UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Security Officer

Responsible Office
Information Technology Services

STANDARD

UNC-Chapel Hill Information Technology Standard for Vulnerability Management

Purpose and Background

Many universities have experienced data breaches that have had significant negative consequences for those institutions and their affiliates. In many cases, an effective vulnerability management program could have identified and remediated the underlying vulnerabilities which allowed the breach to occur.

Audience

All UNC-Chapel Hill Affiliates responsible for systems requiring vulnerability scanning under the UNC-Chapel Hill Information Security Controls Standard.

Standard

This standard is intended to represent a minimum baseline for managing vulnerabilities on UNC-Chapel Hill systems required by the UNC-Chapel Hill Information Security Controls Standard to be scanned for vulnerabilities. Business units may implement stricter standards for their systems or for systems making trusted connections to theirs. This standard may not address every requirement for remediation. Risk assessments, access control processes, and other requirements may determine that additional remediation beyond this standard is required for a particular system.

Scanning and Mitigation:

In compliance with the University's Vulnerability Management Policy, all computing devices covered by the UNC-Chapel Hill Information Security Controls Standard which are required by that standard to be scanned for vulnerabilities, must mitigate those vulnerabilities according to this standard.

Systems working with University Sensitive Information (SI) or that serve mission-critical computing purposes must be remediated and mitigation of any detected vulnerabilities will be either in accordance with the Remediation and Mitigation standards below or must have a documented approved exception from the Information Security Office (ISO).

University departments must develop and adhere to procedures for vulnerability management, including the regular scanning of systems. Vulnerability management procedures must also address remediating detected vulnerabilities, including timely patch and configuration management and effective change management procedures.

Un-remediated Systems:

The Chief Information Security Officer (CISO) has the authority to take action, as needed, to ensure that un-remediated systems do not pose a threat to University resources.

The CISO shall communicate directly with system owners in advance regarding any actions 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. In the absence of high-risk circumstances (i.e., a vulnerability being exploited currently 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 Liaisons (ISL), the Carolina Technology Consultants (CTC), or other mass-communication paths regarding necessary remediation actions.

High-impact actions such as blocking systems from the campus data network shall require the joint approval of the CISO and Chief Information Officer (CIO) (or in their absence, CISO/CIO delegates) and may involve communication with the department head, Dean or appropriate Vice Chancellor.

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 network. The CISO must consider the risk sufficiently mitigated prior to authorizing network service restoration.

Specific guidelines working within the framework of this standard regarding un-remediated systems may be developed in collaboration with internal University committees or programs working with the CISO to balance the requirements of this standard with potential negative impact to the mission of the University.

Vulnerability Classifications:

The following classifications describe the severity levels that can be assigned to a vulnerability. UNC-Chapel Hill makes available, at ITS expense, Qualys vulnerability management solutions. Although other vulnerability management systems may be

approved by the CISO, the severity classification system described below is the system used by Qualys (https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_levels.htm) :

> **Level Five: Urgent** denotes a vulnerability through which an intruder can easily gain control at the administrator level of any affected host. This class of vulnerabilities poses the highest risk for a system-wide compromise of the UNC-Chapel Hill network.
>
> **Level Four: Critical** denotes a vulnerability through which an intruder could gain access to the host at the administrator level or could possibly access Sensitive Information stored on the host. While this class of vulnerabilities is extremely serious, the risk of a breach or compromise is not as urgent as with a critical vulnerability.
>
> **Level Three: 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.
>
> **Level Two: Medium** 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.
>
> **Level One: Minimal** denotes vulnerabilities that do not pose an immediate threat to the host or the UNC-Chapel Hill 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 to 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.

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 in process, relevant administrators must be working diligently toward approval. Remediation and mitigation should be prioritized based on the degree of associated severity. For vulnerability remediation, Administrators should

perform effective testing and follow reasonable change management procedures to ensure patch installation for affected systems.

Remediation and Mitigation Descriptions:

After a vulnerability is detected, and a fix is available, a timeline for remediation begins. For level 4 (Urgent) and level 5 (Critical) vulnerabilities for systems holding sensitive information and those systems designated "Mission Critical," exceptions to the timeline must be granted by the CISO or delegate. For all other systems, departments are responsible for managing timeline exceptions on a case-by-case or blanket-exception (exemplar) basis and may establish appropriate procedures for managing those vulnerabilities. Please note that in rare instances the CISO or delegate may determine that a specific vulnerability poses unacceptable risk to other University systems, in which case remediation may be required on a timeline determined by the CISO or delegate.

Timelines:

Level 4 & 5 vulnerabilities for SI/MC systems: Remediation is required within 30 days unless a documented exception request has been submitted to the ISO to "halt the clock," and that exception is in process and being worked diligently by relevant administrators or has been approved. ISO-approved exceptions will document the specific remediation timeline requirements for that system (or set of systems for a blanket or "exemplar" exception) or document compensating controls if remediation is not feasible, not necessary, or not appropriate.

In some cases, departments with a high volume of systems encounter patch failures near the end of the timeline. Departments with large enterprise systems may have the need for extended test periods for patches before remediating production systems. Patches occurring "out of band" (e.g. those occurring outside of a scheduled patch-release) may be impossible to schedule for all systems within 30 days. Some systems have extremely narrow or infrequent service downtime windows due to business requirements. These and other circumstances result in a small percentage of campus systems which are not remediated within 30 days. Such systems must apply for and diligently pursue exceptions with the ISO.

