-->

Vulnerability Management Standard

Last Modified on 04/29/2025 3:37 pm EDT

For more details about the Information Security Office, **please visit our website**!

1. Purpose

This Standard is intended to provide high-level responsibilities and timelines for Continuous Vulnerability Management and Monitoring. It addresses both Patch Management and Vulnerability Management. This standard aligns with and adheres to Penn's Security Patching Policy.

A formalized vulnerability management (VM) process helps reduce risk for the School by acting on possible threats and minimizing their attack surface. Through a shared ownership cross-functional collaboration model, the VM process helps key stakeholders identify, and prioritize technological weaknesses that a malicious actor could use to compromise within the Wharton environment.

2. Scope

The Wharton Information Security Office (ISO) will scan for vulnerabilities of systems under Wharton's control. Upon successful completion of a vulnerability scan, the Information Security Office will produce a designation as per the security risk matrix. Contributing factors in the final risk severity calculation include, but are not limited to CVSS ratings, CVE base score range, risk ratings, threat intelligence, and vulnerability relevance to Wharton.

Systems Managed by Wharton/Penn

Wharton systems and applications across the School will follow the vulnerability management framework as detailed in this document.

Systems Owned But Not Managed by Wharton/Penn

It is the responsibility for appropriate system owners and stakeholders to ensure systems are routinely patched when appropriate. System owners should work with Wharton Computing to ensure that endpoints and solutions are managed and protected.

Vendor-Contracted Systems Not Managed by Wharton/Penn

Any vulnerability information available publicly, or from a vendor, or third party shall be reviewed and documented by Wharton ISO. It is still the responsibility for appropriate system owners and stakeholders to ensure systems are routinely patched when appropriate.

3. Vulnerability Management Standard

Wharton ISO leverages a range of vulnerability assessment tools to include dynamic application security testing (e.g., web application vulnerability scans), static application security testing (e.g., source code repository scans), software composition analysis, and vulnerability scanning (e.g., container scans, operating system scans, database scans) to achieve its mission of timely discovery and remediation of vulnerabilities in enterprise IT systems and services.

Wharton will utilize a SCAP (Security Content Automation Protocol) -compliant vulnerability scanning tool to automatically scan all systems to identify all potential vulnerabilities and system misconfigurations. Scanning occurs weekly for the public facing interfaces and for the internal servers.

Wharton will perform authenticated vulnerability scanning of relevant system components, to include operating system/infrastructure, web applications, and databases at least monthly with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

A dedicated account will be used for authenticated vulnerability scans, and not for any other administrative activities, and will be assigned to pre-defined machines at specific IP addresses.

3.1 Severity Risk Matrix

Note: Exceptions may be applicable for patching timelines during University freezes. Please collaborate with ISO.

Service owners are responsible for documenting/submitting exceptions to ISO for consideration. ISO will file a retroactive ITPC variance when an Out-of-Band, Critical, or High-Risk Security Patch is not applied within the mitigation timeframe.

Rating	Definition	Time to Mitigate
Out-of-Band (Expedited)	Publicly identifiable or Information Security declared vulnerability (active in the wild) which could compromise Information Resources or where Sensitive Data has already been exposed (e.g. allow remote access, exploitation code, etc.). There is no current control in place to protect the data. Risk Level = 10	Required 2 days after Ingest and Reporting is completed.
Critical	Immediate threat on Wharton systems. Critical risk of imminent compromise or loss of Sensitive Data from either external or internal sources. There is no control in place to protect the Data. Risk Level = 9	Required 5-7 days after Ingest and Reporting is completed.
High	Actively exploited within High Education Sector. High risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. There is only a single control, or multiple ineffective controls, in place to protect the Data. Risk Level = 7-8	Required 30 days after Ingest and Reporting is completed.

Rating	Definition	Time to Mitigate
Moderate	The risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. Controls are in place that are somewhat effective to protect the Data. Risk Level = 4-6	Recommended 60 days after Ingest and Reporting is completed.
Low	The risk of compromise or loss of Sensitive Data is possible, but not probable or an Information Resource might be used to obtain access to Sensitive Data on a different Information Resource. Risk Level 0-3	Recommended 180 days after Ingest and Reporting is completed.

Remediation of vulnerabilities, which are evaluated as **Out-of-Band** by the Information Security Office, should be prioritized System Owners and/or IT Stakeholders. System Owners and/or IT Stakeholders will jointly develop a remediation/mitigation plan and share it with the Information Security Office within 48 hours.

- System Owners and/or IT Stakeholders must review the Vulnerabilities associated with their Systems and jointly develop timely remediation or mitigation plans. They should also register for security and Vulnerability alerts from the System's vendor and review vendor patches.

- As part of the provisioning process, every System needs to be scanned for vulnerabilities prior to being put into a production environment including physical, virtual, and cloud Systems.

