Point32Health

C&IS 004 –CYBER & INFORMATION SECURITY THREAT AND VULNERABILITY MANAGEMENT STANDARD

Version 1.0

I. INTRODUCTION 1
1. AUTHORITY 1
2. PURPOSE 1
3. SCOPE 2
4. OUT OF SCOPE 2
5. ROLES AND RESPONSIBILITIES 2
6. DEFINITIONS 3
II. STANDARD 4
1. THREAT INTELLIGENCE MONITORING 4
2. VULNERABILITY RATING 4
3. VULNERABILITY TESTING 4
4. EXTERNAL-FACING APPLICATION SECURITY TESTING (WEB AND MOBILE) 4
5. APPLICATION CODE REVIEWS 5
6. VULNERABILITY REMEDIATION SCHEDULE 5
7. MALWARE PREVENTION 5
III. EXCEPTION MANAGEMENT 5
IV. CONTACT INFORMATION 6
V. REFERENCE DOCUMENTS ..... **Error! Bookmark not defined.**
VI. REVISION HISTORY 6

I. INTRODUCTION

1. AUTHORITY

The chief information security officer (CISO), who is also the manager of Cyber & Information Security, is responsible for the development, maintenance and communication of the Cyber & Information Security Threat and Vulnerability Management Standard.

The CISO is responsible for approving the Cyber & Information Security Threat and Vulnerability Management Standard and any material changes to this standard.

This standard applies to Point32Health, its subsidiaries, all offices and divisions and their directors, officers, colleagues, contingent workers, and temporary resources. Point32Health may modify the Information Security Standards at any time at its sole discretion and without prior notice, subject to the approval of the CISO. Certain subsidiaries, offices or divisions might be subject to additional or more restrictive legal or regulatory requirements, depending on the law of the jurisdiction in which they operate.

2. PURPOSE

The purpose of this standard is to provide a documented set of requirements and consistent methodology for planning, conducting, assessing, reporting, and facilitating remediation of identified security threats and vulnerabilities to technology assets. Impacted departments or divisions may consider the use of implementation

specifications, i.e., approved implementation methods for supporting a specific standard, to further define how to apply the requirements outlined below within their areas of responsibility.

3. SCOPE

This standard applies to all Point32Health colleagues (direct employees or contractors) responsible for installing, configuring, or updating technology asset types, as well as software, software components, Application Programming Interfaces (APIs) and applications including, but not limited to the below:

- Operating systems, e.g., MS Windows, Linux, HPUX, IBM z/OS, MacOS, Android
- Network devices, e.g., switches, routers, firewalls, WAFs, wireless access points
- Production network-connected operational technology, e.g., CCTV, HVAC, RFID authentication
- Databases, e.g., MS SQL, Oracle, MySQL, NoSQL
- Network storage devices, e.g., NetApp, EMC, Hitachi
- Virtual hypervisors, e.g., VMWare, Oracle, Citrix
- Aspects of cloud hosted environments configurable by Point32Health, e.g., laaS, PaaS, SaaS
- Web servers, e.g., MS IIS, Apache Web Server
- Middleware, e.g., security (authentication, authorization, identity), proxy, directory servers
- Technology platforms, e.g., Microsoft 365, Salesforce
- Applications and APIs, e.g., OHI, TAHPMaster, Diamond

4. OUT OF SCOPE

This Standard does not apply to systems or applications that are hosted **and** maintained by third-party providers.

5. ROLES AND RESPONSIBILITIES

a. Cyber & Information Security – A team of subject matter experts reporting into the Cyber & Information Security division of the Information Technology that defines the Cyber & Information Security Risk Management process, framework, policies, standards and control requirements. Identifies and reports on risks and remediation activities. Recommends controls and/or approves remediation plans to adequately address identified risk issues.

b. Asset Owner – A Point32Health colleague who has the ultimate accountability to establish and maintain a secure control environment to ensure confidentiality, integrity and availability of the asset. Typically, the asset owner is the most senior manager of the business area that defines the need, requirements and/or creation of the asset. All assets will have a designated asset owner, e.g., information asset owner or technology asset owner.

c. Custodian – A custodian may be a business application owner, the owner of a file share, SharePoint site, Microsoft Teams site, etc., who is accountable for the oversight and implementation of necessary safeguards to protect the asset as defined by the asset owner, including:

i. Management, maintenance and monitoring of vulnerabilities for their applicable technology areas; including any security code flaws identified during application code reviews or application security testing, and

ii. Informing the appropriate asset owner of risks and recommended remediation plans for identified vulnerabilities that have not been corrected or otherwise mitigated within the vulnerability remediation schedule target

d. IT Manager – A Point32Health manager with administrative responsibilities for one or more IT support resources, who is responsible for ensuring that the technical security controls, as defined by the applicable Cyber & Information Security Standards and the custodian, are appropriately implemented and maintained.

