Procedure: Vulnerability Management	
Issue Date: 1/1/2023	Procedure Number: Proc - 02
Revision Number: 1.1	NIST Control: Security Assessment and Authorization, Risk Assessment, Configuration Management, System, and Information Protection
Revision Date: 1/1/2023	Owner: Director of Information Technology

Contents

1. Overview

This Vulnerability Management Procedure details Kentucky Wesleyan College's processes for identifying, assessing, and remediating vulnerabilities. Vulnerabilities are security weaknesses that can be exploited by criminals and other adversaries. Vulnerability management can prevent unauthorized access to a system or network and prevent theft of Confidential Information. This allows college to avoid regulatory, financial, or reputational impact.

2. Scope

This procedure applies to all Information Technology assets owned or managed by Kentucky Wesleyan College, including but not limited to servers, workstations, desktops, laptops, routers, switches, firewalls, security devices, storage and other appliances and devices.

3. Roles and Responsibilities

The following table details the roles and responsibilities that have been assigned by Kentucky Wesleyan College.

Role	Responsibilities
Dir. Of IT / vCISO	Are the owner of the vulnerability management process. Designs the process and ensures it is implemented as designed.
Dir. Of IT / vCISO	Are responsible for configuring the vulnerability scanner, scheduling the various vulnerability scans and other processes for detecting vulnerabilities.
Dir. Of IT / vCISO Managed SOC	The Managed SOC is responsible for the asset scanning. Upon notification from Managed SOC, this role should decide whether the risk associated with identified vulnerabilities are mitigated, transferred, or accepted.
IT Team	The IT Team is responsible for: • Compiling and maintaining monthly reporting metrics. • Planning and implementing remediation actions. • Working with vendors to obtain application patches when vulnerabilities are discovered. • Patching installation for server systems, including operating system and application patches. • Working with faculty, staff, and students when problems arise from patching test systems, or application vendors that do not support the latest patches for their applications.

Role	Responsibilities
	• Directing faculty, staff, and students to patch exception form when patches cannot be applied. • Maintaining a working knowledge of patches that are deployed in the respective areas.
Dir. Of IT / vCISO	• Monthly review of server patch compliance. • Monthly review of patch exceptions. • Work with systems owners with systems on the exception list.
Dir. Of IT / vCISO	• Weekly review of vulnerability scanning results. • Monthly review of patch exceptions. • Working with IT Infrastructure to apply appropriate security measures to systems that cannot be patched. • Maintaining a working knowledge of patches that are deployed in the respective areas.
IT Team	• Working with vendors to obtain application patches when vulnerabilities are discovered in system's supported by team. • Monthly testing of patches applied to servers of application's supported by team.
IT Team	• Workstation patches are applied automatically from vendors. • Other applications, for example, CAMS, BrightSpace, etc., are installed manually.

4. Information Security Standards

This procedure addresses the following Information Security Standards:

Control Family	NIST Control Number
Configuration Management	CM-3, CM-4, CM-6,
Program Management	PM-14
Risk Assessment	RA-5
Security Assessment and Authorization	CA-1, CA-8,
System and Service Acquisition	SA-5
System and Information Integrity	SI-2, SI-3, SI-6, SI-7, SI-8

5. General Standards

The following standards must be considered to implement an effective vulnerability management program:

- To identify potential vulnerabilities, internal and external scans of the college's Information Systems will be conducted at least quarterly, and/or after any significant change to the network.
- In addition to typical system scans, Application Scans must address missing software patches and common coding vulnerabilities. Some of which include, but not limited to:
    - Injection flaws (e.g., SQL injection, OS Command Injections, LDAP, and XPath injection flaws)
    - Buffer overflows
    - Insecure cryptographic storage
    - Winsecure communications
    - Improper error handling
    - Cross-site scripting (XSS) and Cross-site request forgery (CSRF)
    - Improper access control (e.g., insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to function)
    - Broken authentication and session management
    - Publicly known vulnerabilities, such as those identified by the Common Vulnerabilities and Exposures (CVE) database and the National Vulnerability Database (NVD)
        - https://cve.mitre.org/
        - https://nvd.nist.gov/
- Regular tests of security controls must be executed to verify that they are running as expected. This includes verifying firewall rules are blocking traffic, network policies are restricting traffic as designed, etc.

