Vulnerability Management

I. INTRODUCTION

This policy establishes a vulnerability management program to systematically catalog and manage vulnerabilities, as required by the Information Security policy.

II. POLICY OVERVIEW

All systems and software have inherent security weaknesses or vulnerabilities. These vulnerabilities create opportunities for exploitation by criminals and other adversaries, resulting in unauthorized access to a system or network.

The University's vulnerability management policy is designed to detect, document, and address vulnerabilities in software and system configurations in a consistent, efficient, and cost-effective manner. Vulnerability management consists of the following activities:

- Identifying, categorizing, and tracking assets
- Scanning and reporting assets with known vulnerabilities
- Ranking risks
- Mitigating risks
- Following up with remediation scanning.

III. POLICY PROCESS

A. Requirements

1. The University shall maintain an inventory of all vulnerabilities discovered on its network and computer systems.
2. The University shall use a vulnerability scanning tool to perform network and system vulnerability scans.
3. Any device that has an IP address and is connected to the University’s network shall regularly be scanned for vulnerabilities.
4. Internal and external scans shall be performed on a weekly basis or when significant changes occur in the network.
5. Vulnerabilities shall be categorized and prioritized according to severity. See the Vulnerability Rating section for the severity rating system.
6. Vulnerability scan reports must be analyzed and reviewed at least monthly; new vulnerabilities must be researched, evaluated, and a plan must be developed to address them in an efficient and timely fashion.
7. The University will address Critical and High severity vulnerabilities where technically possible. Where not technically feasible or impractical, InfoSec shall provide IT management and the Information Owner with alternative security risk mitigation to address the risks. In addition,

while addressing Critical and High severity vulnerabilities, the University will review lower severity vulnerabilities and address these where feasible, practical and prudent.

8. The University mitigates vulnerabilities based on a combination of the following activities:
    a. Patching vulnerabilities
    b. System configuration management
    c. Implementing compensating controls
    d. Lifecycle management
9. When available, the University will evaluate the use of temporary fixes, workarounds, and/or compensating controls to reduce the immediate risk posed by vulnerabilities.
10. The University must validate that vulnerabilities have been remediated.

B. Roles and Responsibilities

1. The Information Security Office (ISO) is responsible for implementing and running the vulnerability management program.
2. The ISO will work Information Custodians to address the vulnerabilities es discovered.

IV. DEFINITIONS

- **Vulnerability** - Vulnerabilities are flaws in a computer system that weaken the overall security of the device/system. Vulnerabilities can be weaknesses in either the hardware itself or the software that runs on the hardware. Vulnerabilities can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e., perform unauthorized actions) within a computer system.
- **Compensating Control** – a security measure that is designed to satisfy the requirements or some other security measure that is deemed too difficult or impractical to implement.
- **Patching** - A patch is a software update to comprised code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package.
- **Remediation** – is an effort that resolves or mitigates a discovered vulnerability.

Vulnerability Rating

The University uses Tenable's vulnerability scanning solution to identify and manage vulnerabilities. To quantify the risk and urgency of a vulnerability, Tenable assigns all vulnerabilities a severity (Info, Low, Medium, High, or Critical) based on the vulnerability's static CVSSv2 or CVSSv3 score and a dynamic Tenable-calculated Vulnerability Priority Rating (VPR).

Severity	CVSS Range	VPR Range
Critical	CVSS score between 9.0 and 10.0	9.0 and 10.0
High	CVSS score between 7.0 and 8.9	7.0 and 8.9
Medium	CVSS score between 4.0 and 6.9	4.0 and 6.9
Low	CVSS score between 0.1 and 3.9	0.1 and 3.9
Info	CVSS score of 0	

The key drivers for priority rating

- Age of vulnerability – The number of days since the National Vulnerability Database (NVD) published the vulnerability
- CVSS impact score – The NVD-provided CVSS impact score for the vulnerability
- Exploit Code Maturity – The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.
- Product Coverage – The relative number of unique products affected by the vulnerability: Low, Medium, High or Very High
- Threat Sources – A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays No recorded events.
- Threat Intensity – The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: Very Low, Low, Medium, High, or Very High.
- Threat Recency – The number of days (0-180) since a threat event occurred for the vulnerability.