If unable to comply with the published Standards, the responsible IT manager must notify Cyber & Information Security of any variance in accordance with the published Risk Assessment Standard.

e. IT Support Resources – Individuals who work in a technical capacity to design, install, configure, develop, QA, support, or maintain technology assets (e.g., developers, server/networking specialists, database administrators, software engineers, app dev/analysts, quality analysts, business analysts, etc.). IT support resources apply security controls to protect and maintain technical assets. IT support resources are responsible for:

i. Remediating identified vulnerabilities within the corresponding vulnerability remediation schedule for the systems they support, including patching of vulnerable applications, systems, software and/or applying other mitigating controls; and

ii. Ensuring that all applications, infrastructure systems, middleware and platforms continue to be supported and obtain up-to-date security patches from corresponding technology vendors or alternate service providers.

6. DEFINITIONS

a. Asset – For purposes of this standard, there are two primary asset types: an information asset and a technology asset. An information asset refers to any content, report, data (structured or unstructured) or knowledge – in any form, e.g., printed, electronic or verbal. A technical asset represents any technology used to transmit, host, use, store or destroy information assets or services by or on behalf of Point32Health.

b. Threat – A potential (future) event that, if realized, may cause measurable harm to the confidentiality, integrity or availability of an asset or business process.

c. Open Source – Any publicly available software that may be copied, modified, and redistributed in source code format without charge, including but not limited to any publicly available software listed by the Open-Source Initiative (OSI).

d. Vulnerability – An existing technical and/or operational weakness that may allow a threat to be exploited, resulting in compromise of the confidentiality, integrity or availability of an asset.

e. Vulnerability Testing – Testing that makes use of an automated security tool to scan technology assets or open-source code to identify security vulnerabilities most commonly associated with outdated/insecure software, misconfigurations and/or missing security patches of operating systems, network devices, technology platforms, and middleware. Depending upon the specific security tool being used and the complexity of a given application, the assessment may also identify one or more application-specific vulnerabilities. Vulnerability testing will not thoroughly inspect an application to ensure that secure development practices have been applied.

f. Application Security Testing – Manual and/or automated tests of web and mobile applications to identify vulnerabilities derived from insecure coding or business logic implemented within a given application. Types of application security testing include:

i. **Dynamic Application Security Testing (DAST)** – Automated, dynamic tests performed against applications while they are running (e.g., Whitehat, Veracode)

ii. **Manual Penetration Testing (e.g., Red Team)** – Testing that verifies the extent to which a system, device or process resists active attempts to compromise its security. Subject matter experts will leverage knowledge, skills and output of security tools to analyze and execute specialized testing.

g. Application Code Reviews – Manual and/or automated reviews performed to validate the quality and security of custom developed code or scripts. This could include:

i. **Manual Code Reviews** – Process of reading source code line-by-line to identify flaws.

ii. **Static Application Security Testing (SAST)** - Automated analysis of source code (e.g., Veracode, SonarQube).

h. Internal Environment – Comprised of assets that are only accessible from within the Point32Health computing environment.

i. **Demilitarized Zone (DMZ)** - A perimeter network segment that directly interacts with systems and applications in an untrusted environment (e.g., the Internet). The DMZ allows access to resources from untrusted networks while keeping the internal network environment secure.

j. **Managed Device** – Any device that is configured and supported by or on behalf of Point32Health and provides a reasonable level of trust that Assets used or accessed by the device are secure.

II. STANDARD

1. THREAT INTELLIGENCE MONITORING

Cyber & Information Security is responsible for monitoring information from intelligence and special interest groups (e.g., HealthCare Information Sharing and Analysis Center (H-ISAC) and ensuring that mitigating action is taken if there is reasonable potential that a particular threat, such as zero-day threat, may impact the Point32Health environment.

2. VULNERABILITY RATING

When available, Point32Health must use the temporal common vulnerability scoring system (CVSS) from the national vulnerability database (NVD) managed by the National Institute of Standards and Technology (NIST) to help prioritize potential risk to the organization.

