Area of Responsibility:	Information Technology
Responsible Contact:	Chief Information Officer
Policy Identification:	Vulnerability Management Policy
Effective Date:	07/01/2021
Last Revised:	04/26/2022

POLICY

The purpose of this policy is to ensure a higher level of security to the University's IT Resources provided through vulnerability management. In addition, this policy will outline the steps in IT vulnerability management adhering to the Vulnerability Management Policy, to ensure that appropriate tools and methodologies are used to assess vulnerabilities in systems or applications, and to provide remediation.

This IT policy, and all policies referenced herein, shall apply to all members of the University community, including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

PROCEDURES

1. All patches or configuration changes must be deployed to university-owned or managed IT Resources per the timeframe stated in the Vulnerability Management Procedure.
2. Information Technology provides approved standard tools and methodologies for vulnerability assessments.
3. All IT Resources must be part of a patch management cycle as defined in Patch Management Policy.
4. Application and system owners are responsible for the assessment and remediation of IT Resources under their management or supervision.
5. If a solution or remediation is not available to address a vulnerability, IT must approve any compensating or other mitigating controls.
6. Application and system owners must have a written and auditable procedure addressing remediation steps.

Definitions

Compensating control is a data security measure designed to satisfy the requirement or other security measures deemed too difficult or impractical to implement.

IT Resources include computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

A patch is a software update comprised of code inserted (i.e., patched) into an executable program code. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:

1. Upgrading software
2. Fixing a software bug

3. Installing new drivers
4. Addressing new security vulnerabilities
5. Addressing software stability issues

Patch management cycle is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Patch management occurs regularly as per the Patch Management Procedure.

Remediation is an effort that resolves or mitigates a discovered vulnerability.

Vulnerability management is the practice of identifying, classifying remediating, and mitigating vulnerabilities.

Policy Disclaimer Statement
Deviations from policies, procedures, or guidelines published and approved by the IT Director may only be done cooperatively between IT Director and the requesting entity with sufficient time to allow for appropriate risk analysis, documentation, and possible presentation to authorized University representatives. Failure to adhere to cybersecurity written policies may be met with university sanctions.

Vulnerability Management Procedure Steps
Procedure Steps

The following phases must be followed to comply with this procedure:

Discovery Phase

Vulnerabilities are identified on IT Resources

Prioritization Phase

Discovered vulnerabilities and assets are reviewed, prioritized, and assessed using results from technical and risk reports.

Planning Phase

Mitigation efforts are devised

Remediation Phase

Vulnerabilities are addressed

Validation Phase

Successful remediation measures are determined by subsequent analysis

Discovery Phase

Tools that are approved by IT may be used to assess systems or applications for vulnerabilities.

Prioritization Phase

- Address confirmed severity levels: Critical, Severe, or medium findings in Vulnerability Management solution.
    - Address all severity levels findings in Vulnerability Management solution.

    - Application and system owners must address content security policy configurations, application header configurations, or certificate configurations (e.g., self-signed, weak encryption) findings.

- If there are conflicting severity levels among the tools, consult IT for guidance to prioritization.

Planning Phase

Remediation for the vulnerability findings should be mitigated and validated within the following timeframe from initial discovery (first detected date of vulnerability on respective IT Resources):

- Within 30 Days:
    - All Critical findings (should have been considered during the development process)
- Within 60 Days
    - Confirmed severity level 3
    - Medium and low severity levels

IT may identify findings not directly in line with the vulnerability assessment tools and may need to be addressed outside the noted days mentioned above.

Remediation Phase

System and application owners must do one or more of the following:

1. Deploy mitigating control with IT approval
2. Deploy patches
3. Upgrade
4. Remove or discontinue the use of the IT Resource
5. Deploy configuration changes

Validation Phase

1. Deploy the risk management assessment
2. System and applications owners must confirm the vulnerability no longer appears within the discovery tool.
3. If remediation has taken place, and the change is not reflected in a validation scan or deemed not applicable to the system, the application or system owner is responsible for letting IT know via email at Helpdesk@vuu.edu (e.g., if mitigating controls were implemented, vulnerability is a false positive).

Depending on the nature of an OS or application deployed, IT may leverage alternative assessment tools or methodologies to determine vulnerabilities.

SUPPORTING DOCUMENTS (if applicable)

GLOSSARY

Documented Approvers:

_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**