Category: Information Security Legal and Compliance Responsible Office: Chief Information Officer	**Standard Title:** Tenable One Vulnerability Management Implementation Standard Document Number: 6904 Effective Date: August 1st, 2026 This policy item applies to: State-Operated Campuses Community Colleges SUNY System Administration

Table of Contents

Section 1: Purpose, Scope, and Applicability 1
Section 2: Asset Management & Inventory 3
Section 3: Sensor Deployment and Configuration 4
Section 4: Scanning Standards & Configuration 6
Section 5: Vulnerability Remediation 7
Definitions 8

Section 1: *Purpose, Scope, and Applicability*

1.1 Purpose

This standard establishes the minimum operational requirements for all campus units deploying and operating Tenable Vulnerability Management (Tenable VM). It ensures a consistent, risk-based approach to vulnerability identification, prioritization, and remediation across the institution's distributed technology environment.

1.2 Scope

This standard applies to all campus units that have been provisioned with Tenable Vulnerability Management under the SUNY System Administration centralized contract and governs the use of that platform as the primary system of record for vulnerability identification, prioritization, and remediation reporting to SUNY System Administration. The required outcomes of this standard apply to all in-scope asset classes regardless of which vulnerability management tool or combination of tools a campus deploys to achieve them.

1.3 Applicability

This standard applies to all institutionally owned, managed, or controlled technology assets, including:

- Physical and virtual servers, whether on premises or cloud hosted
- Virtualization platforms and management planes, including hypervisors and associated management systems
- Managed end-user devices, including faculty, staff, classroom, virtual desktops, and lab workstations
- Network infrastructure devices, including switches, routers, network appliances, and firewalls
- Internet-facing systems
- Institutionally managed web applications, including both public-facing and internal intranet applications
- Systems and applications that process, store, or transmit sensitive information, as defined by the institution's data classification policy
- Databases and database platforms supporting institutional applications or data stores
- Internet of Things (IoT) and Operational Technology (OT) assets, where technically feasible

Where a campus operates an alternative or supplementary vulnerability management tool for a subset of in-scope assets — including but not limited to Microsoft Defender Vulnerability Management, Rapid7 InsightVM, or Qualys, the following apply without exception:

1. Tenable VM must remain the active system of record for all asset classes not demonstrably covered by the alternative tool at equivalent or greater scan depth and frequency.
2. The campus must document the alternative tool that has met the scan frequency requirements of Section 4.1 and the remediation SLA requirements of Section 5.1 for every asset class it covers.
3. All findings identified by any tool that meets the severity thresholds in Section 5.1 are subject to the remediation obligations defined in policy 6900.
4. Campuses using alternative tools for endpoint coverage must still maintain Tenable VM active enrollment and authenticated scanning for all server and network infrastructure asset classes listed above.

Institutions unable to demonstrate compliant vulnerability management outcomes through any combination of tools must bring affected asset classes into active Tenable VM scope within 90 days of discovery.

1.4 Governing References

- NIST SP 800-40 Rev. 4 – Guide to Enterprise Patch Management Planning
- NIST SP 800-53 Rev. 5 – SI-2 (Flaw Remediation), RA-5 (Vulnerability Monitoring)

- CIS Controls v8 – Control 7: Continuous Vulnerability Management
- SUNY Information Security Policy 6900

Section 2: *Asset Management & Inventory*

2.1 Asset Discovery

Each institution must maintain a complete and accurate inventory of in-scope assets to support effective vulnerability management. At minimum, institutions must implement automated asset discovery processes through Tenable Vulnerability Management module:.

1. Institutions with operating environments that have overlapping or identical IP address spaces must create distinct logical Networks within Tenable VM to prevent duplicate asset records and ensure accurate reporting.
2. Institutions must configure a scheduled, automated Host Discovery scan to run at least every two weeks across all approved, in-scope network segments. Institutions must use multiple detection methods, including TCP, ARP, and ICMP, where permitted by the environment.
3. Institutions must review available Tenable Vulnerability Management and Web Application Scan Templates at least quarterly to assess their applicability to the institutional technology environment.
   a. Applicable templates must be used to conduct targeted, risk-based vulnerability assessments for relevant systems, applications, and network segments.
   b. Institutions must also perform an out-of-cycle review when material changes to technology, architecture, or exposure occur, including the deployment of new internet-facing applications, significant platform changes, or the introduction of technologies for which Tenable provides new or updated relevant templates.

2.2 Asset Tagging

Institutions must implement Tenable VM tags to organize and filter assets for scan targeting and reporting. Required tag categories include:

- Asset Owner, identified as the responsible business unit or department
- Network Exposure (External, Partially Exposed, Internal)
- Asset Criticality (Critical, High, Medium, Low)
- Asset Environment (Production, Development, Test)

Tags must be reviewed and validated on a quarterly basis to ensure accuracy. Target groups may be used as a transitional mechanism but must migrate to tag-based targeting as capabilities mature.