6. Vulnerability Scanning

6.1 Scanning and Testing Frequency

Category	Type	Frequency
Scanning	Internal Authenticated	Quarterly
	External	Quarterly

Category	Type	Frequency
	Ad-hoc	As Needed, Upon Significant Infrastructure or Application Change
Penetration Testing	Application	Annually
	Network (Internal & External)	Annually
	Physical	As of date of last revision, risk not warranted
	Social	Annually
	Wireless	Annually
	Ad-hoc	As Needed, Upon Significant Infrastructure or Application Change

6.2 Vulnerability Scanning Process

Step	Task(s)	Responsibility	Complete by
1. Determine Scope	All networked devices/assets are included in the vulnerability scan.	Dir. of IT	Predefined
2. Determine Type of Scan	Determine whether the scan will be internal or external. • Managed SOC, continuous • Nessus or other, manual		
3. Perform Initial Vulnerability Scan	Perform the vulnerability scan on the assets that were determined to be in scope in Step 1.	Dir. of IT	Predefined
4. Obtain Report	Obtain the report generated by the vulnerability scan and review any vulnerabilities that were found.	IT Team	Predefined
5. Review Vulnerabilities	Review vulnerabilities and risk level based on the severity of the vulnerability and the criticality of the asset(s) affected.	IT Team	Based on criticality
	Technically review vulnerabilities and recommendations for items that can be remediated.	IT Team	
6. Notify Impacted Personnel or Teams	Notify personnel or teams, of the vulnerabilities' impact on the systems they are responsible for.	IT Team	Based on criticality

Step	Task(s)	Responsibility	Complete by
7. Determine / Implement Remediating Actions	Determine / Implement the remediating actions that should be taken to mitigate the risks associated with the vulnerabilities that were identified (e.g., patch, configuration change, etc.). Set a remediation target date based on the risk level of the vulnerability.	IT Team	Based on criticality
8. Notify the Dir. of IT (exceptions)	Notify the Dir. of IT of exceptions to the remediating actions, and target remediation time frames, that were determined in Step 8 and that were predefined as part of this procedure (Asset criticality and risk).	IT Team	Based on criticality
9. Authorize Exceptions	Authorize all exceptions to the defined procedure.	Dir. of IT	Determined by scope of the exception
10. Perform Rescan to ensure effectiveness	Perform another vulnerability scan, using the same configuration and scope that was determined in Step 1. From a technical perspective, provide IT with an overview of the rescan to determine the effectiveness of the remediating actions.	IT Team	On demand

6.3 Vulnerability Severity Ranking

Level	Description
Information	Information only.
Low	A LOW severity vulnerability poses a small threat to the integrity of the organization's infrastructure. Examples include the use of medium-grade cryptographic ciphers or non-critical information disclosures.
Medium	A MEDIUM severity vulnerability poses a greater, but not easily exploitable threat to integrity of the organization's infrastructure. Examples include the use of low-grade cryptographic ciphers or exploits which require special privileges or access.
High	A HIGH severity vulnerability poses a significant threat to the integrity of the organization's infrastructure. Examples include the exploitation or control of critical subsystems and easily exposed public exploits.
Critical	A CRITICAL severity vulnerability poses an imminent threat to the integrity of the organization's infrastructure. Examples include vulnerabilities which, if exploited, would allow malicious code to execute and enable complete control of a host.

6.4 Asset Criticality Ranking

Risk should be assigned according to Kentucky Wesleyan College's asset inventory.

Risk Level	Category
Low	Public Information
Medium	Non-sensitive Internal Information
High	Sensitive Internal Information
Very High	Compartmentalized Internal or Regulated Information

6.5 Vulnerability Prioritization – Severity Based

Asset Criticality		Vulnerability Severity Ranking			
		Low	Medium	High	Critical
	Low	Low	Low	Low	Medium
	Medium	Low	Medium	Medium	High
	High	Low	Medium	High	Very High

	Very High	Medium	High	Very High	Very High

7. Patch Management

7.1 Patch Remediation Targets

Patches must be deployed as mentioned below based on category classification and SLAs starting from the time of the patch being released. Adherence to patch remediation targets can vary.

