VULNERABILITY MANAGEMENT PROGRAM

Information Technology Services Standard

Executive Summary

Cybersecurity vulnerabilities are defined as security flaws in software, hardware, or configuration of information technology (IT) resources that, if exploited, would result in a negative impact to the confidentiality, integrity, or availability of FSU data, the network, or IT resources and infrastructure.

Vulnerability management includes the regular practice of identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities associated with FSU IT systems, devices, software, and the university's network.

The Information Technology Services (ITS) Standard ***Vulnerability Management Program*** establishes a minimum baseline for managing cybersecurity vulnerabilities. At their discretion, University units may adopt and implement stricter standards based upon the IT systems, data, and information they are responsible for managing.

All units are responsible for maintaining compliance with the vulnerability management standards identified in this document.

Overview

Data breaches at higher education institutions have the potential to impose significant negative consequences, including, but not limited to, identity theft, reputational damage, compromise of confidential data, and resulting legal ramifications. An effective vulnerability management program (VMP) will provide FSU with a strategic first-line of defense aimed at identifying, evaluating and remediating system and application vulnerabilities that may allow unauthorized access or malicious exploitation by intruders.

FSU Official Policies, **4-OP-H-5** and **4-OP-H-12**, require university units, information technology personnel, and system owners to properly secure university information technology (IT) systems, applications, and infrastructure; and, protect the data and information such systems utilize, house, or access. IT personnel are required to identify and document all IT resources they are responsible for managing and implement a patch management process for all such resources.

All computers and other devices capable of running anti-malware software also must employ licensed and up-to-date anti-malware software that cannot be disabled by end-users. All computers and other devices must have installed up-to-date security patches. Failure to meet these requirements may result in revocation of network access.

Unit Responsibilities

Vulnerability Identification

For devices and applications that support credentialed vulnerability scans, units are required to implement credentialed scans to ensure that scan results are accurate/complete and reduce the likelihood that certain vulnerabilities would otherwise be missed or overlooked. Appliances or other devices that are auto-updated by the vendor or not under the control of FSU shall also be monitored by units to ensure security updates are applied in a timely fashion. For questions related to credentialed scans, please contact the ISPO for additional information.

All FSU systems and applications are required to be scanned for vulnerabilities, using the ITS vulnerability scanning system, on at least a monthly basis.

Units are responsible for ensuring all of their systems are scanned monthly, reviewing the results of the scan, and determining, what, if any, additional mitigations or remediation activities are required to be implemented, based on the vulnerability's risk level described in *Vulnerability Classifications*.

Identified vulnerabilities shall either be mitigated or remediated in accordance with the timeline described in *Mitigation and Remediation Timeline Requirements*; or, shall have received documented and approved exceptions from the Information Security and Privacy Office (ISPO).

All units are responsible for developing and implementing patch management processes to apply operating system and/or application security patch updates for the IT systems, devices, and applications they are responsible for managing. Similarly, the system and application owners shall adopt and implement baseline, hardened configurations for all systems they are responsible for operating, managing, or supporting.

If units determine that credentialed scans cannot be implemented, or if there is substantial risk associated with running credentialed vulnerability scans, they are required to request an exemption using the process discussed in *Vulnerability Remediation Exemptions.*

Vulnerability Classification

ITS employs enterprise level patch management and vulnerability scanning tools that may differ slightly in terms of classification systems and/or terminology. The following vulnerability risk classifications describe severity levels that may be assigned to an identified vulnerability with an attempt to consolidate terminology used as it relates to this standard.

Sources for cybersecurity vulnerabilities information, CVSS scores, and related risks and exposures include: the **National Vulnerability Database,** which can be found at

https://nvd.nist.gov/vuln-metrics/cvss; and, the **Common Vulnerability Exposure Database,** located at https://cve.mitre.org

Critical Risk Vulnerabilities

Loss of system or data [Confidentiality | Integrity | Availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization, e.g., students, faculty, and staff. Exploit development has reached the level of reliable, widely-available, easy-to-use automated tools. Flaws could be easily exploited by an unauthenticated (or authenticated) remote attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. **Critical CVSS Base Score 9.0-10.0.**

High Risk Vulnerabilities

Loss of system or data [Confidentiality | Integrity | Availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Functional exploit code is available. The exploit code works in most situations where the vulnerability exists. These types of vulnerabilities allow local users to gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service. **CVSS Base Score 7.0-8.9.**

Moderate Risk Vulnerabilities

Loss of system or data [Confidentiality | Integrity | Availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). This rating is given to flaws that may be more difficult to exploit but could still lead to compromise under certain circumstances. These are the types of vulnerabilities that could have a critical or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect or require an unlikely configuration. **CVSS Base Score 4.0-6.9.**

Low Risk Vulnerabilities

Loss of system or data [Confidentiality | Integrity | Availability] is likely to have only a very limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would cause either no adverse effects, or, result in only very minimal adverse consequences. **CVSS Base Score 0.1-3.9.**

Patch and Configuration Management

Patch Management

Vulnerabilities that are directly related to missing security patches shall be remediated within the timeframes established under *Vulnerability Mitigation and Remediation* below. Remediation and mitigation activities should be prioritized based on the assigned vulnerability classification, the resulting exposure to the unit or University if the vulnerability was exploited.

Configuration Management

For configuration changes, system owners, and system/application administrators are responsible for performing effective testing and for following a consistent internal change management process.

Security Patch Management Requirements

System and application owner(s) and/or administrator(s) shall develop and implement a method to show vendor and 3rd party security alerts are regularly reviewed against unit configuration standards and installed and recommended or available patch levels. The output of this process shall be made available to ISPO upon request.

Vulnerability Mitigation and Remediation

The vulnerability risk mitigation and remediation lifecycle can be summarized to include three (3) distinct stages: identification/detection; risk assessment; and, mitigation/remediation planning and implementation.

The mitigation and remediation timeline associated with a known vulnerability begins once the system and application owner(s) and/or administrator(s) have identified the vulnerability using the results from the monthly vulnerability scans and vendor-published security vulnerability information, including recommendations for installing security patches and implementing configuration changes to reduce the likelihood that a system can be compromised.

Mitigation and Remediation Timeline Requirements

Critical Risk Vulnerabilities: Mitigation and/or remediation is required to address all critical risk vulnerabilities on all affected systems within 30 days.

High Risk Vulnerabilities: Mitigation and/or remediation is required to address all high risk vulnerabilities on all affected systems within 30 days.

Medium Risk Vulnerabilities: Mitigation and/or remediation is required to address all medium risk vulnerabilities on all affected systems within 90 days.

Low Risk Vulnerabilities: Mitigation and/or remediation is required to address all low risk vulnerabilities on all affected systems within 120 days.

False Negatives, False Positives, and Not Applicable Results

False Negatives

Units are responsible for ensuring vulnerability scans are not hindered due to inadequate access to the systems, applications, and devices being scanned. This will cause inaccurate and/or incomplete results to be produced. In many cases, credentialed scans should be utilized to ensure that scans analyze the entire system and produce accurate and comprehensive

results. Without required access levels, scan results may produce 'false negative' results which provided an inaccurate picture of the security posture of the system or device being scanned.

False Positives or Not Applicable Results

If the identified vulnerability is believed to be a false positive, or, is otherwise believed not applicable, the following information is required to be concisely documented within the ITS vulnerability scanning system, and made available for ISPO review.

- The affected system(s) and vulnerability.
- The plugin/service/software causing the false positive.
- Information/processes used to confirm the vulnerability is, in fact, a false positive or not applicable.

Mitigation and Remediation Requirements

After confirming the vulnerability scan results that are applicable to their systems, university units are responsible for addressing the risks presented by such vulnerabilities, through implementation of required vulnerability risk mitigation and remediation strategies.

