Vulnerability Management Policy

I. POLICY STATEMENT

Auburn University ("the University," "University") requires that all entities managing assets that transmit, store, or access university data mitigate security-related vulnerabilities.

II. POLICY PRINCIPLES

Vulnerability management is a process supporting the identification of weaknesses in operational systems (applications, operating systems), determining the risks they represent to the University, and addressing the risk through removal, mitigation, or acceptance. It is the responsibility of system owners, system administrators, and/or other responsible parties to ensure their systems' security vulnerabilities are remediated.

The Information Security Office must be granted the ability to run credentialed vulnerability scans on all network connected servers.

All servers connected to the Auburn Network must be registered using the OIT asset management system.

Prior to any firewall rule allowing inbound access to Auburn resources, all critical and high vulnerabilities must be remediated or mitigated.

III. EFFECTIVE DATE

12/1/2018

IV. APPLICABILITY

This policy applies to all University colleges, departments, administrative units, and affiliated organizations. For the purposes of this policy, "affiliated organization" refers to any organization associated with the University that uses university information technology resources to create, access, store, or manage University data. It also applies to any third party creating, storing, or maintaining University data per a contractual agreement.

V. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer
Responsible Executive: Chief Information Officer (CIO)
Responsible Officer: Chief Information Security Officer (CISO)

VI. DEFINITIONS

Vulnerability: A weakness in software or hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability of that component.

Mitigation: Configuration changes, removal of affected products, or addition of components meant to augment security. All mitigation efforts are intended to lower organizational risk to acceptable levels.

Common Vulnerability Scoring System (CVSS): An open scoring system used to standardize ratings of potential severity and potential impact to an organization.

POA&M: A Plan of Action & Milestones document defining specific milestones (including dates), resources required, and risk mitigations that will be undertaken to fix a vulnerability on the network.

Mission Critical Vulnerability: A vulnerability that would have significant immediate impact on the University's ability to maintain operations.

VII. POLICY PROCEDURES

The Chief Information Security Office shall maintain definitions on appropriate vulnerability categories of Critical, High, Medium, Low and Informational.

Devices Requiring External (Inbound) Access

Devices requiring firewall rules configured to allow inbound access from the Internet will be entered into the asset management system and have a current vulnerability scan with all critical and high risk findings mitigated prior to firewall rule creation.

Only approved members of the OIT and Distributed IT staff will be authorized to request firewall modifications.

Scanning Devices

Devices added to or that currently exist on the network will be scanned using the centralized Information Security Team Vulnerability Assessment engine.

Scans will be authenticated using an account with administrative level access.

All servers will be scanned at least monthly.

Remediation, Mitigation of Plan of Action and Milestones (POA&M)

All Critical and High vulnerabilities identified will be remediated, mitigated, or have a Plan of Action and Milestones (POA&M) established within 14 days. The POA&M must contain the information identified in Appendix A.

All medium vulnerabilities will be remediated, mitigated, or have a POA&M established within 90 days.

Once findings are remediated, a re-scan of the affected assets will be performed. If a finding is believed to be a false positive, the system administrator should obtain validation by working with the Information Security Team. (infosec@auburn.edu)

Vulnerabilities that cannot be remediated within specified time periods will be entered into the POA&M process maintained by the Information Security Office.

Mission Critical Vulnerabilities

In situations where the Information Security team determines a vulnerability to be mission critical, vulnerability remediation and mitigation procedures will begin immediately.

The CISO or his designee will manage the process and provide status reports to senior leadership.

Any systems not in compliance, or without approved exceptions from the CIO, will have network access removed or restricted.

Notification Process

The Information Security Office will provide summary results to the dean or department head on a monthly basis.

Removal Process

Systems not remediated (within identified timeframes) or possessing an approved POA&M will be subject to network removal.

All network removals will occur with approval by the CIO or CISO (or designees). The system owner can voluntarily remove a vulnerable system at their discretion.

If a system maintains critical business functions and is designated a high risk system, approval to remain on the network must be granted by the CIO or CISO (or designee).

