University of Alabama at Birmingham
VULNERABILITY MANAGEMENT RULE

March 9, 2020

Related Policies, Procedures, and Resources

Data Protection and Security Policy
Data Classification Rule
Data Protection Rule
Minimum Security for Computing Devices Rule
Patch Management Rule

1.0 Introduction

This purpose of this document is to describe the process used by University of Alabama at Birmingham Information Technology (UAB IT) in mitigating the risks from computer security vulnerabilities. This standard is intended to represent a minimum baseline for managing vulnerabilities on UAB systems pursuant to the Data Protection and Security policy. Business units may implement more strict standards. This standard may not address every requirement for remediation. Risk assessments, data classification, access control processes, and other requirements may determine that additional remediation beyond this standard is required for a particular system.

2.0 Scope and Applicability

All systems where UAB data is stored, processed, or transmitted must be regularly reviewed for vulnerabilities. Any vulnerability identified will be mitigated based on the criticality of the vulnerability, and the classification of data within the system.

3.0 Roles & Responsibilities

Chief Information Security Officer (CISO)

The CISO is the owner of the vulnerability management process. The CISO designs the process and ensures is implemented as designed. Additionally, the CISO is responsible for approving and overseeing campus use of an enterprise scanning and assessment tool. Further, the CISO has the authority to take action as needed, to ensure that all systems have vulnerabilities are remediated and that any un-remediated issues do not pose a threat to University resources.

UAB Information Security

Members of the UAB and UAB Health System Information Security teams are

responsible for developing and implementing an information security program as well as the supporting data security and protection policies, standards and procedures. UAB Information Security is responsible for providing the approved enterprise vulnerability management and penetration testing service. Further UAB Information Security is responsible for providing the results of vulnerability scanning and penetration testing activities to appropriate system administrators and/or Information Security Liaisons, and validating remediation of any noted vulnerabilities.

Information Security Liaison (ISL)

Each unit or department senior manager will designate at least one ISL who will act as a liaison to the UAB Information Security team. ISLs oversee information security responsibilities for the departments, including assisting with security awareness and security incident response.

For UAB covered entities, UAB Health System has established the Entity Security Coordinator who will act as a liaison to the UABHS Information Security Team and the Entity Privacy Coordinator who will act as a liaison to the UABHS Privacy Officer.

Data Stewards

Data Stewards have administrative control and are officially accountable for a specific information asset. Data Stewards are:

- Responsible for assigning an appropriate classification to the information;
- Accountable for who has access to information assets; and
- Responsible for ensuring compliance with policies and regulatory requirements related to the information.

Data Custodians

Data Custodians safeguard the data on behalf of the Data Steward.

UAB's central Information Technology (IT) units shall be responsible for protecting all institutional data maintained/stored in the institutional information systems.

UAB Health System Information Services (HSIS) shall be responsible for protecting all Health System data maintained/stored in the institutional information systems.

System Administrators

System Administrators are individuals within the central IT/HSIS or school/department units with day-to-day responsibility for maintaining information systems. They are responsible for following all data security protection procedures and practices.

Data Users

Data Users are individuals authorized to access UAB data and are responsible for protecting the information assets on a daily basis through adherence to UAB policies.

4.0 Vulnerability Discovery

Vulnerabilities in computing devices across campus will be discovered by two means: vulnerability scanning and penetration testing. Vulnerability discovery may be conducted from an internal campus network, or an external perspective.

4.1 Vulnerability Scanning

All computing devices connected to the UAB network, or systems storing or processing UAB business data, are required to be scanned for vulnerabilities on a periodic basis. Vulnerability scanning will be conducted on a monthly basis as a part of normal production operation. More frequent scanning is recommended for systems storing or processing data which is classified as Sensitive or Restricted/PHI, or as required by applicable regulations or standard.

Additionally, scanning activity will occur on an as needed basis under the following circumstances:

- New service or system prior to becoming Internet-facing,
- Major change with existing information system to revalidate security controls,
- Emerging threat due to newly discovered vulnerability,
- Incident response and recovery.

