Point32Health

C&IS 008: CYBER & INFORMATION SECURITY THIRD-PARTY 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 Risk Assessment Standard.

The Cyber & Information Security Committee is responsible for approving the Cyber & Information Security Risk Assessment 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 Cyber & Information Security Standard 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 set of consistent requirements for assessing and addressing inherent risk associated with third-party vendors and providers. All colleagues are required to adhere to the requirements and objectives within this standard when engaging with any new third-party, adjusting the scope of services of an existing third-party, altering the type and/or volume of information accessed, or modifying how the existing third-party accesses assets, e.g., information, systems, applications, facilities.

3. SCOPE

The focus of this Standard is to assess and manage inherent risks associated with third-party providers with access to any of Point32Health's assets, e.g., information, systems, applications, facilities. It is important to enforce that this standard is not limited to third parties with access to personal information (PI) or protected health information (PHI); third-party providers with access to any information owned, managed, created by, or created on behalf of Point32Health are considered within scope of this standard. Also included within the scope of this standard are technology-hosting providers, software providers, employee benefits providers, third parties with physical access to Point32Health facilities, and third parties that have been provided with remote access to the Point32Health network.

This Standard is not intended to provide specific technical requirements associated with secure transmission or storage of information at or between Point32Health and the third-party provider. These control requirements are defined in other Cyber & Information Security standards and may be included within the scope of a security risk assessment.

This Standard only refers to those aspects of a third party's contract and capabilities associated with Cyber & Information Security. This Standard does not address other contractual obligations that may need to be performed by Procurement, Legal, Privacy, or other internal resources.

Third-party vendors retained for purposes of purchasing commodity-based office equipment that will never be connected to the Point32Health network, Internet, wireless network, cellular, or satellite networks, e.g., paper, chairs, desks, are considered out-of-scope for this standard.

4. ROLES AND RESPONSIBILITIES

a. **Cyber & Information Security** – Subject matter experts reporting into the Cyber & Information Security division of the IT Department. Cyber & Information Security is responsible to assess the inherent risk and mitigating security controls of the third-party provider and for delivering assessment results to the appropriate risk owner.

b. **Enterprise Security, Privacy, and Resilience Committee** – Approves the non-technical Information Security Standards, recommends standard effective dates, and support the need for departments or divisions they represent to develop implementation plans. Accountable for ensuring that departments or divisions represented are adhering to the Standards.

c. **Asset Owner** – A Point32Health employee 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.

d. **Information 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. All third-party relationship owners are considered the custodian for all Point32Health information or systems/applications accessible by the third-party vendor/service provider. Custodians shall obtain input and approval from the appropriate asset owners before submitting risk acceptance, depending upon the type of risk. As

examples, risks to the disclosure, modification, or destruction of information must be approved by the corresponding information asset owner(s).

e. **IT Support Resources / IT Managers** – Individuals that work in a technical capacity to design, install, configure, integrate, develop, QA, support, or maintain assets (e.g., developers, server/networking specialists, database administrators, software engineers, app dev/analysts, quality analysts, business analysts, etc.). IT Support resources and/or their managers are responsible for engaging with Cyber & Information Security to gain support for proposed remediation plans where safeguards have not previously been applied or are no longer adequate, in accordance with the Cyber & Information Security Policy and Standards. Upon gaining approval and support from Information Security, they are responsible for implementing the approved remediation plan and reporting progress to Cyber & Information Security towards the completion of that approved plan.

f. **Point32Health Manager** – All colleagues who have a job title referencing the term "manager" or have one of more colleagues reporting directly and/or indirectly to them. Responsible for awareness of the Information Security standards and ensuring that requirements defined within the standards are adhered to within their areas of responsibility, as appropriate.

   If unable to comply with the published standards, the responsible Point32Health manager must escalate to their leadership and to appropriate Cyber & Information Security representative(s).

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 and 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. **Inherent Risk Rating** – The severity of consequence to Point32Health of a given Asset being compromised or otherwise made unavailable. Assets are assigned a Potential Business Impact Rating of: Tier 1 (Very High), Tier 2 (High), Tier 3 (Medium), Tier 4 (Moderate), and Tier 5(Low). The following criteria are considered when determining the Potential Business Impact Rating:
   i. type of information: personal, financial, client, intellectual property
   ii. information classification: Public, General Business, Restricted, Highly Restricted
   iii. volume of information
   iv. financial impact
   v. business dependency upon the Asset (business criticality)
   vi. systems, applications, computing environments, and facilities available to the third-party

c. **Third-Party Providers** - Include those that have access to Point32Health information that is not assigned a classification of "Public" or is not otherwise in the public domain; technology-hosting providers; software providers; third parties with access to Point32Health facilities; and those with remote access to the Point32Health computing environment.

II. STANDARD

This Standard addresses third-party provider responsibilities in connection with the protection of Point32Health Information Assets, systems, applications, and other related resources.

1. SECURITY ASSESSMENT

The Information Custodian or designee must engage with the Point32Health Procurement Department to assist with the coordination of reviews and approvals by authorized representatives from Cyber & Information Security, Legal, Privacy and other stakeholders. All contracts, whether master agreements, statements of work, end user license agreements, non-disclosure agreements, or any other contract to support the procurement of products or services to be delivered by the external party in support of Point32Health's business operations, colleagues, customers, or members must include engagement by the Procurement Department. No contracts should be signed without first obtaining support to do so by Point32Health's Procurement Department, Cyber & Information Security, Legal, and other authorized stakeholders.