If a system must be removed, the CIO, CISO, and college level IT director (or equivalent) will be notified.

NOTE: Any outage communication to end users must be made by the system owner or responsible IT department.

Returning a system to the network requires verification from the Information Security team and the college level IT director (or equivalent).

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

All exclusions to this policy must be approved by the CIO or the CISO.

X. INTERPRETATION

For interpretations of this policy please refer to the Chief Information Security Officer.

Appendix A:

Heading	Contents
Item Identifier	A unique weakness identifier used to track and correlate weaknesses that are ongoing throughout quarterly submissions within the organization. The numbering schema for the weakness identifier will be determined by the organization.
Weaknesses or Deficiency	A weakness or deficiency represents any program or system-level information security vulnerability that poses an unacceptable risk of compromising confidentiality, integrity, or availability of information. Describe weakness or deficiency identified by certification/validation testing, annual program review, IG independent evaluation, or any other work done by or on behalf of the Service/Agency. Sensitive descriptions are not necessary, but sufficient detail must be provided to permit oversight and tracking.
IT Security Control Mapping	The Security Controls are listed in the NIST SP 800-53 and shall directly relate to the weakness identified in Column 2. For a security weakness found by means other than a security controls assessment (e.g., vulnerability test), map the deficient function into the applicable security control.
Point of Contact (POC)	A POC is the organization or title of the position within the organization that is responsible for the mitigation of the weakness. Assigned responsible individuals shall be identified by name as well as organization/title.
Status	Remediation Status including false POC verification and any updates regarding timelines or fix actions.
Resources Required	Estimated funding and/or manpower resources required for mitigating a weakness. The source and type of funding (current, new, or reallocated) and any funding obstacles should be noted. Note: Be sure to include the total funding requirements in the Security Costs field in Column 13 of the POA&M.
Scheduled Completion Date	Completion dates shall be determined based on a realistic estimate of the amount of time it will take to procure/allocate the resources required for the corrective action and implement/test the corrective action. Once assigned, this date shall not be changed. If a security weakness is resolved before or after the originally scheduled completion date, the actual completion date shall be placed in the Status field. Note: This column should never be left blank, or marked TBD or Unknown. A date must be provided unless the risk is accepted. If risk is accepted, enter N/A.
Milestones with Completion Dates	Milestones with completion dates outline the specific high-level steps to be executed in mitigating the weakness and the estimated completion date for each step. Initial milestones and completion dates should not be changed. Changes to milestones should be placed in the Changes to Milestones field.

Changes to Milestones	Changes to milestones indicate the new estimated date of a milestone's completion if the original date is not met. The new date and reason for the change in milestone completion should be recorded. No changes should be made to the original data recorded in columns 6 and 7.
Weakness or Deficiency Identified By	This column indicates the source of the weakness (e.g., security controls assessment, penetration test, IG audit, certification testing), the reviewing agency/organization, and the date that the weakness was identified. For example: Quarterly internal security controls review on December 10, 2017
Risk Level	The risk level is a ranking (CRITICAL, HIGH, MEDIUM, LOW) that determines the impact of a vulnerability, if exploited, to the system, data, and/or program.
Estimated Cost	The estimated cost of correcting the weakness or deficiency. The total estimated cost (arrived at by adding up the individual estimated costs of correcting each weakness or deficiency) is entered in the Security Costs box in Section 1.
Comments	Include any amplifying or explanatory remarks that will assist in understanding other entries relative to the identified weakness(es). Also include mitigating factors that will lessen the risks to the system and the network. Recommendations to downgrade a finding based on implemented/inherited mitigations should be listed here as well. The 'Comments' column shall also be used if there is a delay or change in a Milestone or Scheduled Completion Date. Additionally, the 'Comments' column shall identify other, non-funding-related, obstacles and challenges to resolving the weakness (e.g., lack of personnel or expertise, or developing new system to replace insecure legacy system).
Remediation	Recommended fix actions.

https://nvd.nist.gov/vuln-metrics/cvss
https://nvd.nist.gov/vuln
http://www.auburn.edu/oit/security/minimum-security-standards.php