Vulnerability Management Policy

Policy Statement

Computing devices storing the University’s Sensitive Information (as defined below) or Mission-Critical computing devices (as defined below) must be fully scanned at least monthly, and preferably weekly, for vulnerabilities. Any detected vulnerabilities must be remediated in accordance with the specific timeframes described in this Policy.

To ensure that scans are comprehensive and accurate, scans should be performed by users logged in with Administrator-level access on the respective computer device.

Scope

This Policy establishes a framework for identifying and promptly remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities.

Audience

It is imperative that all System or Application Administrators adhere to this Policy.

This policy applies to all Users (faculty, students, staff, temporary employees, contractors, outside vendors, and visitors to campus) who have access to information or data that constitutes the University’s Sensitive Information or who have responsibility for Mission-Critical computing devices. Users in this group must be aware of University requirements regarding scanning and patching. IT personnel are responsible for assisting the Users they support with compliance with this policy.

Compliance

Failure to adhere to this policy 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 Policy will be referred to the Honor System. Contractors and vendors who fail to adhere to this
Policy may face termination of their business relationships with the University. Violation of this policy resulting in the unauthorized disclosure of Protected Health Information or Personal Identifying Information (see the definition of “Sensitive Information” below) may also carry the risk of civil or criminal penalties.

Definitions

**Administrator (System or Application):** Generally, a University staff member who manages and maintains computer devices for the University and is authorized to have access beyond that of an end user.

**Critical Asset:** Any system that serves or supports a Mission-Critical function or that stores or processes Sensitive Information.

**Mission-Critical Resource:** Includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.

**Sensitive Information:** Sensitive Information includes all data, in its original and duplicate form, which contains:

- “**Personal Identifying Information,**” as defined by the [North Carolina Identity Theft Protection Act of 2005](https://www.ncleg.gov/EnactedLegislation/Statutes/ByYear/2005/Chapter162). This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources,
- “**Protected Health Information**” as defined by [HIPAA](https://www.hhs.gov/hipaa),
- Student “education records,” as defined by the [Family Educational Rights and Privacy Act (FERPA)](https://www2.ed.gov/policy/gen/guid/ferpa/index.html),
- “Customer record information,” as defined by the [Gramm Leach Bliley Act (GLBA)](https://www.consumerfinance.gov/glossary/),
- “Card holder data,” as defined by the [Payment Card Industry (PCI) Data Security Standard](https://www.pcisecuritystandards.org/).
Security Standard.
- Confidential “personnel information,” as defined by the State Personnel Act, and
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act.

Sensitive data also includes any other information that is protected by University policy or federal or state law from unauthorized access. Sensitive Information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, social security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.

Reason for Policy

Many colleges and universities have experienced data breaches that have had significant consequences for these institutions and for their students, employees, alumni, and patients. In many cases, an effective vulnerability management program could have identified and remediated the underlying vulnerabilities, which allowed the breach to occur.

Detection of Vulnerabilities and Remediation

University departments must develop and adhere to procedures for vulnerability management, including the regular scanning of systems storing or processing Sensitive Information and Mission Critical systems.

In particular, systems storing the University’s Sensitive Information or systems considered to be Mission Critical for UNC-Chapel Hill must be fully scanned for vulnerabilities at least monthly and preferably weekly, using scanning software approved by the Information Security Office (445-9393 or security@unc.edu). The Information Security Office (ISO) makes a number of shared vulnerability assessment tools available to customers for scanning desktops and servers, web applications, and databases.

To ensure that scans are comprehensive and accurate, scans should be performed by Users logged in with Administrator-level access on the respective computer device.
Vulnerability management procedures should also address remediating detected vulnerabilities, including timely patch management and testing change management procedures. It is recommended that changes be documented in writing for future reference.

Any detected vulnerabilities must be remediated in accordance with the specific timeframes described below.

For purposes of remediation and mitigation, the severity rating assigned by the vulnerability scanning tool used by ISO will serve as the basis for classifying a vulnerability unless specifically indicated as an exception by the ISO. The following classifications describe the severity levels that can be assigned to a vulnerability.

Vulnerability classifications for desktops and servers:

**Critical** 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.

**High** 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.

**Medium** 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.

**Low** 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. These vulnerabilities may often be mitigated through firewall and intrusion prevention systems that limit access by intruders from outside the University network. 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, either related to missing patches or improper configuration, must be remediated within the timeframes specified below based on the degree of associated severity. For vulnerability remediation, System Administrators should perform appropriate testing and follow existing change-management procedures to ensure proper patch installation for affected systems.

<table>
<thead>
<tr>
<th>Remediation and Mitigation Table</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Level</strong></td>
</tr>
<tr>
<td>After detection, remediation required within less than</td>
</tr>
<tr>
<td>critical</td>
</tr>
<tr>
<td>high</td>
</tr>
<tr>
<td>medium</td>
</tr>
<tr>
<td>low</td>
</tr>
</tbody>
</table>

**Related Documents**

- Information Security Policy and related Procedures and Standards
- Password Policy for System and Application Administrators
- General User Password Policy

**Contacts**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>FAX/E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report a Violation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Information Security Consulting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**History**
Effective Date:  
Revised Date: 6/30/10  
Next Review Date: