Augusta University
Policy Library

Vulnerability and Patch Management Policy

Policy Manager: Chief Information Security Officer

1. PURPOSE

POLICY STATEMENT
Augusta University's Vulnerability and Patch Management Policy outlines necessary behaviors and actions to:

a. Maintain the integrity of network systems and data by applying the latest operating system and application security updates/patches in a timely manner.

b. Establish a baseline methodology and timeframe for patching and confirming patch management compliance.

c. Develop and implement a vulnerability management plan that includes, but is not limited to:

    1) Conduct continuous monitoring to identify and verify the presence and effectiveness of implemented measures (i.e., vulnerability scanning).

    2) Technology upgrades, which include, but are not limited to, operating systems upgrades on servers, routers, and firewalls. Appropriate planning and testing of upgrades must be addressed, in addition to departmental criteria for deciding which upgrades to apply.

    3) Security patches and security upgrades, which include, but are not limited to, servers, routers, endpoints, mobile devices, and firewalls. Application and testing of the patches and/or security upgrades must be addressed, in addition to departmental criteria for deciding which patches and security upgrades must be applied and how quickly.

    4) Intrusion Prevention System (IPS) and/or firewall configurations to detect anomalous activity in a timely manner to understand potential impacts. Documentation of the baseline configuration is requirement for each IPS and/or firewall with expected dataflow diagrams, updates of the documentation for all authorized changes and periodic verification of the configuration to ensure that it has no changes during software modifications or rebooting of the equipment.

    5) Endpoint configuration management requires the creation and documentation of a baseline configuration following the principle of least functionality for each organizationally owned

device grouping (i.e., Faculty/Staff, Location, Role) with expected dataflow diagrams, updates of the documentation for all authorized changes and periodic checking of the configuration unique to the group to ensure that it has not changed during software modifications.

6) Server configurations, which must clearly address all servers that have any interaction with internet, extranet, or intranet traffic. Creation and documentation of a baseline configuration following the principle of least functionality for each server with expected dataflow diagrams, updates of the documentation for all authorized changes and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment and their associated system dependencies is required.

7) Server hardening, which must cover all servers throughout the organization, not only those that fall within the jurisdiction of the organization's IT area. The process for making changes based on newly published vulnerability information as it becomes available must be included. Implement principles of least functionality. Implement and enforce an organization policy for making security upgrades and security patches.

8) Software management and software licensing, which must address acquisition from reliable and safe sources and must clearly state the organization's policy about not using pirated or unlicensed software. Implement integrity checking protocols to vary software, firmware, and information integrity.

9) Scan identified assets for vulnerabilities, which are documented and mitigated or remediated.

d. Cyber Defense is charged with helping to protect the University's electronic information. To do so, Cybersecurity conducts regular scans of the entire enterprise looking for misconfigured and/or unsecured electronic devices. Cybersecurity then works with IT, IT Partners, and other units, to verify and remediate discovered vulnerabilities, especially when a new threat has been discovered.

2. SCOPE

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: Account Holders - Vendors

3. DEFINITIONS

Refer to the Cybersecurity Program (Charter) Policy

4. POLICY

a. Vulnerability Management

Develop and implement a vulnerability management plan that includes, but is not limited to:

1) Server hardening, which must cover all servers throughout the organization's IT area.

2) The process for making changes based on newly published vulnerability information as it becomes available must be included.

3) This must address, and be consistent with, the organizations' policy for making security upgrades and security patches.

4) Cybersecurity is authorized to conduct routine scans of devices, systems, and applications connected to enterprise networks to identify operating system and application vulnerabilities.

5) All System Owners are required to ensure routine initiation and review of the results of vulnerability scans of devices, systems, and applications for which they are responsible; and to evaluate, test, and mitigate, where appropriate, identified vulnerabilities based on the below target priorities established by Information Security.

6) Cybersecurity will conduct continuous monitoring to verify and validate the protective measures implemented.

7) A plan for technology upgrades such as servers, routers, and firewalls will be established to include appropriate criteria for discerning which upgrades to apply. This will also include upgrade planning and testing.

8) A plan will be maintained covering IPS, and firewall configurations including documented baseline configurations and expected dataflow diagrams. The configuration will be verified periodically to ensure no unauthorized changes have been made. IPS and firewalls will detect abnormal traffic and behavior in a timely manner to understand potential impacts.

9) Documentation will be maintained for endpoint configuration management to include baseline configuration and expected dataflow diagrams. The documentation will be updated with all authorized changes. The principle of least functionality will be implemented for the baseline of each device group and checks will be performed to ensure no unauthorized changes have been made.

10) Servers baseline configurations must be documented, following the principle of least functionality, and clearly address all servers that have any interaction with internet, extranet, or intranet traffic. Documentation will also include data flow diagrams and records of authorized changes. Periodic checks will be performed to ensure unauthorized changes have not been made to the baseline configuration.

11) Server hardening must cover all servers throughout the organization. A process for making changes based on new vulnerability information will be maintained. This process will be consistent with upgrade and patch management policy.

b. Remediation Target Priorities

1) The following table defines how remediation priorities will be assigned and the target resolution timeframe for vulnerabilities in each priority rank. The use of "days" versus "business days" in expressing times is significant – not all vulnerabilities can wait until the start of the next business day.

Priority Rank	*Definition*	*Initial Assignment*	*Target Resolution*
Critical	*Vulnerability that is remotely exploitable with no compensating controls*	*1 day*	*2 days*

High	*Vulnerability that is remotely exploitable with compensating controls*	*2 business days*	*1 week*
Medium	*Vulnerability that is not remotely exploitable*	*5 business days*	*30 days*
Low	*Vulnerability that cannot immediately be exploited.*	*1 month*	*90 days*

2) It may be necessary to further prioritize hosts within the priority rankings above by system/data classification, compliance requirements, and pre-existing risk.

c. Patch Management

1) Every IT asset and application must have an identified IT Team responsible for its maintenance and patching. This team must define a process for patching the systems they are responsible for. This process must include:

    a) A risk-informed patch cycle for all server, endpoint, and network operating systems; as well as known and approved applications.

    b) Any emergency patching outside of the routine patching schedule must be done according to level of risk, as determined by the Cybersecurity team using timelines in above table.

    c) Servers, services, or applications must be maintained with current OS, application, or security patch levels, as recommended by the software manufacturer, and informed by risk, to protect Enterprise information from known cybersecurity issues.

2) Using an automated centralized patch management distribution tool, whenever technically feasible, which:

    a) maintains a database of patches

b) deploys patches to endpoints
c) verifies installation of patches
d) removal of end-of-support or end-of-life software in production

3) The written patch management procedure shall include:

a) If patch management is outsourced, or a system is vendor managed, service level agreements must be in place that address the requirements of this policy and outline responsibilities for patching. If patching is the responsibility of the third party, system analysts must verify that the patches have been applied.

b) Removing end-of-support/end-of-life software in production. End of support software will not be utilized in production.

d. Exemptions from the Scanning Process

a) Vulnerability management scanning is an essential practice for a secure organization and the goal is to have 100% participation. If scanning creates issues for a system, the system owner or administrator shall work directly with Cybersecurity to review feasible options. Those options might include disabling a specific vulnerability check that may be causing an issue. An approach that solves the specific problem will be preferred over a general exemption as more general exemptions may cause critical vulnerabilities to be missed.

b) Exemptions from vulnerability scanning for an entire system will be granted only after an exception form has been signed by the head of the department and submitted to Cybersecurity for review and documentation.

c) Systems that perform endpoint scanning must be continuously updated as new vulnerabilities are discovered, announced, and scanning methods developed.

d) Scanning for vulnerabilities in systems and hosted applications, where permissible, following an organization defined frequency and/or when new vulnerabilities potentially affecting the system are identified and reported.

e) Employing vulnerability scanning tools and techniques that facilitate interoperability among existing tools and automate parts of the vulnerability management process for efficiency.

i. Analyzing vulnerability scan reports and results from control assessments (i.e., scans, assessments, and audit reviews and engagements).

ii. Employing vulnerability scanning tools that include the capability to readily update the vulnerabilities definitions and signatures to be scanned.

iii. Sharing information obtained from the vulnerability scanning process and control assessments with USG cybersecurity community (where appropriate) to help eliminate similar vulnerabilities in other systems.

5. ENFORCEMENT OF POLICY

a. Staff members found in violation of this policy may be subjected to disciplinary actions, up to and including termination.

b. The cybersecurity office will monitor compliance with this policy.

REFERENCES & SUPPORTING DOCUMENTS

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).

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 4/9/2024

President, Augusta University Date: 4/9/2024