Once engaged, Cyber & Information Security resources will assess the third-party provider's security control capabilities to ensure that they are able to appropriately meet expectations associated with protection of information, systems, applications, and resiliency of business operations. When the security risk assessment has been completed, a summarized report of security issues and recommendations will be shared with the Information Custodian.

Access to information, technology resources, applications, or facilities may not be granted to the third-party until the security risk assessment has been completed and any identified risks have been recognized and addressed (accepted, corrected, mitigated).

The following represent the minimum third-party security controls that will be reviewed and retained by Cyber & Information Security, where applicable:

i. human resources
ii. Cyber & Information Security governance and risk management
iii. identity and access management
iv. network security
v. physical security
vi. information systems acquisition, development, and maintenance
vii. application security
viii. third-party and offshore security
ix. business continuity and disaster recovery
x. privacy-related security requirements
xi. information handling and destruction, and
xii. threat detection & response
xiii. data protection

2. ASSURANCE LEVELS

a. The Information Custodian entering the contract must collaborate with Cyber & Information Security to confirm the Potential Business Impact Rating of the Asset(s) accessible by the third-party provider. The Cyber & Information Security assigned resource will use this information to help ensure that the third-party provider meets the relevant security requirements to adequately address the inherent risk introduced.

b. Assessment activities must be aligned in accordance with the Information Security Potential Business Impact Rating.
    i. Contracts must be validated per Section 3 (“Contract Management”) below when the Cyber & Information Security Potential Business Impact Rating for a third-party provider has been assigned as Tier 1, 2, 3, or 4.
    ii. Security controls must be assessed, commensurate with the scope of service, for third-party providers rated Tier 1, 2, or 3.
    iii. Findings must be reported to the Information Custodian upon review of contracts and/or completion of the security controls assessment.
    iv. Risks must be addressed according to the Cyber & Information Security Risk Assessment Standard requirements. Acceptance of risks by the Asset Owner must occur prior to any finalization of contractual terms and conditions.

3. CONTRACT MANAGEMENT

a. Legal, in coordination with Cyber & Information Security, will ensure that contracts contain assurances in the following areas, as appropriate:
    i. third-party provider’s security program aligned with an industry-recognized framework.
    ii. compliance with applicable laws and regulations for the services to be performed
    iii. Point32Health’s right to audit
    iv. notification to Point32Health of a security breach
    v. in-depth background checks of the third-party provider’s employees and contingent workers
    vi. written consent prior to sharing any of Point32Health’s information with any external party
    vii. written consent prior to engaging with any third-party provider (vendor) that is owned, operated, managed by, or makes use of resources located outside of the United States to support services issued to Point32Health
    viii. Point32Health’s right to request secure disposal and destruction of Point32Health information or property
    ix. business continuity and disaster recovery plans commensurate with the Point32Health business criticality and associated recovery expectations
    x. authentication requirements; and
    xi. encryption requirements

4. SECURITY CONTROLS ASSESSMENT

a. Cyber & Information Security will ensure that third-party providers demonstrate security control assurances as appropriate.
    Results of independent assessments must be provided to Cyber & Information Security where available (e.g., SSAE 18 SOC 2 report, HIPAA certification, ISO 27001 certification).
b. Evidence of the third-party provider’s current security controls must be made available upon request.
c. When a third-party provider hosts or otherwise manages Point32Health information, systems, applications, software, or technology infrastructure, they must:
    i. provide evidence of Restricted and Highly Restricted information being encrypted at-rest and in-transit; and
    ii. provide evidence of multi-factor authentication implemented for remote access to any Restricted or Highly Restricted information; and
    iii. Provide evidence of multi-factor authentication implemented for any privileged access

d. When technology hosting is provided, the third-party provider must:
   i. deliver evidence and summarized results of an independent application assessment (e.g., penetration test) of all externally facing systems and applications used to support the Point32Health organization. Application assessments must be performed at least annually; and
   ii. collaborate with Point32Health stakeholders to address requests to correct or mitigate any control deficiencies or vulnerabilities which place Point32Health information, systems, applications, or services at risk.
e. When third-party services require high availability, evidence of appropriate business continuity and recovery plans and testing must be provided.

5. ASSURANCE INTERVALS

a. Potential Business Impact Rating criteria must be reviewed and validated by the custodian (relationship owner) of the third-party provider at least every three (3) years

b. Assessments must be performed by Cyber & Information Security for all:
   i. new third-party provider relationship or contracts, and
   ii. existing third-party providers during the contract renewal process and/
   iii. during negotiation of any changes to the scope or type of service being provided, including any new or upgraded Statements of Work that include

c. Security assessments must be performed periodically to maintain visibility into the third-party provider's security posture:
   i. An annual security risk assessment must be performed for third-party providers assigned with a Tier 1–Very High, Potential Business Impact Rating
   ii. A security risk assessment must be performed every two years for third-party providers assigned with a Tier 2-High, Potential Business Impact Rating if PII or PHI is at risk
   iii. A security risk assessment must be performed every three years for third-party providers assigned with a Tier 3-Medium, Potential Business Impact Rating if PII or PHI is not at risk
   iv. A security risk assessment may be performed for third-party providers assigned with a Tier 4-Moderate, Potential Business Impact Rating upon request by the custodian or by Cyber & Information Security at its sole discretion

III. EXCEPTION MANAGEMENT

Inability to meet the requirements set forth in this 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 Policy and Standards, 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 its publication. During the 90-day period, impacted technical and business stakeholders must complete a gap analysis and a recommended target to be provided to the CISO for applying material security changes to the existing environment, where applicable.