- The Information Security Office will regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

4. Patch Management Standard

- Wharton will deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates (or at most one major version behind) provided by the Manufacturer.

- Deploy automated software update tools in order to ensure that third-party software and firmware on all systems is running the most recent security updates provided by the software vendor.

- Updates must be first installed in test environments to test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

- Wharton will incorporate flaw remediation into the organizational configuration management process.

- Updates are installed regularly, and the vulnerability scans ensure that any needed patches not yet applied are identified and the Wharton ISO then tracks remediation.

Wharton/Penn-Managed and Third-Party-Managed Systems:

- Must be supported, up-to-date, and patched.
- Third party suppliers must be prepared to provide evidence of up-to-date patching (per Wharton minimal standards, or the vendor's evidenced patch policy).
- Timely implementation of non-security related patches should be conducted to mitigate against degradation of functionality, and/or interoperability (e.g. bugfixes, features, performance).

4.1 Patch Management Responsibilities:

- All System Owners will document and maintain patch management procedures aligning to this Wharton Vulnerability Management Standard. The Information Security Office will facilitate the vulnerability management process.
- Timeliness of patch management prioritization may be impacted by several factors, including:
- Consideration of asset classification and data affected
- Regulatory requirements and business standards
- Potential risk to the environment
- System owner patch management procedures
- Business Considerations

Note: If a business unit requires an exception from this standard, then that unit must adhere to the Wharton Exception Standard. All exceptions will be reviewed by ISO and submitted to Penn IT Policy Committee (ITPC) as variances to the Wharton Standard and Penn Policy.

All "System" Owners: Responsible for understanding, developing, and maintaining procedures in compliance with the Wharton patch management policy.

Third Parties: Responsible for providing evidence of adherence to their patch policy (or Wharton policy) - upon request.

Role	Responsibilities
Vendor	• Source of information on critical notices, vulnerabilities, exploits, malware, and threats unique to the School.

Role	Responsibilities
Information Security Office (ISO)	- Present analyses on vulnerabilities and prioritize threats and risks unique to Wharton attack vectors. - Monitor fix has been applied successfully - Facilitate review meetings - Report findings on risk register; runs compliance to ensure completion - Document and report the risk levels of Wharton/Penn-managed systems.
Program Leadership	- Accountable for ensuring Vulnerability Management standard is upheld for all systems and projects under their purview - Helps prioritize and define remediation strategy with technical leads.
Service Owner	- Technical Lead - Helps define remediation strategy - Deploys remediation/mitigation fix to affected hosts.
Wharton Leadership	- Provides oversight and governance.

5. Vulnerability Management Roles (RACI)

Stage	Wharton Leadership	ISO	Program Leadership	Service Owner	Vendor
Identify		R	I	I	R
Prioritize		R, A, C	A, I	C, I	
Patch	I	A, I	A, I	R, A, C	
Monitor		R, A, I		R, C, I	A
Lessons Learned	C, I	R, I, C	C, I	R, A, C	

RACI Matrix Key:

RACI Matrix Key:
(R)esponsible: Person whose contributions and efforts results in a tangible deliverable or completed task - "The Do'er"
(A)ccountable: Person whose approval is required before the task or activity is considered completed - "The Delegator"
(C)onsulted: Person or role whose subject matter expertise is typically required in order to complete the item - "The SME"
(I)nformed: Person or role that needs to be kept informed of the status of item completion - "Those kept up to date"

- **Wharton Leadership:** CIO
- **ISO:** Wharton Information Security Office
- **Program Leadership:** Departments, Centers, Initiatives
- **Service Owner:** Designated internal Wharton staff member(s) responsible for overseeing a specific system, application, or service.
- **Vendor:** Third party vendors and/or organizations external to Wharton.

6. Vulnerability Management Process

Stage 1	Identify
When	Security Scans reports received
Who	Wharton ISO
What	Vulnerability Scan reporting
How	Leverage industry threat intelligence to address impact and criticality in Wharton environment

Stage 2	Prioritize
When	Security scan review meetings
Who	Service Owner, Wharton ISO
What	Security provides a prioritized list of vulnerabilities for review

Stage 2	Prioritize
How	Team devises a remediation strategy

Stage 3	Patch
When	As defined in Prioritize stage
Who	Service Owner
What	Agreed upon remediation strategy is implemented
How	To be determined

Stage 4	Monitor
When	Validation of remediation efforts
Who	Wharton ISO
What	Security validated agreed upon work completed through vulnerability scanning tools. Provides tracking and monitoring from compliance. Provides monthly reporting to Wharton security leadership at least monthly. Ensure vulnerability trends are meeting expectations
How	Validation through authoritative vulnerability scans or by artifact provided by Service Owner

Stage 5	Lessons Learned
When	Quarterly, Annually
Who	Wharton Leadership, ISO
What	A comprehensive review or pending action items and trending vulnerability data
How	Team discussion