronic Protected Health Information (ePHI): ePHI as defined in the Health Insurance Portability and Accountability Act of 1996, (“HIPAA”), as amended. *ePHI* means individually identifiable health information that is Transmitted by electronic media or Maintained in electronic media

Electronic media means:
1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Payment Card Industry Data Security Standard (PCI DSS): Data collected by organizations that accept, store, transmit, or process cardholder data must comply with the PCI DSS and is administered by the PCI SSC (Payment Card Industry Security Standards Council) to decrease payment card fraud across the internet and increase payment card data security. This includes sensitive data that is presented on a card or stored on a card - and personal identification numbers entered by the cardholder.

Sensitive Information (SI): Any information relating to identified or identifiable individual or entity that is confidential, proprietary, or sensitive to such individual or entity and may cause harm to such individual or entity if accessed, used, or disclosed by unauthorized persons, or lost, either internal or external to AU. This includes, but is not limited to Confidential Information, Protected Health Information, Personally Identifiable Information, Payment Card Industry (PCI) data, undisclosed financial statements, audit reports, and other information subject to federal and state regulations.

Unsecured Protected Health Information: Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary (of HHS) in the guidance issued under section 13402(h)(2) of Public Law 111-5. This guidance specifies that only encryption and destruction, consistent with National Institute of Standards and Technology (NIST) guidelines, renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that notification is not required in the event of a breach of such information.

AU workforce: Full-time or part-time employees, trainees, vendors, contractors, or any other individuals who may create, use, disclose, access, or transmit any sensitive information.

POLICY

- Device encryption must address the following as defined by HIPAA, NIST, FERPA, GLBA, PCI and Proof that the data is sufficiently scrambled in a way that a third party could not possibly extract data from a lost or stolen hard drive or device,
- The key used to scramble the data must be strong enough to prevent guessing, even using brute force programs, and
- Controls must be in place to prove compliance with this standard if a device is missing.
- Unsecured protected health information, FERPA, GLBA encryption and PCI data must be destroyed and consistent with, at minimum, National Institute of Standards and Technology (NIST) guidelines.
- Federally Protected and PCI data must be destroyed following National Institute of Standards and Technology (NIST) guidelines.

Device encryption must address the following requirements as defined by HIPAA, NIST, FERPA, GLBA and PCI:

- Make a reasonable effort to ensure that all devices are properly encrypted before accessing, creating, or storing sensitive information,
- Not store sensitive information on unencrypted devices, and
- Promptly report lost, stolen, or compromised devices to law enforcement or any member of the Compliance Team.

PROCESS & PROCEDURES

1. The CISO shall make a reasonable effort to ensure:

- That all devices that may access, store, or create sensitive information are encrypted using methods that comply with this standard.
- That data is encrypted at rest and while in transit within reasonable industry standards or data security is otherwise addressed and documented.
- That the AU workforce is provided with the adequate tools and equipment to properly access, store, create, and transmit sensitive information.

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the Augusta University network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all networked devices must use only encrypted authentication mechanisms unless otherwise authorized by AU Cyber Defense or by the CIO.

Historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

Encryption, or equally effective measures, is required for all sensitive or confidential information, as defined in the Data Management and Classification Policy, that is stored on portable electronic storage media (including, but not limited to, CDs/DVDs, external/mobile storage and USB drives) and on portable computing devices (including, but not limited to laptop and notebook computers). This policy does not apply to mainframe and server tapes.

2. The CISO is responsible for:

- Establishing specific encryption standards to support encryption in a manner consistent with applicable regulatory standards and provide adequate protections for sensitive information and to complying with HIPAA, HITECH, FERPA, GLBA, PCI DSS and other applicable federal, state, or local laws and regulations that may relate to:
    - The protection and security of all sensitive information,
    - The protection and security of systems that accesses sensitive information, and
    - The protection and security of the methods used to access both systems and sensitive information within them.
- Ensuring that all waiver requests are reviewed to determine the level of risk to the organization prior to approval.

3. Sanctions:
Failure to comply with this policy will result in disciplinary actions, up to and including termination.

REFERENCES & SUPPORTING DOCUMENTS

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Gramm-Leach Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security regulations
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended
NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-52 Guidelines for the Selection and Use of TLS Implementations
NIST Special Publication 800-77 Guide to IPsec VPNs
NIST Special Publication 800-113 Guide to SSL VPNs
And other FIPS 140-2 validated processes
Payment Card Industry (PCI) PCI Security Standards Council
Privacy Rule (16 C.F.R. Part 313)

RELATED POLICIES

Acceptable Use of Electronic Mail & Electronic Messaging Policy
Data Management & Classification Policy
Mobile Device Policy

Remote Access Policy
Information Security Risk Management Policy
Secure Transmission of ePHI Policy
Electronic Access Control Policy
Workstation Security Policy
Securely Disposing of Electronic Media Policy

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021