Where possible, units are required to permanently resolve the risks associated with the vulnerability through implementation of permanent fixes that will usually include installation of vendor security patches and/or configuration changes. Permanent fixes also may require changes to unit-specific policies and procedures. All changes should be documented and made available for ISPO review upon request, as previously discussed.

If a vendor security patch or configuration change is not available to permanently resolve the risk associated with the vulnerability, units will be required to develop and implement compensating controls, which are applied at the network, IT system, and/or application level. The controls are required to mitigate the risks of the vulnerability and shall be consistently implemented until a permanent remediation is implemented.

Remediation Strategies

Patching the software or service and developing a continuous remediation process. Removing the software or services that are not needed, if possible. Implement configuration changes using security features within the application, operating system, other software, and/or infrastructure to further reduce the attack plane. Adopt a strategy only to allow/install required services that are needed on the device.

Vulnerability Remediation Exemptions

The Chief Information Security Officer (CISO) is authorized to approve exceptions and take action, as needed, to ensure systems with un-remediated vulnerabilities do not pose a threat to University resources.

Department heads can request an exception through the ISPO. The ISPO will provide an Exception Form which will be filled out by Technical staff and routed through their respective Department Head. Requests will be reviewed by the CISO or the CISO's designee. Approval of the request documents the department head has been informed of the risk, agrees with the need for the exception, and, accepts the risk associated with the exception request.

If the exemption requestion is approved, units are responsible for monitoring the system on a regular and on-going basis and documenting the vulnerability exception within the ITS vulnerability scanning environment.

Glossary

Appliance	A set of integrated hardware and software components provided as a dedicated single solution or hardware/software device.
Attacker, Adversary [NIST SP 800-30]	Individual, group, organization, or government that conducts or has the intent to conduct detrimental (or criminal) activities.
Availability [ISO/IEC 27000:2014]	Property of being accessible and usable upon demand by an authorized entity.
Confidentiality [ISO/IEC 27000:2014]	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Compensating Control	A compensating control, also called an alternative control, is a temporary solution mechanism that is put in place to manage a security risk and meet a security objective that is otherwise deemed impractical to implement at the present time. Compensating controls should only be considered when a specific security requirement or security control objective cannot be met due to legitimate technical or documented business or legal constraints. Compensating controls are required to sufficiently manage or mitigate the risk associated with the vulnerability through implementation of other alternative controls.
Exploit	An exploit is an actual or potential attempt to penetrate a network or IT system or resource through utilization of a security flaw or vulnerability. Malicious exploits often result in system disruptions and serious loss of data and system confidentiality, integrity, and availability.
Exposure	An exposure is a vulnerability or threat to an IT system, resource, or data set that is susceptible to attack via a known exploit or attack. Exposure examples include: inappropriate Windows, Linux, VMWare settings or configuration; inappropriate desktop, server or storage system configuration; running services or daemons that enable common attack points; using applications or services that are susceptible to brute force

	attack.
False Positive and False Negative	A false positive is an instance in which a vulnerability is identified where no such vulnerability exists. Conversely, a false negative represents an instance in which a vulnerability is not identified where such a vulnerability exists.
Information Security Risk [NIST SP 800-30]	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See *Risk*.
Information System – Related Security Risks [NIST SP 800-30]	The risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of *Information Security Risk*. See *Risk*.
Information Security Testing [NIST SP 800-115]	The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.
Integrity [ISO/IEC 27000:2014]	Property of accuracy and completeness
Information Technology Resources	Information Technology (IT) resources means data processing hardware, software and services; network data and telecommunications; information systems; supplies; personnel; computing facility resources; maintenance, and training. Examples of IT resources include computers, networks, software applications, data files and records, computer accounts, web sites, social media sites, hand held and wireless devices, telephone devices such as cellular phones, beepers, office telephones and cloud-based platforms and services
Mitigation Strategies	Vulnerability risk mitigation is defined as the set of temporary actions required to be performed to reduce the potential adverse effects associated with a given threat or vulnerability. They are utilized when permanent solutions are not currently available. Mitigation activities are also used to reduce the likelihood that a vulnerability could be exploited. Mitigation actions may not completely resolve the risks associated with such threats, but when implemented with appropriate compensating controls, their effect is to reduce the level of risk to an acceptable level and limit the adverse effects that are expected if the threat or vulnerability is successfully exploited.
Qualitative Risk Assessment	Use of a set of methods, principles, or rules for assessing risk based on non-numerical methods.

