Policy Title:	Vulnerability Management
Policy Number:	UNIV-484
Revision Date:	February 2023
Policies Superseded:	None
Policy management Area(s):	Information Technology Services

SUMMARY:

Vulnerability management is an essential component of information security programs and is critical for Coastal Carolina University to address responsibly in compliance with federal and state laws and policies. The purpose of this policy is to ensure the establishment of a process to effectively conduct vulnerability assessment and scanning of networked assets in order to determine potential vulnerabilities within the University technology infrastructure and information system components, which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data. In addition, this policy ensures that the remediation of identified vulnerabilities will provide appropriate protection against threats (such as cyberattacks, denial of service, malware, etc.) that could adversely affect the security of the information system or data entrusted on the information system.

POLICY:

I. DEFINITIONS

A. University data or information covers any item of information that is collected, maintained, and/or used for the purpose of carrying out the business of the University in accomplishing its mission. University data may be stored either digitally or on paper in multiple formats (e.g., text, graphics, sound, etc.).

II. RESPONSIBILITIES AND ROLES

A. The development, implementation, and execution of the vulnerability management process is the responsibility of the ITS-Information Security Area in collaboration with network and assigned IT staff, plus other impacted units as directed by the Associate Vice President for Information Technology and Chief Information and Technology Officer (CITO).

III. SCOPE

A. This policy applies to all University colleges, departments, administrative units, and affiliated organizations that use University information technology resources to create, access, store, or manage University data. The policy also applies to all faculty, staff, students, affiliates, prospective students, contractors, sub-contractors, and others who are authorized to interact with the University systems and processes. This policy is not intended to replace other existing University policies and procedures relating to the use or maintenance of sensitive information, such as the UNIV- 483 Data Privacy, Classification and Protection Policy, the UNIV- 480 Payment Card Industry Data Standard Security (PCI-DSS) policy, and/or the UNIV- 450 General Usage - Network and Computing policy.

IV. VULNERABILITY MANAGEMENT

A. Vulnerability Assessment

1. Testing/scanning for vulnerabilities in information systems (including applicable hosted applications) shall be conducted at least annually and whenever new vulnerabilities that could potentially affect the information systems /applications are reported.
2. Access to vulnerability scanning tools and vulnerability reports must be controlled and limited to privileged and authorized individuals. Centrally managed vulnerability assessment solutions will be utilized; use of any other network-based tools to scan or verify vulnerabilities must be approved in writing by the AVP for Information Technology/CITO.
3. The University must analyze vulnerability scan reports and results from security control assessments and remediate identified vulnerabilities in accordance with conducted IT risk assessments.
4. Periodic or continuous vulnerability assessment scans will be performed on all network assets deployed on the University IP address space.

B. Flaw Remediation and Patch Management

1. The University must conduct penetration testing exercises on an annual basis, either by using internal resources or by employing an independent third-party penetration team to identify, report, and correct information system flaws.
2. The University must establish a formal process to test and patch software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.
3. The University must install the latest stable versions of applicable security software and firmware updates.

4. The University must establish a patch cycle (e.g., system maintenance windows) that guides the normal application of patches and updates to systems.

Related information and policy links include, but are not limited to:

UNIV- 449 University Website policy
UNIV- 480 Payment Card Industry Data Standard Security (PCI DSS) policy
UNIV- 450 General Usage - Network Computing policy
Data Classification Schema and Guidelines