Augusta University
Policy Library

Vulnerability and Patch Management Policy

Policy Manager: Cyber Defense Department

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

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

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

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.

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
The Information System Owner (also referred to as **System Owner**) is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system.

POLICY

Vulnerability Management

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

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.

Remediation Target Priorities

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

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

Exemptions from the Scanning Process

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 possible 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.

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

Patch Management

A) 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:

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

   II. 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.

   III. 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.

   IV. Using an automated centralized patch management distribution tool, whenever technically feasible, which:

      i. maintains a database of patches
      ii. deploys patches to endpoints
      iii. verifies installation of patches.

B) 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.

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
N/A

APPROVED BY:
APPROVED BY:

Interim Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 12/19/2020

President, Augusta University Date: 12/19/2020