Augusta University
Policy Library

Workstation Security Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT
The purpose of this policy is to provide guidance for workstation security for Augusta University owned workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the following are met:

- HIPAA Security Rule "Workstation Security" Standard 164.310(c)
- FERPA
- GLBA
- PCI Compliance

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: Any individual who is issued or uses an AU workstation

DEFINITIONS
Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

PROCESS & PROCEDURES
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including, but not limited to, student information, student financial information, and protected health information (PHI) and that access to sensitive information is restricted to authorized users.

A. Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

B. AU will implement physical and technical safeguards for all workstations and workstations with access to electronic protected health information to restrict access to authorized users.

C. Appropriate measures include:
- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Complying with all applicable password policies and procedures. See Password Policy.
- Ensuring workstations are used for authorized business purposes per the Acceptable Use Policy.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers or within the appropriate system of record.
- Securing laptops and other mobile devices with encryption per the *Mobile Device Security policy* and the *Encryption Policy.*
- Comply with the baseline configurations. See *Augusta University End User Device Standard Configuration.*
- Restricting local admin access to those verified to need access.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents.
- Ensuring workstations have an up to date managed antivirus software installed.
- Ensuring workstations receive security patches on a timely basis.
- If wireless network access is needed to transmit PHI, proprietary, or sensitive data, devices must connect through the AU-Secure network.

D. Exceptions to this policy must be approved by the Chief Information Security Officer.

E. The Cybersecurity Office will monitor compliance with this policy.

F. Failure to comply with this policy may result in disciplinary action up to and including termination of employment.

REFERENCES & SUPPORTING DOCUMENTS

HIPAA Security Rule "Workstation Security" Standard 164.310(c)
Augusta University End User Device Standard Configuration
2020 USG Information Technology Handbook - VERSION 2.9.2

RELATED POLICIES

Acceptable Use of Information Technology
Mobile Device Policy
Encryption Policy
Password Protection Policy

APPROVED BY:

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

President, Augusta University Date: 6/2/2021