4.2 Penetration Testing

Penetration testing is required for all UAB mission critical systems, all systems hosting Restricted/PHI or Sensitive data, and all Internet-facing systems on no greater than a biennial basis. Penetration testing is also required prior to the deployment of new systems and applications or following major changes, service rollouts, or system upgrades to existing systems and applications.

Penetration testing is subject to the Scope and Rules of Engagement, as defined, drafted, and agreed upon by UAB Information Security and the responsible ISL or system administrator.

Any exploitable vulnerabilities discovered during the penetration test are subject to the same remediation timelines as defined in the Vulnerability Classification Remediation Timeline.

4.3 Scanning and Mitigation

All computing devices connected to the UAB network or systems storing/processing UAB business data are required to be scanned for vulnerabilities. Vulnerability scanning will include the regular credentialed scanning of systems.

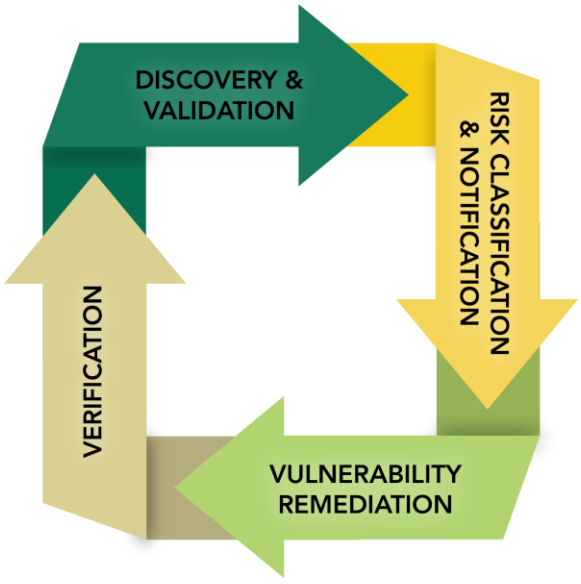
Information Security Liaisons and/or systems administrators must correct any identified vulnerabilities according to this standard, which could include:

- Deploying available updates and/or software patches,
- Performing configuration changes which address the vulnerabilities identified,
- Removing outdated software versions as newer versions are made available.

Information Security Liaisons and/or systems administrators must request and justify all exceptions to mitigate according to this standard.

All university schools, colleges, centers and business units must develop and adhere to procedures for vulnerability management, including the regular credentialed scanning of systems. Vulnerability management procedures must also address remediating detected vulnerabilities, including timely patch and configuration management, effective change management procedures, and reporting the status of issues to the University Risk Cabinet.

UAB Information Security will be utilizing a continuous monitoring methodology for vulnerability management. This methodology of Discovery & Validation, Risk Classification & Notification, Vulnerability Remediation, and Verification of mitigation will occur in a cyclical basis. Additionally, UAB Information Security will maintain metrics to the vulnerability management program and report the status of issues to the University Risk Cabinet and other organizational leaders by unit on a quarterly basis.



5.0 Un-remediated Systems

The CISO, or delegate, shall communicate directly with Information Security Liaisons and appropriate system administrators in advance regarding any action required to give the department the opportunity to respond. This communication relies upon accurate ownership information and staff contact information being available to the CISO and UAB Enterprise Information Security. In the absence of high-risk circumstances (i.e., a critical vulnerability being actively exploited against a relevant system), the CISO shall communicate at least five days in advance of any action to be taken. In the event of large-scale, high-risk vulnerabilities, the CISO may communicate campus-wide to all Information Security Liaison (ISL), Data Custodians, System Administrators, or other mass-communication paths regarding necessary remediation actions.

High-impact actions such as blocking systems from the campus network shall require the joint approval of the Vice President of Information Technology and Chief Information Officer (CIO), and Associate Vice President and Chief Information Security Officer (or in their absence, CIO/CISO delegates) and may involve communication with appropriate unit leader.

