UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	Vulnerability Management Standard
Standards Number:	104
Effective Date:	3/8/24
Revised Date:	N/A
Responsible Authority:	Information Security Office
Pages:	7

ACCOUNTABILITY/APPLICABILITY:

This policy applies to all colleges, departments, units, and individuals associated with the university, including faculty, staff, students, contractors, and any external parties accessing university resources via university owned equipment. It encompasses vulnerability assessment and management, while addressing vulnerabilities introduced through remote work scenarios.

STANDARDS STATEMENT:

This Vulnerability Management Standard outlines the procedures and guidelines to manage and mitigate vulnerabilities within the university's network and systems, with a specific focus on addressing vulnerabilities introduced by remote work scenarios. This standard is designed to support UCF policy 4-002, section A, item 14. The standard covers all colleges and divisions under the university's umbrella and aims to ensure a secure computing environment that protects sensitive information, research, and operations. The policy extends to remote work environments.

BACKGROUND:

As a hub of data and innovation, the University must prioritize security in our digital age. A Vulnerability Management Program (VMP) is vital for safeguarding our intricate digital ecosystem.

Benefits of a VMP:

1. **Data Security:** Protects sensitive student and research data.
2. **Upholding Reputation:** Averts breaches that could damage the university's standing.
3. **Regulatory Adherence:** Ensures compliance with data protection mandates.
4. **System Efficiency:** Ensures optimal system performance and user experience.
5. **Cost-Effectiveness:** Proactive vulnerability management reduces breach-related expenses.
6. **Educational Standard:** Sets cybersecurity examples for students.

Risks of Overlooking a VMP:

1. **Data Breaches:** Increased risk of unauthorized data exposure.
2. **Financial Burden:** Fines, lawsuits, and breach mitigation costs.
3. **Reputation Impact:** Potential loss of trust from the academic community.
4. **Operational Setbacks:** Vulnerabilities may cause system outages affecting university functions.
5. **Regulatory Penalties:** Non-adherence can lead to sanctions and scrutiny.

In essence, a university's adoption of a VMP is crucial for its operational integrity, reputation, and regulatory compliance in today's digital era.

DEFINITIONS:

1. **Authenticated Scan:** A type of security scan that uses specific access credentials (like a username and password) to get detailed and precise information about a computer system's weaknesses. Think of it as a security checkup that the system 'knows' is happening.
2. **Compensating Control:** A temporary measure used to manage a security risk when the ideal solution is not currently practical. This might be due to technical challenges, or specific business or legal issues. It's like using a spare tire when you get a flat – it's not a permanent solution, but it keeps things moving for now.
1. **Consolidated University Unit:** A group of related departments or teams within the university that share the responsibility of following IT policies and rules. They work together under one management team.
2. **KEV Catalog:** A comprehensive and organized collection of information that details the known, emerging, and verified (KEV) security threats and vulnerabilities relevant to the university's information systems. This catalog serves as a reference for IT professionals and stakeholders in the university to understand and prioritize security issues. It may include descriptions of the threats, their potential impact, suggested remedies or mitigations, and the status of the university's efforts to address each issue. Think of it as a detailed, constantly updated 'security watchlist' that the university's IT team uses to protect our digital environment.
3. **Information Security Incident:** Any event where there is a real or potential threat of unauthorized people gaining access to or tampering with the university's digital information. This includes anything from hacking attempts to breaches of personal data.
4. **Internet of Things (IoT):** Devices that are connected to the internet, ranging from smart refrigerators and thermostats in a building to health monitoring devices. Basically, if it's not a computer or phone but connects to the internet, it's likely an IoT device.
5. **IT Administrator:** Technical staff member responsible for patching and maintaining IT assets.
6. **IT Assets:** These are the technology tools the university owns or manages. This includes computers, networking equipment, servers, software applications, and databases – essentially, all the tech resources used to operate and achieve the university's mission.
7. **Mitigation:** A temporary action taken to lessen the harm a security threat might cause when that threat cannot be completely removed. It's like putting up a temporary fence around a construction site to keep people safe until the work is finished.
8. **Remediation:** The process of fixing or patching a security weakness in our computer systems, networks, or software. Think of it like repairing a hole in a wall to prevent further damage.

9. **Threat:** Any situation or event that could harm the university's operations, reputation, resources, or people through unauthorized actions in our information systems. This could be anything from a computer virus to an attempted hacking.
10. **Vulnerability:** A weak spot in our computer systems, security procedures, or controls that could be exploited by a threat. It's like a weak lock on a door that a burglar might target.
11. **Tier-0** – A system with the highest level of privilege in the domain. Ability to write back to domain controllers or otherwise elevate access to domain admin.
12. **Tier-1** – A server system without tier-0 access. Most servers fall under this category.
13. **Tier-2** – An end-user facing workstation or endpoint.

