UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

POLICY

UNC-Chapel Hill Information Technology Vulnerability Management Policy

Policy Statement

Computing devices covered by the UNC-Chapel Hill Information Security Controls Standard which require vulnerability scanning are covered by this policy. Any UNC-Chapel Hill Affiliate with responsibility for a covered computing device must ensure that detected vulnerabilities are remediated in accordance with the specific timeframes described in the UNC-Chapel Hill Standard for Vulnerability Management unless an approved exception exists.

The Chief Information Security Officer (CISO) has the authority to take action, with appropriate communication with system owners in advance, to ensure that un-remediated systems do not pose a threat to University information resources. Drastic actions such as blocking systems from the campus data network shall require the joint approval of the CISO and CIO (or in their absence, CISO/CIO delegates). In support of this policy, the CISO shall publish needed controls, standards, and procedures. Such standards shall include processes for determining remediation exceptions for systems and types of systems based on (at least): compensating controls, prohibitive technical and operational obstacles, or other system-specific circumstances.

Specific guidelines regarding compensating controls, developed in collaboration with internal University committees and the CISO, may make exceptions to the requirements specified in the UNC-Chapel Hill Standard for Vulnerability Management. These exceptions will balance the requirements of this standard with potential negative impact to the mission of the University.

Purpose and Background

This policy applies to all UNC-Chapel Hill Affiliates who have responsibility for covered computing devices.

Audience

This policy applies to all UNC-Chapel Hill Affiliates who have responsibility for covered computing devices.

Compliance

Failure to comply with 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 may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

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

Roles and Responsibilities

Chief Information Security Officer: Compliance with this policy throughout the University. Adjudicate and escalate exceptions to policy.

Administrators/IT Managers/Information Security Liaisons (ISL): Ensure users and systems administrators adhere to this policy and supporting guidelines and standards or to escalate to University management.

Other Affiliates: Cooperate with Administrators/IT Managers/ISLs with respect to scheduling of system downtime, service outage windows, providing access to systems to facilitate vulnerability remediation, and maintaining awareness of vulnerability status of systems for which you are responsible.

Definitions

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

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

UNC-Chapel Hill Affiliate: UNC-Chapel Hill faculty, staff, students, retirees, contractors, distance learners, visiting scholars and others who require UNC-Chapel Hill resources to work in conjunction with UNC-Chapel Hill.

Related Documents

UNC-Chapel Hill Information Security Controls Standard

UNC-Chapel Hill IT Standard for Vulnerability Management

Contacts

Subject	Contact	Telephone	Online/Email
Policy 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: June 30, 2010, Chief Information Officer

Revised Date: February 18th, 2016, Chief Information Officer. Added exception section, CISO authority clarification.