If a system is removed from the network for non-remediated vulnerabilities, the CISO may require additional controls or a control plan prior to allowing a system back on the campus network. The CISO must consider the risk sufficiently mitigated prior to authorizing network service restoration.

The Enterprise Information Security Office will work in collaboration with internal University committees or programs to develop specific guidelines regarding un-remediated systems within the framework of this rule. These guidelines will be approved by the CISO and will balance the requirements of this rule with the potential negative impact to the mission of the University.

6.0 Vulnerability Classifications

The following classifications describe the severity levels that can be assigned to a vulnerability. UAB IT utilizes multiple commercial and open-source tools to conduct vulnerability assessments and penetration testing. Microsoft System Center Configuration Manager is used to inventory assets and patch levels within windows-based systems. These tools provide output that maps into the NIST National Vulnerability Database with Common Vulnerability Scoring System (CVSS), an open framework for communicating the characteristics and impacts of IT Vulnerabilities. Validated findings will be assessed based on the risk of the system and data classification, and will be assigned vulnerability classification as listed below.

End-of-life operating systems or applications are considered a critical vulnerability per CVSS scoring (CVSS Base Score of 10) and are not permitted for UAB business use under the

Minimum Security for Computing Devices Rule. These systems must be remediated expediently as would any other urgent classified vulnerability.

Level 5: Urgent – denotes a vulnerability through which an intruder can easily gain control at the administrator level of any affected host. This class of vulnerability poses the highest risk for a system-wide compromise of the UAB campus network.

Examples: Domain administrator account compromise of UAB Active Directory.

Level 4: Critical – denotes a vulnerability through which an intruder could gain access to an individual host at the administrator level or could possibly access Restricted/PHI or Sensitive data stored on that host. While this class of vulnerabilities is extremely serious, the risk of a break or compromise is not as urgent as with a level 5 vulnerability.

Examples: Compromise of a server administrator account to an individual server, Internet-accessible remote code execution vulnerability of a system with Restricted/PHI Data or other sensitive data.

Level 3: Serious – denotes a vulnerability that may allow an intruder to gain access to specific information stored on the host, including security settings. While not immediately associated with a compromise of an affected host, these vulnerabilities allow intruders to gain access to information that may be used to compromise the host in the future.

Examples: Cross-site scripting (XSS) vulnerability within a web application, malformed document which can cause an application to crash.

Level 2: Medium – denotes a vulnerability through which intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

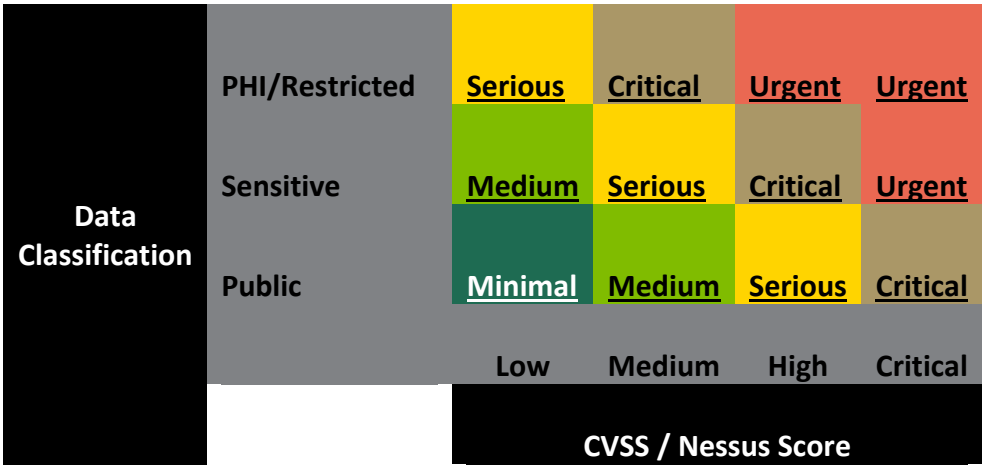
Examples: Configuration issues with services presenting application versions in banners.

Level 1: Minimal – denotes a vulnerability that do not pose an immediate threat to the host or the UAB campus network. These vulnerabilities refer mostly to weaknesses in a device that allow an intruder access to information that may be used in the future to compromise the host. Intruders can collect information about the host (open ports, services, etc.) and may be able use this information to find other vulnerabilities. Departments may opt to mitigate these vulnerabilities based on their network architecture or set up a timeframe for remediation based on the information stored on the device.

Examples: Open ports and services available on a particular device as identified by nmap.

Any identified vulnerabilities related to missing patches or improper configuration must be remediated within the timeframes specified below, or an exception must be in process or approved. For exception requests to be considered in process, relevant administrators must be working diligently toward approval, and Enterprise Information Security Office must have the exception request in hand. Remediation and mitigation should be prioritized based on the degree of associated severity, and the classification of data stored or processed by the system.

For vulnerability remediation, administrators should perform effective testing and follow reasonable change management procedures to ensure patch installation for affected systems.



7.0 Remediation and Mitigation Descriptions

After a vulnerability is detected, and a fix is available, a timeline for remediation begins. Level 5 (Urgent) vulnerabilities of mission-critical systems or those systems holding Restricted/PHI may require activation of the UAB Incident Response process for a critical incident at the direction of the CISO.

For level 5 (Urgent) and level 4 (Critical) vulnerabilities for systems holding Restricted/PHI or Sensitive data and/or those systems designated as mission critical, exceptions to the timeline must be granted by the CISO or delegate. Any required remediation activity involving enterprise, mission critical systems must follow the UAB Enterprise Change Management process to deploy and test in an expedient manner and during agreed maintenance windows.

For all other systems, departments are responsible for managing time exceptions on a case-by-case or blanket-exception basis and may establish appropriate procedures for managing those vulnerabilities within the stated timelines. Please note that in rare instances the CISO or delegate may determine that a specific vulnerability poses unacceptable risk to other UAB systems, in which case remediation may be required on a timeline determined by the CISO or delegate.

Remediation is required within the listed periods unless a documented exception request has been submitted to Enterprise Information Security to “halt the clock,” and that exception is in process and being worked diligently by relevant administrators or has been approved. CISO-approved exceptions will document the specific remediation timeline requirements for that system or document compensating controls if remediation is not feasible, not necessary, or not appropriate.

Vulnerability Remediation Timeframes

Urgent	1 day
Critical	14 days
Serious	31 days
Medium	Case-by-case
Minimal	Case-by-case

8.0 Sanctions

Due to the significant level of risk tied to Urgent issues and the danger that they pose to UAB users and resources, failure to remediate Urgent issues within one day of notification will result in network access to the offending system(s) or applications(s) being terminated until the Urgent issue has been successfully remediated. Urgent issues involving enterprise, mission-critical systems must follow UAB Enterprise Change Management process to deploy any appropriate mitigation activities during maintenance windows and is not subject to this sanction.

Any device that does not remediate vulnerabilities as outlined in this standard may be removed from the UAB network, disabled, etc., as appropriate until the device can comply with this standard or an exception request be approved.

9.0 Exceptions

Exceptions may be granted in cases where security risks have mitigating controls in place to lessen the intensity from a critical to a minimal level. To request a security exception, complete the UAB Security Policy Exception request from the UAB IT portal.

Approval / Revision History:

Revision	Approval	Revision Description	Approval Date	Effective Date
1	Curt A. Carver Jr., Ph.D., VP of IT	Initial document	7/1/2017	8/1/2017
2	Curt A. Carver Jr., Ph.D., VP of IT	• Added related documents • 4 – Clarified a number of concerns with Vuln Scanning and Penetration Testing requirements. Added credentialed scanning requirements. • 6 - Changed names of tools utilized • 7 - Increased remediation times • 8 - Referenced change management process	3/9/2020	3/9/2020
3				
4				