STANDARDS:

1. Objectives:

- **Identify and Assess Vulnerabilities:** Utilize vulnerability assessment capabilities to identify vulnerabilities in university systems, applications, and networks, accounting for vulnerabilities arising from remote work connections.
- **Prioritize Based on Risk:** Leverage risk assessment to categorize vulnerabilities by severity, potential impact, and exploitability, considering remote work-related risks.
- **Effective Remediation:** Implement timely and effective measures to remediate vulnerabilities, addressing vulnerabilities in both on-campus and remote work settings. Prioritize remediation of vulnerabilities listed in the Known Exploited Vulnerability (KEV) catalog to reduce the likelihood of compromise by known threat actors.
- **Enhance Security Awareness:** Promote a culture of proactive vulnerability management by providing training on the vulnerability management platform, remote work security best practices and the importance of addressing KEV catalog vulnerabilities.
- **Compliance:** Ensure compliance with relevant laws, regulations, and industry standards, including remote work security measures and addressing KEV catalog vulnerabilities.

2. Vulnerability Management Process:

1. **Vulnerability Identification:** Conduct regular vulnerability assessments, considering vulnerabilities introduced by remote work connections. IT Administrators coordinate assessments in collaboration with the ISO.
2. **Risk Assessment and Prioritization:** Utilize risk assessment features to categorize vulnerabilities, factoring in remote work-related risks. Categories include Critical, High, Medium, or Low risk levels.
3. **Reporting and Communication:** Provide vulnerability assessment reports to the ISO. The ISO communicates vulnerabilities, risks, and remediation recommendations, addressing remote work vulnerabilities.
4. **Remediation Timeframes:**
    a) **Zero Day Vulnerability:** A zero-day vulnerability refers to a flaw or weakness, which is actively being exploited, in software or hardware that is unknown to the vendor or developers. These vulnerabilities should be patched as soon as one is made available.
    b) **Critical Vulnerabilities:** A critical vulnerability is a known flaw in a system that, if exploited, can have a severe impact on security, leading to potential system

compromise, data breaches, or unauthorized access. Please refer to the matrix below for remediation requirements based on system type.

c) **High Vulnerabilities:** High severity vulnerabilities are significant weaknesses that, if exploited, can cause substantial harm to a system or its data. Please refer to the matrix below for remediation requirements based on system type.

d) **Medium Vulnerabilities:** Medium severity vulnerabilities represent weaknesses that may not have as severe an impact as critical or high severity ones but could still lead to security breaches or data compromise if exploited. Please refer to the matrix below for remediation requirements based on system type.

Vulnerability Remediation Timeframe	Zero Day	Critical Exploitable	Critical	High	Medium
Tier 0	2 Days	3 Days	7 Days	2 Weeks	3 Weeks
Tier 1 - Public	2 Days	7 Days	2 Weeks	3 Weeks	4 Weeks
Tier 1 - Private	3 Days	7 Days	2 Weeks	3 Weeks	4 Weeks
Tier 2	7 Days	7 Days	2 Weeks	3 Weeks	4 Weeks

***Note:** These timeframes are from the time a patch or fix has been identified.

5 **Verification and Validation:** Verify mitigation effectiveness with assistance from IT Admins, ensuring successful resolution in both on-campus and remote work environments.

3. Responsibilities:

- **Information Security Office (ISO):** Oversee the vulnerability management program, coordinating assessments, and addressing vulnerabilities introduced by remote work. Monitor the KEV catalog and ensure prioritized remediation of listed vulnerabilities.
- **Enterprise IT:** Handles vulnerability and patch management for enterprise managed assets. Reports any security incidents to the Information Security Office.
- **Federated IT (with Enterprise Support):** Areas that receive support from enterprise IT in handling vulnerability and patch management for their assets. Reports any security incidents to the Information Security Office.
- **Distributed IT:** Areas with technical staff separate from enterprise IT that handle vulnerability and Patch Management for their assets. Reports any security incidents to the Information Security Office.
- **IT Administrators:** Conduct reviews of vulnerability management dashboard, facilitate remediation efforts, report findings to ISO, considering remote work vulnerabilities.

