Augusta University
Policy Library

Information Technology Configuration Standards

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

Augusta University requires that all information technology (IT) devices be configured such that they can be managed and secured to maintain confidentiality, integrity and availability of clinical, instructional, research, and business resources and to enable IT configuration standards to meet certain industry, federal, and regulatory requirements.

Information technology that inputs, transmits, processes, or stores Augusta University data must be configured in accordance with the applicable configuration standard. Standards must be written and maintained by the unit responsible for the management of the technology in cooperation with Cybersecurity.

Prior to implementation, IT configuration standards must meet the applicable configuration standard to protect Augusta University data and information technology by ensuring a consistent, secure configuration across technology devices.

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: Business Associates

DEFINITIONS

Business Associate: A person or entity that creates, receives, maintains or transmits protected health information to perform certain functions or activities on behalf of a covered entity.

Three categories of service providers are specifically identified as business associates under the final rule:

- Health information organizations, e-prescribing gateways, and other people or entities that provide data transmission services to a covered entity with respect to protected health information and that require access on a routine basis to such protected health information;
- People or entities that offer personal health records to one or more individuals on behalf of a covered entity; and
- Subcontractors that create, receive, maintain or transmit protected health information on behalf of business associates.

Information Technology Device: Any institutionally or personally owned device to include, desktops, laptops, servers, network/telecommunications equipment, mobile devices, and storage systems that store, process, or transmit Augusta University data.

Device Managers: Entity or unit owning responsibility for maintaining or managing information assets and devices as assigned by the respective Cybersecurity Officer, CISO or CIO.

Configuration Standard: A document or collection of documents that describe how a device should be configured. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy.

Information assets can be defined as:

1. All categories of automated information, including, but not limited to, records, files, and data bases; and,
2. Information technology facilities, equipment (including endpoints, personal computer systems), and software owned or leased by a USG organization.

Cybersecurity: Organization official responsible for: 1) maintaining the cybersecurity of different types of information within the organization that typically involves maintaining computer networks to ensure that sensitive financial or private information is kept secure and cannot be accessed by someone not authorized to do so; 2) that usually reports to a chief information security officer or other member of upper management, such as a vice president in charge of information technology (IT) or cybersecurity.

PROCESS & PROCEDURES

General

All technology should have standards built with the intent of updating the standards for as long as it is in use. This should include sign-off by the CIO and Executive Sponsor, or their designees, at key milestones based on agreed-upon criteria. *See USG IT Handbook.*

Device Managers are responsible for developing and maintaining configuration standards for the information assets or devices over which they have primary responsibility. All standards will ensure compliance to any University System of Georgia (USG) requirements. The standards must be reviewed and updated on an annual basis at minimum. Prior to implementation, Device Managers will coordinate with Cybersecurity for analysis and review.

Standards and Quality Practices

Standards, procedures and practices for key IT processes should be identified and maintained. Industry best practices such as NIST guidance should be used for reference when improving and tailoring the organization’s quality practices.

When reviewing and updating configuration policies, Device Managers will identify, record, control, report, and verify the configuration standard.

Configuration Standard Baseline

- AU information systems must have baseline configurations developed, documented and securely maintained. Baseline configurations should be reviewed and updated:
  - Annually
  - When required due to system upgrades, patches, or other significant changes.
  - As part of information system installations and upgrades.
- Must include documented, up-to-date specifications to which the information system is built and configured.
- Must document and provide information about the components of an information system including, but no limited to:
  - Standard operating system and/or installed applications with current version numbers
  - Standard software that should be loaded on workstations, servers, network devices and mobile devices
  - Patch information should be kept up-to-date
  - If applicable, changes to network topology should be kept up to date – Logical placement of component should be consistent with enterprise architecture
- Must meet the security standards as approved by cybersecurity.

REFERENCES & SUPPORTING DOCUMENTS

Standards are available upon Request
USG IT Handbook https://www.usg.edu/information_technology_services/it_handbook/

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

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

President, Augusta University Date: 6/2/2021