Level 4 & 5 vulnerabilities for other systems: IT staff must review and assess each vulnerability. Remediation is required within 30 days unless the department IT Director (or delegate) or Information Security Liaison (as determined by the Department) responsible for that system has determined that an exception situation exists.

Level 2 & 3 vulnerabilities for all SI/MC systems: IT staff must review and assess each vulnerability reported. Remediation is required within 90 days unless the department IT Director (or delegate) or Information Security Liaison (as determined by the Department) responsible for that system has determined that an exception situation exists.

Level 1 vulnerabilities for all systems: IT staff must review and assess each vulnerability reported. Remediation is required within 90 days unless the department IT Director (or delegate) or Information Security Liaison (as determined by the Department) responsible for that system has determined that an exception situation exists.

Exceptions:

Exceptions for level 4 & 5 vulnerabilities to SI/MC systems may be submitted for approval by the CISO or delegate via Remedy help ticket (unless a system is registered with SAI and an SAI portal submission has already been completed). Departmental IT Directors (or delegates) or Information Security Liaison (as determined by the Department) can approve exceptions for all other vulnerabilities. Departments must create and retain documentation regarding exceptions approved by departmental staff.

All exception review (whether departmental or ISO) shall include consideration of: compensating controls in place, impact on organizational mission, any recommendations from campus resources related to a specific vulnerability or specific system's remediation, technical obstacles to remediation, operational obstacles to remediation, any other environment-specific information provided in the request. Generally speaking, if cost is the obstacle to remediation, cost to remediate must be prohibitive to the department and the appropriate data steward and responsible departmental authority must sign off in order for an exception to be considered.

For ISO exceptions, during review of the documented exception request by the CISO or delegate, the remediation timeline will be on hold (following procedures established by the ISO). However, depending on risk to the University, the CISO may determine that the timeline may not be abated. Non-SAI-portal exceptions (submitted via Remedy ticket to the ISO) may be for individual systems, or may be "exemplar" exception requests. The ticket should include narrative description of the system(s) to be covered and the remediation strategy and/or compensating controls for the system(s). Examples of exemplar requests include: non-standard systems such as appliances; groups of systems for which longer patch-testing timelines are required; systems out of support by the OEM for which alternative ongoing support has been procured.

If an exception is not granted, the remediation timeline resumes. However, the department may appeal the denial to the CIO; the CIO may request involvement of the affected Department Head. If the result of non-remediation would be removal of the system from the network or other drastic action, the CISO shall seek approval of the CIO to take such action.

For department-level exceptions, departments may set up and document exception procedures in any way they deem appropriate. Review and assessment of all vulnerabilities is always required. Involvement of the Business Manager in analysis of level 3-5 vulnerabilities is strongly recommended. Exceptions may be granted on a case-by-case basis, or as blanket exceptions by vulnerability, vulnerability level, for groups of similar systems, for systems sharing the same set of compensating controls, or in other configurations as determined by the department. Departmental staff should feel free to seek consultation from the ISO.

ISO-Approved blanket exceptions:

Recognizing that it may not be feasible for some systems (such as cloud applications not owned by the University) to follow the Standard for Vulnerability Management, specific vulnerability management practices may be identified for such systems in any applicable risk assessment.

Additional University-wide blanket exceptions may be added to the standard as they occur, but the ISO may communicate these exceptions through other means.

Compliance

Failure to comply with this standard may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this standard may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with UNC-Chapel Hill.

Violation of this standard may also carry the risk of civil or criminal penalties.

Roles and Responsibilities

Chief Information Security Officer: Compliance with this standard throughout the University. Adjudicates and escalates exceptions to policy.

Administrators/IT Managers: Ensure user and systems administrator adherence to this standard including adherence to heightened standards for administrator vulnerability management.

Definitions

Administrator (System or Application): Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, appropriate security parameters, and sound implementation of established information security best practices and University policy and procedures.

Computing Devices: For the purposes of this standard, computing devices include all information technology hardware capable of processing and storing data, including, but not limited to, servers, workstations, laptops, and other mobile devices in use at UNC-Chapel Hill.

Mission-Critical Resource: Includes any resource that is critical to the mission of the University. Typical mission-critical resources have a maximum downtime of three consecutive hours or less. The owning business unit determines whether a resource is mission-critical. Once designated as mission-critical, information security policies and standards apply in an effort to assure that the resource remains available. If a business unit does not designate a source as mission-critical, that resource may not be a priority for restoration of services in the event of an incident or outage.

Sensitive Information: Sensitive information is defined here as information that is protected against unwarranted disclosure. See the reference links in the Related Documents section for assistance in recognizing and managing sensitive information at the University.

Related Documents

UNC IT Vulnerability Management Policy

UNC-Chapel Hill Information Security Controls Standard

Contacts

Subject	Contact	Telephone	Online/Email
Standard Questions	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Request Information Security Consulting	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Report a Violation	UNC ITS Information Security Office	919-962-HELP	N/A
Assistance with Sensitive Information	UNC Privacy Office	919-962-HELP	privacy@unc.edu

Informational Resources:
System Administration Initiative

Sensitive Information: UNC Help & Support: What is Sensitive Information, UNC Help & Support: Securing Sensitive Information and UNC Help & Support: Examples of Sensitive Information

Document History

Effective Date: Previous Standards were incorporated in Vulnerability Management Policy dated 30 June 2010. Standalone Standard effective 2/18/2016, signed by the Chief Information Security Officer

Revised Date: