Point32Health

C&IS 005 – CYBER AND INFORMATION SECURITY - INFRASTRUCTURE AND PLATFORM SECURITY STANDARD

Version 1.0

I. INTRODUCTION

1. AUTHORITY

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

The Enterprise Security, Privacy, and Resilience Committee is responsible for approving the Cyber & Information Security Policy and Standard Framework and any material changes to this Standard.

This Standard applies to the following subsidiaries of Point32Health, Inc.: Harvard Pilgrim Health Care, Inc., Harvard Pilgrim Health Care of New England, Inc., HPHC Insurance Company, Inc., Harvard Pilgrim Group Health Plan, Tufts Associated Health Maintenance Organization, Inc., Tufts Health Public Plans, Inc., Tufts Insurance Company, CarePartners of Connecticut, Inc., Point32Health Services, Inc. group health plans, Tufts Benefit Administrators, Inc., and Total Health Plan, Inc., their employees, contractors, and temporary workers (“colleagues”).

Point32Health may modify the Cyber & 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 may 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 baseline of cyber and information security controls within Point32Health's technology areas. 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

The standard applies to all colleagues, custodians, IT support resources and IT managers responsible for installing, configuring, updating, or supporting the following categories of technology assets:

- Operating systems, e.g., MS Windows, Linux, HPUX, IBM z/OS, MacOS, Android
- Network devices, e.g., switches, routers, firewalls, WAFs, WAPs, segmentation infrastructure
- Security logging and monitoring repositories, e.g., Microsoft Sentinel, Netwitness
- Malware prevention and endpoint detection and response agents, e.g., Cylance, MS Defender
- 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, i.e., IaaS, PaaS, SaaS
- Web servers, e.g., MS IIS, Apache Web Server
- Middleware, e.g., security (authentication, authorization and identity), proxy, directory servers, password safe, multi-factor authentication tools (MFA), MS Azure, SiteMinder, etc.
- Technology platforms, e.g., Microsoft 365, ServiceNow, Workday, SailPoint
- Network connected embedded devices, e.g., sensors, IOT devices, network printers

This standard applies to all Point32Health managed environments, whether hosted on-premises, by a third-party hosting provider, or in the cloud. This includes but is not limited to development, test, QA, and production computing environments.

4. ROLES AND RESPONSIBILITIES

a. **Cyber & Information Security** –Subject matter experts reporting into the Cyber & Information Security division of the IT department. Provides support and consultancy to affected managers and stakeholders regarding requirements and implementation plans, develops supporting in-practice guidance documents and approves technical baselines.

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 and technology asset owner.

c. **Custodian** – A business application owner or the owner of a file share, SharePoint site, Microsoft Teams site, etc. Accountable for the oversight and implementation of necessary safeguards to protect the Asset as defined by the Asset Owner

d. **IT Support Resources** – Individuals who work in a technical capacity to design, install, configure, develop, QA, support or maintain technical assets (e.g., developers, server/networking specialists, database adminstrators, software engineers, app dev/analysts, quality analysts, business analysts, etc.). IT support resources apply security controls to protect and maintain technical assets and may create and publish procedures and technical baselines that detail specific processes and steps necessary to comply with standards within areas of responsibility.

e. **IT Manager** – A Point32Health manager with administrative responsibilities for one or more IT support resource. Responsible for ensuring 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 per the published Risk Assessment standard.

5. 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, verbal. A Technology Asset represents any technology used to transmit, host, use, store, or destroy Information Assets or services by or on behalf of Point32Health.

b. Technical Baselines – The minimum level of security configuration settings that Technology Assets (e.g., operating system, database, platform, network devices) must adhere to. Technical Baselines take into consideration Information Security requirements and are also mapped to industry hardening standards such as National Institute of Standards and Technology (NIST) or Center for Internet Security (CIS).

c. Threat – Refers to a potential event that, if realized, may cause measurable harm to the confidentiality, integrity, or availability of an Asset or business process.

II. STANDARD

1. SECURE CONFIGURATION

a. Processes must exist to restrict the ability for users to install unauthorized software on endpoint computers.

b. In-scope technology areas must have documented secure configuration standards (i.e., Technical Baselines, also commonly referred to as “hardening standards”) that are developed based upon Cyber & Information Security requirements and industry-leading hardening standards, e.g., NIST, CIS.

Note: The NIST Security Technical Implementation Guidelines (STIGs) are the default industry source for Point32Health. Where not available or applicable, the Center for Internet Security (CIS) Benchmarks should be considered next, followed by other trusted and authoritative sources.

i. Technical Baselines must include services / daemons that are required to be disabled by default.
ii. Technical Baselines must include a list of the specific security-related event details that will be captured and sent to an approved location on the network for logging and/or monitoring (i.e., security event logging requirements).
iii. Technical Baselines must include a list of all intended access groups (or lists) that will be granted administrative privileges to the given Asset.
iv. New or modified Technical Baselines must be approved by Cyber & Information Security.
v. Technical Baselines must be reviewed at least annually by appropriate IT Support resources in consideration of revised Cyber & Information Security requirements, industry standards, or vendor recommendations.

c. Periodic compliance reviews, as agreed by Cyber & Information Security, will be performed to validate that technical areas are compliant with approved Technical Baselines, no less frequently than annually. The frequency and method by which compliance reviews will be performed must be included within the applicable Technical Baseline documentation.

Note: The frequency of the compliance efforts is considerate of inherent risk and complexity; annual reviews should not be considered the "default" frequency to validate secure configurations but the minimum, often for lower risk Asset types.

d. All in-scope technology areas must be synchronized to external network time (NTP) sources approved by Cyber & Information Security.

2. PATCH MANAGEMENT

a. Custodians must document and maintain patch management processes for each in scope technology area.
b. All patch management processes and procedures must take into consideration the security rating assigned by the vendor or any applicable CVSS rating.
c. Patch management processes must include emergency and out-of-cycle security updates.

3. NETWORK SECURITY

a. Unauthorized devices must be restricted from connecting to the Point32Health network, via wired or wireless means.
b. Unauthorized wireless access points shall be technically restricted from connecting to the Point32Health network.
c. Appropriate segmentation must exist to restrict access between systems of different criticality or exposure to risk (e.g., production, non-production, and shared services/systems).
d. All external network connections must be protected by firewalls and intrusion detection systems (IDS).
    i. Firewalls must be placed between untrusted networks (such as external, DMZ, enclave, "guest") and the Point32Health core/internal (trusted) network. All access between these trusted and untrusted networks must be blocked ("deny all") unless it has been specifically authorized via the Point32Health Change Management process.
    ii. Firewall rules must be configured to limit specific application ports to communicate between authorized source and destination elements (e.g., IP addresses, DNS names, usernames, tags, etc.).
    iii. Point32Health's network must not allow traffic from unmanaged networks using source IP addresses that fall within non-routable IP ranges (such as 10.x.x.x, 172.x.x.x, 192.x.x.x, etc.) set aside for private networks.
e. Firewalls and IDS devices must be appropriately managed to ensure policies for all users and groups are efficiently created, distributed, and enforced.
    i. Network management and administration must be conducted using approved management infrastructure and secure protocols.
    ii. All remote administrator access to network devices must be forced to connect through a secure, virtual access tunnel approved by Cyber & Information Security (i.e., VPN).
    iii. On a semi-annual basis all custom firewalls rules must be reviewed to identify those that have not been used in the past 13 months and to disable any that are no longer required. All disabled firewall rules will be disabled for a period of 12 months and then subsequently deleted if no longer required.
f. Web Application and API Protection capabilities must be installed and configured to help protect externally facing applications and APIs hosted by Point32Health.
g. Distributed Denial of Service (DDoS) monitoring and protection coverage must be implemented to protect external facing technology Assets.
h. Databases must not be directly accessible from the Internet.

i. Databases must be separated by firewalls and corresponding firewall port/protocol restrictions if accessed by systems that are accessible from the Internet or the DMZ.
j. Technology Assets must employ malicious code (e.g., malware) protection capabilities to perform real-time scans of files from external/Internet sources prior to being made available for use by the system(s) or application(s) supported by the infrastructure; detection of malicious code must be escalated in accordance with the Cyber & Information Security Incident Management Standard.

k. Controls must be enabled to restrict access to external high-risk destinations and inappropriate websites, as defined by Human Resources and Cyber & Information Security, in consultation with Legal.

l. Internal-hosted technical Assets, other than user endpoint computers (workstations, laptops, VDIs), must be restricted from accessing any Internet destination.

m. User endpoint computers (workstations, laptops, VDIs) must be restricted from downloading executable files from any Internet source that is not considered “trusted” or otherwise authorized for this purpose via an authorized vetting and approval process, e.g., vendor sites, third-party providers, business partners, software providers.

n. User endpoint computers (desktops, laptops, VDIs) must be restricted from uploading information to:

   i. Internet-based file sharing or storage destinations (e.g., Box.com, GoogleDocs, Box.com, Apple Intune Device Backup), unless otherwise approved

   ii. Social media sites (e.g., Facebook, LinkedIn, Instagram, Twitter, MySpace)

   iii. College or university sites

   iv. Webmail sites (e.g., Yahoo Mail, Gmail)

   v. Internet or “cloud” printing (HP, FedEx)

   vi. Any site rated “high” or “medium” risk or flagged as “uncategorized” by the Point32Health-approved web proxy solution

o. User endpoint computers (desktops, laptops, VDIs) must be restricted from accessing any Internet destination that is not accessible via standard ports and protocols: 80 (http) and 443 (https).

p. Email filtering systems must be installed to remove any executable files or potentially malicious file attachments from incoming and outgoing email.

q. Electronic mail (incoming and outgoing) must be scanned for malware before being made accessible to colleagues.

r. Email filtering systems must automatically quarantine emails with suspicious email attachments and automatically remove specific file attachments.

4. SECURITY LOGGING AND MONITORING

a. The following security-related events must be captured and stored in a secured location on the network approved by Cyber & Information Security, where they will be continuously monitored for unauthorized activity:

   i. Granting, modifying, or revoking access rights, including creation of new users or groups; user privilege modifications; changes to file, folder, or database object permissions; and user password changes

   ii. User logon and logoff events

   iii. Clearing of an audit log, modification to audit log settings, or re-routing the audit log

   iv. Changes to firewall rules

   v. Suspicious/malicious activity, such as activity from an intrusion detection or prevention system, anti-virus or anti-spyware system

b. Security logs must include the source and destination information (e.g., system name, IP address, etc.), the identity of the account or user, and a timestamp of the event.

c. The captured logs must be made available online for at least 30 calendar days and at least 10 additional months of aggregated security event logs must be made available via archive storage.

d. Access to aggregated security-related logs must be provisioned in accordance with the principle of least privilege, allowing access only to those individuals with a job-related need.

5. CHANGE MANAGEMENT

a. All security-related configuration changes to in-scope assets must follow the corresponding Point32Health Change Management process.

6. ENCRYPTION

a. All encryption and signature algorithms used must meet the current version of the Federal Information Processing Standards (FIPS) Publication 140-2.
b. Keys used in the cryptographic process must be securely generated, distributed, and stored.
c. Master recovery/root keys for each encryption implementation must be centrally managed and secured.
d. Internal certificates cannot have expirations that exceed the following:
   i. Internally trusted certificates: 4 years
   ii. Internally trusted root and issuing certificates: 10 years

e. External certificates cannot have expirations that exceed the following:
   i. Externally trusted certificates: 3 years
   ii. External trusted root and issuing certificates: 10 years

f. The following must be encrypted:
   i. Transmission of system or user log-in credentials
   ii. Transmission of restricted or highly restricted information between untrusted networks and the trusted Point32Health internal network (e.g., DMZ to internal network)
   iii. Transmission of restricted and highly restricted information between an untrusted network and any other untrusted network (e.g., DMZ to cloud-hosting provider)
   iv. Transmission of all HTTP, FTP, Telnet, and ODBC traffic (internal and external)
g. Databases that host restricted or highly restricted information must be encrypted at rest.
h. All hard disks on local workstations and laptop computers must be encrypted.
i. Any multi-function printer with local storage (e.g., hard disks) must be encrypted.
j. Restricted or highly restricted information transmitted to authorized external parties, including third-party providers, vendors, and business partners, must be encrypted.

7. REMOVABLE MEDIA

a. By default, information users must not be allowed to write information to removable media (e.g., USB thumb drives, SD cards, CD/DVD, etc.).

8. REMOTE ACCESS

a. Colleagues and contingent resources remotely connecting to the Point32Health network infrastructure must utilize Point32Health endpoint computing devices and connect through a secure, virtual access tunnel (i.e., VPN).
b. Colleague and contingent resource remote access solutions must restrict direct access (“split tunneling”) to all non-Point32Health environments that have not specifically been approved within the corresponding secure configuration, as stated in the Technical Baseline document.
c. Remote access from non-Point32Health devices must limit access to only specific systems, applications, activities, and information that are required to meet contractual obligations. This access will also be restricted by approved static IP address ranges provided by the external entity. If the entity does not have a static IP address, a limited VPN access point for this specific purpose will be provided to support external vendor user connections.
d. Remote access to the Point32Health environment must be verified, in writing, by the Point32Health relationship managers no less than once every six months or whenever changes are made. Relationship managers should also keep an inventory of systems accessed and maintain a list of active user rosters by external entities. Revisions should be reported via a ServiceNow ticket and processed within 24 hours of notification.
e. All remote access to network devices, middleware, platforms, or operating systems must make use of approved remote access solutions. Administrative access to these devices must not be allowed directly from the public internet, telephone/modem, or other untrusted networks.

9. PERSONAL MOBILE DEVICES

a. Only devices with approved mobile device management software installed will be allowed to access Point32Health Assets.
b. Approved mobile device management software must enable the following minimum control requirements:
   i. A minimum of a six (6) character PIN or password is required before access is to Point32Health resources is permitted. Biometric authentication is authorized for use as a alternate means of authentication.
   ii. Timers must be set to require reauthentication after no more than 5 minutes of inactivity.
   iii. Restrict ability to copy or download Point32Health information to any location that is not owned or managed by Point32Health.

10. ASSET MANAGEMENT

a. All technology assets owned or managed on behalf of Point32Health, including those hosted externally, in a DMZ, and in a cloud environment, including SaaS applications and APIs, must be inventoried and logically organized.
b. Asset inventories must include asset name, business ownership information, IT support resource information, application(s) supported, and all generic accounts used to support the asset, where applicable.

III. EXCEPTION MANAGEMENT

Inability to meet the requirements set forth in this Information Security standard poses a potential risk to the Point32Health organization. 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 for applying material security changes to the existing environment, where applicable.