The following are definitions of vulnerability severity levels:

i. Critical = CVSS score of 9.0 – 10.0
ii. High = CVSS score of 7.0 – 8.9
iii. Medium = CVSS score of 4.0 – 6.9
iv. Low = CVSS score of 0.1 – 3.9

3. VULNERABILITY TESTING

a. All security tools utilized to help identify vulnerabilities must be approved by Cyber & Information Security.
b. Populated IP ranges (internal, DMZ, and external/Internet) will be scanned for new hosts monthly via discovery scans.
c. All Point32Health owned IP ranges (internal, DMZ, and external/Internet) will be scanned for new hosts via discovery scans on a quarterly basis.
d. Authenticated (or agent-based) vulnerability testing shall be performed monthly for all in-scope technology assets.
e. Open-source code must be scanned monthly for vulnerabilities *(Refer to the Application Security Standard for additional information regarding code scanning requirements).*
f. Point32Health will maintain the capability to perform vulnerabilities scans upon request.

4. EXTERNAL-FACING APPLICATION SECURITY TESTING (WEB AND MOBILE)

a. Applications, including APIs and “micro sites” that are accessible from the Internet must undergo application security testing (DAST) each month.
b. All external-facing applications must undergo application security testing (manual penetration testing) upon introduction to the production environment, at least annually, and upon request by Information Security.
c. All application security testing must be conducted by an independent, qualified third-party that has been approved by Cyber & Information Security.
d. Authenticated and non-authenticated tests must be conducted whenever applicable.

5. APPLICATION CODE REVIEWS

All changes to custom code will require an application code review of the components (e.g., APIs, UI, database, scripts, etc.) being changed prior to production release. Static application security testing must be used to complete the review when it is available and applicable to the code being assessed. The code review for these changes needs to be documented and/or approved to align with the code change/program change process.

6. VULNERABILITY REMEDIATION SCHEDULE

a. For newly introduced changes (e.g., new applications, systems, software, code, scripts, etc.), all identified vulnerabilities are expected to be addressed (i.e., corrected, mitigated or risk accepted) prior to being released into production.
b. For existing assets, the chart below represents the expected timeframe to address any identified vulnerabilities, with consideration for the environment in which the asset is hosted and the assigned rating of the identified vulnerability.

Environment	Vulnerability Rating	Timeframe
Internet Accessible / DMZ	Critical	ASAP; no more than 15 calendar days
	High	30 calendar days
	Medium	60 calendar days
	Low	120 calendar days
Internal Network	Critical	45 calendar days
	High	90 calendar days
	Medium	180 calendar days
	Low	As time permits

7. MALWARE PREVENTION

a. Microsoft Windows, Linux, and Apple Macintosh operating systems must make use of host-based malware prevention (anti-virus) and endpoint detection and response (EDR) software.
b. All malware prevention and EDR software being used on Point32Health operating systems must be at a version currently supported by the corresponding security vendor.
c. All malware prevention and EDR software must be configured to restrict the ability of operating system users, including operating system administrators, to modify predetermined configuration options without prior authorization from Cyber & Information Security.
d. All malware prevention and EDR software must be configured to update malware definition files and threat intelligence information at least daily, where applicable.
e. All malware prevention and EDR software must be configured to immediately scan all file types installed, opened, or copied that have the potential to insert malware, modify files or delete programs.
f. Host-based malware prevention software must be configured to clean malware that has been identified. If the identified malware cannot be cleaned, malware must be quarantined so that it will not be directly accessible by users of the operating system.
g. Endpoint Detection and Response (EDR) software must be configured to prevent unauthorized or suspicious activities considered high risk by the EDR provider.

III. EXCEPTION MANAGEMENT

Inability to meet the requirements set forth in this Information Security Standard poses a potential risk to Point32Health. As such, any variance must be shared with Cyber & Information Security, who will assess the risk and recommend an appropriate course of action (e.g., eliminate, correct, mitigate or accept the identified

risk).

IV. CONTACT INFORMATION

For all inquiries / questions regarding the Cyber & Information Security Policies or Standards, please contact: CyberInformationSecurity@point32health.org.

V. REVISION HISTORY

Version	Effective Date	Changed By	Change Description
1.0	April 1, 2024	Cyber & Information Security	Initial publication

All material changes reflected in the latest version of this Standard will become effective 90 calendar days after publication of the Standard. During the 90-day period, impacted technical and business stakeholders must complete a gap analysis and provide a recommended target to the CISO to request to apply material security changes to the existing environment, where applicable.