[NIST SP 800-30]	
Quantitative Risk Assessment [NIST SP 800-30]	Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
Remediation Strategies	Remediation activities are intended to result in a permanent solution which removes vulnerability as a potential threat. Remediation activities often include: the installation of permanent security patch software; implementation of permanent security configuration changes; or development and implementation of additional security controls, policies, and procedures.
Risk	Effect of uncertainty on objectives [ISO/IEC 27005:2011, ISO Guide 73, ISO/IEC 27000:2014] Combination of the probability of an event and its consequence [ISO/IEC 27000:2009] A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. See *Information System-Related Security Risk.* [NIST SP 800-30]
Risk Analysis [ISO/IEC 27000:2009]	Systematic use of information to identify sources and to estimate the risk
Risk Assessment	The overall process of risk analysis and risk evaluation [ISO/IEC 27000:2009] the overall process of risk identification, risk analysis and risk evaluation [ISO/IEC 27000:2014], [ISO/IEC 27005:2011]
Risk Assessment Methodology [NIST SP 800-30]	A risk assessment process, together with a risk model, assessment approach, and analysis approach.
Risk Criteria [ISO/IEC 27000:2009]	Terms of reference by which the significance of risk is assessed
Risk Estimation [ISO/IEC 27000:2009]	Activity to assign values to the probability and consequences of a risk
Risk Evaluation [ISO/IEC 27000:2009]	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk

Risk Factor [NIST SP 800-30]	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment
Risk Model [NIST SP 800-30]	A key component of a risk assessment methodology (in addition to the assessment and analysis approach) that defines key terms and assessable risk factors.
System Owner and/or System/Application Administrator(s) or Responsible Technical Staff	Business and/or technical staff who are responsible for the security posture and configuration, including vulnerability management, risk assessment, configuration, management and/or implementation of compensating controls required to remediate the vulnerability successfully.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization [ISO/IEC 27000:2014] Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST SP 800-30]
Semi-Quantitative Assessment [NIST SP 800-30]	Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts.
Version Scanning [NIST SP 800-115]	The process of identifying the service application and application version currently in use.
Vulnerability	1. A weakness of an asset or control that can be exploited by one or more threats [ISO/IEC 27000:2014] 2. A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST SP 800-30]
Vulnerability Exemption	A vulnerability exemption (or exception) is the removal of a vulnerability from a report and will no longer be considered after an exemption or exception has been approved for a specific system or set of systems by the ISPO.
Vulnerability Assessment [NIST SP 800-30]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Additional Resources

ITS Patch Management Service.

https://its.fsu.edu/service-catalog/it-professional-services/patch-management

Common Vulnerability Scoring System (CVSS) Specification.

https://www.first.org/cvss/specification-document

CERN Computer Security Baselines.

https://security.web.cern.ch/security/rules/en/baselines.shtml

Center for Internet Security (CIS) Security Benchmarks.

https://www.cisecurity.org/cis-benchmarks/

Microsoft Security Compliance Toolkit.

https://www.microsoft.com/en-us/download/details.aspx?id=55319

Cisco Security Baselines (IOS, Network, Switching, Routing).

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap7.html

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap3.html

Revision History

Version	Date	Name	Description
0.9	January 10, 2019	Jack May, Joseph Brigham, Bill Hunkapiller, Ken Johnson	