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 Augusta University owned workstations to ensure the security of (i) information that is on the workstation, and (ii) information that 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)
- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Compliance (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, personal, financial, and PHI) and to ensure that access to sensitive information is restricted to authorized users.

A. Workforce members using workstations will consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.

B. AU will implement physical and technical safeguards for all workstations to restrict access to authorized users.

C. User measures include:

Office of Legal Affairs Use Only
Executive Sponsor: VP and Chief Information Officer
Next Review: 6/2028

a. Required:
    - Restricting physical access to workstations to only authorized personnel.
    - Securing workstations prior to leaving area to prevent unauthorized access. Please refer to your local department's guidance for your specific devices and systems, or Knowledge Base (KB) Article 'How to Lock Your Screen (Windows/MacOS/Linux)'.
    - Powering off a workstation completely when left unattended and not connected to an AU network.
    - Complying with all applicable password policies and procedures. See Password Protection Policy.
    - Ensuring workstations are used for authorized business purposes per the Acceptable Use of Information Technology Policy.
    - Never installing unauthorized software on workstations.
    - Storing all sensitive information, including PHI on network servers or within the appropriate system of record.
    - Exiting running applications and closing open documents.
    - Ensuring workstations are powered on and maintain connection to the AU network (three days a week) to ensure workstations receive security updates on an ongoing basis. If the use of the devise in not used on a regular basis, it should be turned back into IT inventory.
    - If wireless network access is needed to transmit PHI, proprietary, or sensitive data, devices must connect through the AU-Secure network. Devices that use network access to transmit PHI, proprietary, or other sensitive data must connect through the AU-Secure network. Please see KB Article 'How to Connect To The AU-Secure Wireless Network'.

b. Recommended:
    - Installing privacy screen filters or using other physical barriers to alleviate exposing data.

D. Required IT Department measures include:
- Securing laptops and other mobile devices with encryption per the Mobile Device Policy and the Encryption Policy.
- Complying with the baseline configurations. See *Augusta University End User Device Standard Configuration*.
- Restricting local administrative access to individuals verified and approved for access.
- Ensuring workstations have an updated and managed antivirus software installed.

E. Any AU workstations that are not configured to baseline security controls or will not follow policy must have a documented exception; those exceptions must be reviewed by cyber defense annually. Coordinate through IT Support for any exception processes. Exceptions to this policy must be approved by the Chief Information Security Officer.

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

G. 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
2023 USG Information Technology Handbook - VERSION 2.9.7.1
Family Education Rights and Privacy Act (FERPA)
Gramm-Leach-Bliley Act (GLBA)
Payment Card Industry Compliance

RELATED POLICIES

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

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/13/2023

President, Augusta University Date: 6/13/2023