Augusta University
Policy Library

Cybersecurity Training Policy

Policy Manager: Cyber Defense Department

POLICY STATEMENT
This policy applies to all employees and staff of Augusta University. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive information (SEI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to data involved with FERPA, SEI, PHI, or ePHI.

AU cannot protect confidentiality, integrity and availability of information and information systems without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.

This policy is in accordance with the requirements of the University System of Georgia (USG) Information Technology Handbook and the Board of Regents Policy Manual for cybersecurity awareness, training, and education.

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: Other Account Holders - Vendors

DEFINITIONS
Protected Health Information (PHI): PHI as defined in the Health Insurance Portability and Accountability Act of 1996 privacy regulations, ("HIPAA"), as amended.

Sensitive Electronic Information (SEI): 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 or AU Health. 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 any valid exception to the Georgia Open Records Law.

FERPA: Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

RESPONSIBILITIES

- Responsibility - It is the responsibility of the Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) to develop, implement, and manage the cybersecurity and privacy training program.

- Program Contents - The cybersecurity and privacy awareness and training program content will include a basic understanding of cybersecurity and privacy and the actions required to maintain security and to respond to suspected security incidents. The cybersecurity and privacy program should include topics such as the following:

    - The HIPAA Security Rule (§ 164.308(a)(5)): o Definition of SEI
    - Definition of PHI and e-PHI
    - Data included in FERPA regulations
    - Security Reminders
    - Protection from Malicious Software
    - Log-in Monitoring
    - Password Management
    - Workstation Security
    - Usage and Login Monitoring
    - Access Controls
    - Insider Threats
    - Incident and Breach handling procedures for employees
    - Names and contact information for the CISO, CPO, and Compliance Reporting Line.
    - AU Security and Privacy Policy and Procedure.
    - Expectations of compliance and AU Sanctions Policy for noncompliance.

PROGRAM COMPLIANCE

- Basic security and privacy training will be held upon hire and annually thereafter for all workforce members who come into contact with PHI or SEI.
- Advanced security and privacy training for IT staff will be held upon hire and annually thereafter.
- In addition to basic security training, cybersecurity training will be conducted semiannually, and completion will be documented.
- This content must be appropriate for the workforce members' knowledge, role, and responsibilities. This includes eliminating the requirement for the workforce member to complete training on areas outside of their scope of works (e.g. HIPAA and FERPA).
- The Security Awareness and Training shall be reviewed at least annually or within a reasonable after there are significant changes to HIPAA/FERPA/GLBA and other compliance frameworks.
- When information is obtained that could improve the cybersecurity and privacy training program or any shortcomings of the program are discovered, the program should be updated.
- The cybersecurity and privacy training program will be protected, controlled, and retained in accordance with federal, state, and organizational requirements.

- Remedial training will be required of workforce members as necessary response to a privacy or cybersecurity incident.
- Each workforce member's completed training is electronically recorded within the learning management system (LMS). Training transcripts may be printed after the courses are completed. Training content and learning reports must be retained for six years from the date of their creation or the date when it was last in effect, whichever is later.

- It is the workforce member's duty to complete all training assignments.
    - The Office of Compliance is responsible for ensuring training compliance with the staff under their supervision.
    - The Office of Compliance in collaboration with Cybersecurity, and Human Resources Workforce Development oversees the auditing and monitoring of privacy, confidentiality and cybersecurity workforce training.

    - Failure to complete assigned cybersecurity and privacy training will result in the workforce member's loss of access to PHI until the assignment is completed or may result in other disciplinary action.

REFERENCES & SUPPORTING DOCUMENTS
Board of Regents Policy Manual

Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy and Security Regulations

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended (including the Breach Notification Rule)

USG IT Handbook – Version 2.9.2

RELATED POLICIES
N/A

APPROVED BY:

Interim Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 1/15/2021

President, Augusta University Date: 1/15/2021