Task/Activity	ISO	IT Admin	System Owners	Senior Leadership	External Vendors
Identify vulnerabilities	R		C	I	C
Assess the risk of vulnerabilities	R	C	C	I	
Prioritize vulnerabilities	R	C	C	A	

Define patching or remediation strategy	R	A	C	I	
Implement patches or remediations	C	R	A		I
Verify patch or remediation implementation	R	C	C		
Monitor for recurrence or new vulnerabilities	R	C			
Report on vulnerability status	R	C	C	A	
Continuous education & awareness	R	C	C	A	

Key:

R (Responsible): *Those who do the work to complete the task.*
A (Accountable): *The person who is ultimately accountable for the task being completed. This is often a decision-maker or final approver.*
C (Consulted): *Those whose opinions are sought and have involvement in the process but are not directly responsible for executing the task. May have insight to applications and/or legacy software that could adversely be affected.*
I (Informed): *Those who need to be kept "in the loop" regarding results or decisions, but don't have an active role in the process or task.*

4. Risk Acceptance Model:

In cases where the identified vulnerabilities cannot be immediately remediated due to technical, operational, or resource constraints, a risk acceptance model will be applied. The Information Security Office will work with campus IT Administrators to review and assess the risks associated with the vulnerability and collaboratively identify the best mitigation strategy. If necessary, the Office and / or business unit may accept specific risks based on a predefined risk tolerance threshold. The ISO will maintain records of accepted risks and monitor them periodically for changes in circumstances or emerging threats.

5. Baseline Configuration and Best Practices:

The university will establish a set of baseline configurations and policies for operating systems that includes essential security configurations, patches, and updates. This baseline will serve as the foundation for secure computing across all colleges and units. Best practices, aligned with industry standards, will be applied to this baseline to ensure a consistent security posture across the university.

6. Removal from the Network:

The primary objective of the vulnerability management program is to promptly address and mitigate potential threats that could jeopardize the security of the campus network, computers, or the broader internet ecosystem. In cases where a threat is deemed significant, steps will be taken to restrict network access for the system(s) responsible for the threat. These

guidelines outline the criteria for determining when to block access and the associated procedures.

The responsibility and authority to assess the severity and urgency of network threats, as well as to initiate mitigation measures, lie with the Information Security Office (ISO). The actions taken will be guided by the level of risk posed by the threat and the potential negative impact on the university's mission if the offending system(s) remains accessible. Examples of threats that warrant invoking these procedures include:

- Excessive network activity causing significant network performance degradation.
- Unauthorized acquisition of system administrative privileges.
- Launching an attack on another computer or network.
- Unauthorized collection of confidential, private, or proprietary electronic information or communications from the network.
- Excessive overdue patches and/or vulnerable software.
- Absence or outdated status of required virus protection software.
- Receipt of ongoing complaints about inappropriate activity with no response from the relevant departmental contact.

7. College/Unit Exceptions:

Recognizing the diverse needs of each college or unit, allowances for exceptions to the baseline image and best practices are permitted, subject to approval by the college dean or unit head and the ISO. These exceptions will be evaluated based on their potential impact on security and operational requirements. If you are unable to abide by this standard or have a compliance question, please reach out to the Information Security Office at infosec@ucf.edu.

8. Security Awareness and Training:

Organize training on the vulnerability management platform, remote work security practices, the risk acceptance process, and the importance of adhering to the baseline configuration, policies, best practices, and remediation timeframes to educate college members.

9. Approval and Buy-off:

Gain approval and buy-off from each college dean, highlighting the policy's focus on addressing vulnerabilities introduced by remote work, risk acceptance, baseline configuration, policies, best practices, and specified remediation timeframes. Collaborate with deans to ensure alignment and understanding of remote work security implications.

10. Review and Revision:

Review the policy annually or as needed to address emerging threats, technology changes, and evolving remote work practices. Propose updates in collaboration with stakeholders, ensuring remote work considerations, risk acceptance, baseline images, best practices, and specified remediation timeframes. Obtain university leadership approval.

By adhering to this standard, incorporating vulnerability assessments, addressing remote work vulnerabilities, implementing a risk acceptance model, adhering to baseline configurations, policies and

best practices, and following specified remediation timeframes, the university and its colleges strengthen their cybersecurity posture, protect critical assets, and foster a secure environment for learning, research, and innovation across various work settings while accommodating specific college or unit needs.

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office)

Standards Number: 104

Initiating Office: Information Security Office

Chief Information Security Officer: *David Zambri*

Signature: David Zambri Digitally signed by David Zambri Date: 2024.03.08 10:59:18 -05'00' Date:_____