Device Type	Vendor defined severity	Emergency	Critical	Important	Unspecified	Low	Compliance Acceptable Level
Critical Assets		7 Days	30 Days	30 Days	60 Days	90 Days	100%
Internet facing server		7 Days	30 Days	30 Days	60 Days	90 Days	95%
Non-Internet facing server		7 Days	30 Days	30 Days	60 Days	90 Days	95%
Laptop/Desktops		7 Days	30 Days	30 Days	60 Days	90 Days	95%
Network Devices		7 Days	60 Days			90 Days	95%

Notes:

- A critical asset is a small set of assets deemed "Critical" by Information Security.
- Severity is defined by vendor for each patch.
- Unspecified patches are focused on reliability and performance updates.
- Information Security may define a patch as "Emergency" which must take priority based on risk. An example would be a critical vulnerability that is actively being exploited in the threat landscape.
- Servers include Linux, Unix, and Windows.

7.2 Configuration Remediation Targets

On many occasions, vulnerability scans will identify configuration issues in addition to missing patches. In these situations, the IT team will utilize SLAs as defined in 7.1 as technically feasible.

7.3 Microsoft Patching

Patches are to be deployed as mentioned below based on category classification and SLAs starting from the time of the patch being released as technically feasible.

Day of Month	Task(s)
2nd Tuesday	Patch Tuesday Microsoft
Based on criticality, type of patch, depending on application. Ongoing	Review Patch List for month.
	Submit Change Control for patches to be applied.
	Send patches for testing on Servers (Servers TEST OU).
	Send patches for Workstations is handled automatically
Ongoing	Test Patches on Servers, depending on applications
Ongoing	Server Patching, depending on applications
Ongoing	Active Directory Domain Controllers
Ongoing	Additional patching needed/Patch remediation
	Reporting
As required	Patch Tuesday Microsoft

7.4 Patching Process

The following process, in general, describes the patching process utilized by Kentucky Wesleyan College.

Step	Task(s)	Responsibility
1. Download	Download patches from a trusted source as soon as patches are made available.	Automatic
2. Test	Where applicable, test patches to identify any adverse effects.	IT Team
3. Change Management from the ITS Policy Handbook	Any patches being applied to a system, regardless of severity, must be submitted and approved via Change Management by the IT Team researching and determining if patch is approved. Once approved it is documented in helpdesk or via email to effected stakeholders for notification of the status of the approval.	IT Team

Step	Task(s)	Responsibility
4. Deployment	Patches will be deployed per requirements defined in 7.1	IT Team
5. Validation	Once the change has been implemented, the change will be tested.	IT Team / End User
6. Close Change Request	Once the change has been implemented and tested, close out the helpdesk ticket per Change Management process.	IT Team

8. Exceptions

8.1 Error & Exception Handling

The IT Patch Management Team is responsible for identifying and rectifying failed patch deployments. Compliance with approved patches must be verified at least on a weekly basis.

Systems and devices which are not patched via the centrally managed services must be updated as per the SLA defined in section 5.0.

When patching is not possible an exception must be obtained from the Director of Information Technology and appropriate compensating controls should be implemented to mitigate the risk. Examples include:

- Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented by the device/system/application owner and have the necessary compensating control(s) implemented.
- Patch provided by vendor creates instability within the system or a dependent system and instability outweighs the risk.

8.2 Compensating Controls

When vulnerabilities cannot be addressed, reasonable and appropriate compensating controls must be considered and implemented. Examples of additional compensating controls:

- Network segmentation.
- Access Control Lists.
- Host Intrusion Prevention Systems or other Information Security Control.

8.3 Exception Form

To document the nature of the exception and compensating controls, an Exception form is completed and approved.

- A service request ticket must be generated for the IT Team to review before the exception form is sent for signatures.
- Document the reasons for the request.
- Track the exception.
- Document the periodic review of the risk. The standard review is quarterly, unless otherwise agreed to by the Director of Information Technology.

9. Enforcement

Any personnel found to have violated this procedure may be subject to disciplinary action up to and including termination of employment.

10. Revisions

Version	Date	Author	Revisions
1.0		GreyCastle Security	Initial Draft
1.1	8/2/2022	KWC Team	Review, Approve, Publish