Section 3: *Sensor Deployment and Configuration*

3.1 Sensor Types

Institutions must deploy an appropriate mix of Tenable sensors to achieve complete asset visibility. Tenable VM supports three primary sensor types:

- Tenable Nessus Scanners (network-based) – for on-premises network segments and infrastructure devices, student networks.
- Tenable Agents (host-based) – for endpoints that are remote, frequently offline, or cannot be reached by a network scanner
- Tenable Cloud Sensors – for scanning assets with publicly routable IP addresses and for cloud-hosted workloads

3.2 Nessus Scanner Requirements

All Institutionally deployed on-premises Nessus scanners must comply with the following:

- Scanners must be placed at each firewall boundary.
- Scanners must meet or exceed Tenable's published hardware minimum specifications.
- All scanner traffic to Tenable VM cloud (cloud.tenable.com) must use outbound TCP port 443 with TLS 1.2 or later (4096-bit key).
- Scanners must be linked to Tenable VM using a valid Linking Key. Once linked, the linking key is no longer active; a unique 256-bit key is assigned to the sensor.

3.3 Tenable Agent Requirements

Tenable Agents are mandatory for institutionally owned, managed, or controlled Microsoft Windows, Linux, and macOS devices. Institutions must:

- Organize agents into named Agent Groups aligned to the institutional asset classification (e.g., 'Windows-Servers-Production', 'Remote-Laptops').
- Use Agent Profiles to enforce consistent software versioning, define freeze windows during critical operation periods, and limit CPU utilization on production hosts.

3.4 Connectivity & Firewall Requirements

All sensors (Nessus Scanners, Tenable Agents, and Tenable Network Monitor) must have outbound access to the Tenable cloud endpoints listed in the Tenable VM documentation. Firewall allow-list entries must be maintained and reviewed annually.

3.5 Sensor Health, Versioning, and Coverage Validation

Institutions must maintain a repeatable process to monitor sensor health, enforce supported software versions, and verify that all in-scope assets are assessed at the required frequency.

Sensors that are offline, outdated, or assigned to the wrong scope create coverage gaps equivalent to having no sensor deployed.

3.5.1 Sensor Health Monitoring

Institutions must monitor the operational status of all deployed sensors as part of the routine vulnerability management cycle. At minimum, institutions must:

- Review sensor status in the Tenable VM Sensors dashboard monthly and verify that all linked Nessus Scanners and Tenable Agents report an Online or Healthy status.
- Investigate and remediate sensors in Offline, Warning, or Critical status within 30 days.
- Review the Last Scanned and Last Plugin Update fields monthly. A sensor with a Last Scanned date exceeding twice the scheduled scan interval must be treated as a coverage gap and investigated within 30 days.
- Investigate agents in safe mode, remediate the triggering condition, and confirm that the agent exits safe mode within 45 days of detection.
- Review agents remaining in safe mode for more than 60 calendar days without documented justification for decommissioning in accordance with Section 3.5.4.

3.5.2 Software Version Standards and Update Governance

Institutions must maintain current and consistent sensor software versions to support accurate and complete vulnerability data. At minimum, institutions must:

- Enforce a minimum supported version for all deployed Tenable Agents.
- Document an exception for any agent that cannot be upgraded within 60 calendar days. Ensure that all Nessus Scanners linked to Tenable VM meet or exceed Tenable's published minimum hardware specifications for the deployed version.
- Review scanner hardware against current Tenable specifications annually and flag non-compliant scanners for refresh or redeployment in the next budget cycle.

3.5.3 Coverage Validation and Gap Identification

Institutions must maintain a formal coverage validation process to confirm that all in-scope assets are assessed at the required frequency and that all managed network segments are within sensor coverage.

At minimum, institutions must:

- Compare the asset inventory produced by bi-weekly Host Discovery scans (Section 2.1) against the active asset list in the Tenable VM Assets workbench on a monthly basis. Assets identified in Host Discovery that have not been assessed (Asset Assessed = false) must be reviewed, assigned to an appropriate scan scope, or formally documented as out-of-scope with institutions information security program lead acknowledgment.
- Conduct a network segment coverage audit on a biannual basis.

- Maintain a sensor-to-segment coverage map that documents which sensor or sensor group is responsible for each managed network segment, the sensor type deployed, and the date the assignment was last validated. This map must be updated whenever network topology changes occur (e.g., VLAN additions, subnet reallocation, new building or facility onboarding) and reviewed in full on a semi-annual basis.
- Apply a dynamic tag (e.g., Sensor-Coverage: Gap) to assets identified in Host Discovery that have not been assessed within the expected scan cycle for their asset classification tier. Tagged assets must be reviewed and either brought into active scan scope or formally documented as exceptions per Section 1.3 within 30 calendar days of tag assignment.

