Administrative Procedure 7227

IT Vulnerability Management

Responsible Office: Office of Information Technology

PURPOSE

The Superintendent has adopted this Administrative Procedure to establish requirements for Vulnerability Management (VM) capabilities for Washoe County School District (District) Information Systems. VM is the process that enables timely identification, assessment, and remediation of IT Security vulnerabilities which could cause harm to the confidentiality, integrity, or availability of District systems or data.

DEFINITIONS

1. "Acceptance" is acknowledgement that the potential loss from a risk is not enough to warrant addressing the risk through remediation or mitigation.
2. "Compensatory Control" also called an "alternative control" is a mechanism put in place to satisfy a security requirement that is deemed too difficult or impractical to implement within the remediation timeline.
3. "Configuration Management Database (CMDB)" refers to a centralized inventory of all District Information Resources that stores information about hardware and software assets and the relationships between them.
4. "Evaluation" is a process of judgement or estimation of the nature and qualities of the vulnerability including the base, temporal, and environmental factors that might impact the District's implementation of particular technology.
5. "Information Resources" are data and information assets and systems of the organization.
6. "Metric" is a quantitative measurement that indicates the performance of a program or system.
7. "Mitigation" is a treatment method that reduces the severity of a vulnerability being exploited or reduces its harmful effects and minimizes the potential impact to the organization.
8. "Patch" is a set of changes to a computer program or its supporting data designed to update, fix, or improve functionality or security.
9. "Penetration Testing" is a form of ethical hacking where a trusted party attempts to exploit vulnerabilities in systems, networks, applications, and user security.
10. "Remediation" is the ideal treatment because it fixes or patches a vulnerability permanently, so there is no potential for the vulnerability being exploited.
11. "Reporting" is the process of collecting, analyzing, and processing technical artifacts related to the VM process and presenting them to organizational leaders.

12. "Risk" is a threat to business data or operations associated with the use, ownership, operation, involvement, influence, or adoption of IT within the District.

13. "Vulnerability" means a weaknesses or flaw in design, system procedures, controls, implementation, or configuration that could be exploited to cause harm to the confidentiality, integrity, or availability of Information Resources.

PROCEDURE

1. Roles and Responsibilities

    a. Chief Information Officer (CIO)

        i. Oversees the District's IT VM Program;

        ii. Allocates shared resources based on business priorities;

        iii. Reviews and processes Vulnerability Deferral Requests escalated by the IT Security Officer; and

        iv. Reviews and processes IT Security requests to delegate vulnerability scanning or penetration testing authority to trusted third-parties.

    b. Office of Information Technology

        i. Designates organizational hardware and software standards; and

        ii. Maintains the District Configuration Management Database (CMDB) which provides current and accurate reporting on all Information Resources and components.

    c. System Administrator

        i. Installs, manages, and maintains systems;

        ii. Documents system technical requirements, components, and integrations;

        iii. Implements patches and remediation actions; and

        iv. Validates systems operation after performing vulnerability mitigations.

    d. System Owner

        i. Responsible for the business processes that associated IT assets support;

ii. Identifies criticality of assets and information processed by systems to aid in enterprise VM;

iii. Coordinates with System Administrators and Users to minimize operational impacts when performing system changes; and

iv. Requests Vulnerability Deferral Requests depending on operational impact of system patching, configuration change, or other mitigations.

e. System Users

i. Verifies and report out-of-date patches or failures in automated processes and tools.

f. IT Security Department

i. Identifies and assesses vulnerabilities through manual and automated scanning;

ii. Delegates authority to perform vulnerability scanning or penetration testing activities to approved third parties; and

iii. Reports on the effectiveness of the VM Program.

g. IT Security Officer

i. Reviews and accepts, rejects, or escalates Vulnerability Deferral Requests; and

ii. Ensures that the VM Program is implemented as designed by providing guidance and resources to stakeholders.

2. Vulnerability Management

a. The District maintains an IT VM Program to methodically identify, evaluate, and address IT Security vulnerabilities.

b. All District Information Resources must be regularly evaluated for vulnerabilities including monthly scheduled scanning or manual review to identify known vulnerabilities.

c. Detected vulnerabilities must be addressed through the VM Procedure.