3.5.4 Sensor Decommissioning

Orphaned sensors, scanners or agents that remain linked in Tenable VM after their host system has been decommissioned, reimaged, or reassigned, distort coverage reporting and consume license capacity without contributing scan data. Institutions must establish a sensor decommissioning procedure integrated with their broader asset lifecycle and change management processes. At minimum, institutions must:

- Unlink or remove from Tenable VM any Nessus Scanner or Tenable Agent associated with a host that has been decommissioned, retired from service, or permanently removed from the network. Sensor removal must be completed within 30 days of host decommissioning.
- On a biannual basis, audit the linked sensor list for agents and scanners that have not reported a Last Scanned date within the prior 60 days. Sensors exceeding this threshold without a documented operational justification (e.g., approved freeze window, seasonal lab closure) must be unlinked and the associated host investigated to determine whether the endpoint is still in active use.
- Coordinate sensor decommissioning with the coverage validation process in Section 3.5.3: before unlinking any scanner, confirm that the network segments previously covered by that scanner remain within the coverage scope of another active sensor. Scanner removal that creates a coverage gap must be escalated and documented by the institution's information security program lead before proceeding.

Section 4: *Scanning Standards & Configuration*

4.1 Scan Frequency Requirements

Scan frequency is driven by asset criticality and data classification. At minimum, institutions must adhere to the following schedule:

- Critical and Restricted systems: Full credentialed vulnerability scan weekly
- High Criticality or Confidential systems: Full credentialed vulnerability scan bi-weekly
- Medium / Standard systems: Full credentialed vulnerability scan bi-weekly (minimum)
- All in-scope systems: Host Discovery scan bi-weekly (minimum)

Scans must also be performed after any significant change to the network environment, including new system deployments, major software upgrades, and network reconfigurations.

4.2 Scan Templates

Institutions must select the most appropriate Tenable-provided scan template for each use case. Custom scan policies may be used only when no standard template meets the operational requirement. The following templates are pre-approved for routine use:

- Basic Network Scan – general vulnerability assessment for standard network assets
- Advanced Network Scan – comprehensive scanning where full plugin flexibility is required
- Credentialed Patch Audit – authenticated scan enumerating missing patches; mandatory for all servers
- Host Discovery – weekly asset discovery; assets found in discovery scans do not count against the license
- Policy Compliance Auditing – configuration compliance checks against approved baselines

4.3 Credentialed Scanning

Credentialed scanning is required for all servers and workstations where technically feasible. Unauthenticated scans are acceptable only for devices that do not support credential-based access. Institutions must:

- Maintain dedicated service accounts for Tenable scanning with the minimum privileges required for vulnerability enumeration.
- Rotate scanning credentials on a schedule consistent with the institutional password policy.
- Store credentials exclusively within Tenable VM's encrypted credential store; credentials must never be embedded in scan configuration exports or documentation.
- Enable the 'Create unique identifier on hosts scanned using credentials' setting to improve asset deduplication.
- Servers and workstations with agents installed and conducting the scan satisfy this requirement.

Section 5: *Vulnerability Remediation*

5.1 Remediation Process

Upon identification of a vulnerability finding, the responsible campus unit must:

- Prioritize remediation of Critical and High severity findings on internet-facing or Restricted-data systems above all other findings.
- Prefer vendor-supplied patches as the primary remediation mechanism.

- Launch a Remediation Scan following remediation to confirm closure. Remediation scans must use the Advanced Network Scan template or a template that best fits that need.

5.2 Remediation Exceptions

When a finding identified as Critical or High that cannot be remediated within the defined Policy remediation timeframe, the asset owner must formally document the exception along with the following information:

- Asset identification and finding details (CVE, plugin ID, severity)
- Justification for the exception
- Compensating controls currently in place
- Proposed re-evaluation date (maximum 12 months)

Exceptions are reviewed and approved by the designated ISP. Exceptions shall be retained in the Tenable Vulnerability Management platform or retained in a manner similar to Information security program exceptions as outlined in SUNY Policy 6900.

Definitions

System of Record: The authoritative platform or repository used to maintain official vulnerability management data, including asset coverage, findings, scan results, remediation status, and reporting.

Asset Discovery: The process of identifying active technology assets within approved network segments, typically through scheduled Host Discovery scans or equivalent automated discovery methods.

Credentialed Scanning: Vulnerability scanning performed using authenticated access to a system, allowing deeper inspection of missing patches, configuration issues, software versions, and system-level vulnerabilities.

Tenable Sensor: A scanning or data collection component used by Tenable VM, including Nessus Scanners, Tenable Agents, Tenable Cloud Sensors, and related sensor technologies.

Coverage Gap: A condition where an in-scope asset, network segment, or sensor is not being assessed at the required frequency or is not properly included within vulnerability management scope.

Remediation Scan: A follow-up vulnerability scan conducted after corrective action has been taken to verify that a vulnerability finding has been resolved.

Remediation Exception: A formally documented and approved condition where a Critical or High vulnerability cannot be remediated within the required timeframe and must include justification, compensating controls, and a re-evaluation date.

Orphaned Sensor: A Nessus Scanner or Tenable Agent that remains linked in Tenable VM after the associated host has been decommissioned, reimaged, reassigned, or otherwise removed from active use.

Safe Mode: A Tenable Agent operating state that indicates the agent has entered a protective or limited-function condition due to a triggering issue that must be investigated and remediated.

Network Exposure: A classification describing how accessible an asset is from external or internal networks, such as External, Partially Exposed, or Internal, used to support scan targeting, prioritization, and reporting.