3. Vulnerability Management Procedure

a. The VM Procedure is a five-phase process including: Identification, Evaluation, Treatment, Verification, and Reporting.

b. During the Identification phase, IT personnel identify enterprise assets connected to the District network and which vulnerabilities might impact the systems. Assets are added to the CMDB.

c. During the Evaluation phase, District personnel will take steps to validate and confirm vulnerabilities and assign them a Risk Rating based on the Common Vulnerability Scoring System (CVSS), an industry-standard method of identifying and classifying vulnerabilities. The most severe vulnerabilities should be addressed first.

d. During the Treatment Phase, the System Owners and supporting personnel must determine how to address discovered vulnerabilities. Treatment is the overall strategy for addressing vulnerabilities through remediation (fixing or patching), mitigation (modified operation or compensating control), or acceptance. Vulnerability treatments must be selected and implemented within the following timeframes:

WCSD Risk Category	WCSD CVSS Rating	Timeframe (from notification)
Critical	9.0 or higher	>15 days
High	7 – 8.9	>30 days
Medium	5 – 6.9	>60 days
Low	5 or less	>90 days

e. During the Verification phase, the IT Security Department confirms that the vulnerability has been addressed. This may involve performing additional scanning activities to confirm that vulnerabilities have been appropriately identified, evaluated, and treated.

f. During the Reporting phase, IT personnel update the District CMDB regarding new system baselines and generate reports on the strategy and efficacy of treatments performed. VM Exception Requirements.

a. If a security patch or other mitigation cannot be implemented within the required timeframe due to operational requirements, the System Owner or Administrator may request an Exception (or vulnerability deferral) through the IT Security department.

b. The System Owner or Administrator must provide the request in writing to the IT Security Department with an explanation of why the recommended fix cannot be implemented, whether this is a temporary or permanent exception, and any compensatory controls that will be implemented.

c. The IT Security Officer may approve, deny, or escalate the request to the CIO depending on its merits. That decision will be relayed to the appropriate parties (including the requester) for follow-on action(s).

5. Centralized Management

    a. The Office of Information Technology centrally manages and performs VM implementation, operations, and procedures.

    b. Centralized management ensures that VM efforts are adequately resourced, validated, and performed in a way that does not inadvertently introduce additional risks to District IT systems.

    c. The Office of Information Technology must develop and maintain centralized resources supporting VM including:

        i. A centralized inventory of all District Information Resources, commonly known as a Configuration Management Database (CMDB), that stores information about hardware and software assets and the relationships between them;

        ii. A Vulnerability Scanning system that supports automated vulnerability scanning and identification. VM systems support the entire VM lifecycle including asset discovery, verification, reporting, and reassessment;

        iii. Enterprise Patch Management capabilities that support identifying and deploying needed patches. Patch Management systems support bundling or sequencing as appropriate, validating patch integrity, and methodically deploying patches to Administrator-designated locations (i.e., phased deployments); and

        iv. Shared Repositories that ensure that network resources are not overloaded during patch distribution and securely store associated backup activities.

6. Vulnerability Scanning and Penetration Testing

    a. The IT Security Department is authorized to perform vulnerability scans of all devices connected to the District Network. Scans may be passive or active in nature and must be performed and documented at least quarterly or after any significant change to the network.

    b. The IT Security Department may delegate authorization to perform limited scanning to third parties with the written approval of the CIO.

    c. District personnel may not interfere with vulnerability scanning through unapproved obfuscation technologies or blocking connections to the enterprise vulnerability scanner.

    d. In addition to conventional vulnerability scanning, Penetration Testing may be performed in defined, limited engagements.

7. Program Reporting

    a. The IT Security Department will develop reporting methodologies that track trends and demonstrate the effectiveness of the VM Procedure and its effects on the organization, systems, and users.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Regulation the goals of the District's Strategic Plan, and aligns/complies with the governing documents of the District, to include:

    a. Board Policy 7205, Information Technology – Data Access Policy; and

    b. Board Policy 7210, Information Technology Services and Operations;

REVISION HISTORY

Date	Revision	Modification
06/15/2022	1.0	Adopted