Point32Health

C&IS 003 – CYBER & INFORMATION SECURITY RISK ASSESSMENT 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, consistent methodology for assessing, reporting, and addressing identified security risks with a focus on the confidentiality, integrity, and availability of Point32Health's information and technology assets.

3. SCOPE

This standard may apply to any information asset, system, application, or business process that may introduce an information security risk to Point32Health.

4. 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. **Cyber & Information Security Committee** – This committee approves and implements the non-technical Information Security standards; recommends standard effective dates; and ensures that the departments or divisions they represent 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. **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), or risks to the availability of systems and business services must be approved by the corresponding technology asset owner, or their authorized delegates.

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 employees 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. **Potential Business Impact Rating** – The severity of consequence to Point32Health resulting from a given asset being compromised or otherwise made unavailable. Assets are assigned a potential business impact rating of: Tier 1 (highest severity), Tier 2, Tier 3, Tier 4, and Tier 5 (lowest severity). The following criteria are considered when determining the potential business impact rating:
    i. Type of information: personal information, protected health information, financial, client, intellectual property
    ii. Information classification: public, general business, restricted, highly restricted
    iii. Volume of information (e.g., number of unique records)
    iv. Financial impact
    v. Business dependency (criticality) upon the asset.

c. **Threat/Hazard** - A potential (future) event that, if realized, may cause measurable harm to the confidentiality, integrity, or availability of an asset or business process.

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

e. **Likelihood** – A scale indicating the probability of a threat occurring based upon the following criteria, where available and applicable:
    i. Threat/hazard type: ransomware, business email compromise, denial of service, etc.
    ii. Environmental exposure: internal, Internet, third-party managed, etc.
    iii. Exploitability: industry familiarity, exploit available, complexity, etc.

f. **Business Risk Category** - The type of impact that may occur in the event of a risk being realized:
    iv. Business interruption
    v. Brand / reputational damage
    vi. Financial impact
    vii. Legal / regulatory impact
    viii. Competitive advantage

II. STANDARD

1. CYBER & INFORMATION SECURITY RISK ASSESSMENT

a. Cyber & Information Security must maintain a Cyber & Information Security Risk Assessment process to identify, rate, report and address cyber & information security-related risks.

b. Risk Assessments must be performed, documented, and communicated to appropriate stakeholders to:
   i. Outline the occurrence of environmental changes that include, but are not limited to, technology architecture, users, applications, business processes and third-party relationships
   ii. Determine risks associated with information assets, IT assets, or business processes that exist within the organization but may not have recently been assessed
   iii. Validate that controls and safeguards currently in place continue to meet the organization's security expectations (targeted risk assessment)

c. Risk is determined by considering the potential business impact rating, threats, vulnerabilities, likelihood, and control(s) that may be in place.
   i. The risk rating assigned to a Point32Health asset or business process after a risk assessment has been completed must only consider safeguards and controls that are currently implemented and is referred to as the residual risk rating.
   ii. The risk rating assigned to a Point32Health asset or business process after considering existing safeguards and controls (residual risk rating), as well as those recommended to be implemented later (resultant risk rating).
   iii. One of four risk ratings will be assigned to identified risks: minor, important, significant, or major.

d. A risk repository must be in place to document and provide transparency of identified risks and risk owner remediation plan / efforts.

2. RISK TREATMENT

a. Risks may be addressed in four different ways:
   i. Eliminated: removal of the system or third-party relationship associated with the risk
   ii. Corrected: actions applied to a given asset such that the risk is no longer actionable
   iii. Mitigated: alternative workaround(s) applied to reduce the risk rating; often temporary
   iv. Accepted: no immediate action will be taken; assets will remain vulnerable until the risk is effectively eliminated, corrected, or mitigated

b. Risk acceptance, including those risks that have a future remediation date, requires written approval by the appropriate level of management authorized for the specific risk type. It is important to clarify that the asset owner with authority to accept risk may not be the same as the asset owner for which the vulnerability exists. Except for risks associated with underlying technology infrastructure, the Information Owner, or authorized delegate within their organizations will be responsible for risk acceptance:
   i. Minor: A Point32Health Manager or another delegate assigned by the asset owner (SVP)
   ii. Important: A vice president that reports into the asset owner's organization (SVP)
   iii. Significant: Asset owner (SVP) and chief information officer (SVP)
   iv. Major: Executive vice president and chief executive officer

c. Remediation plans to address identified risk:
   i. Must be documented and approved by the custodian and IT support resources / IT managers who support the asset, where applicable.
   ii. Must have an associated remediation plan owner and target completion date
   iii. Must be submitted to Cyber & Information Security within 30 calendar days of risks being identified and communicated.
   iv. Must be reviewed and agreed to by Cyber & Information Security Risk Assessment Services team to validate that the target resultant risk rating will be realized upon successful implementation of the remediation plan; and
   v. Must be tracked by the remediation plan owner and monitored by the custodian.

d. For temporarily accepted risk issues, progress toward remediation plans must be communicated to Cyber & Information Security at least quarterly.

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 Policy or standards, please contact: CyberInformationSecurity@point32health.org.

V. REFERENCE DOCUMENTS

VI. REVISION HISTORY

Version	Effective Date	Changed By	Change Description
1.0	April 1, 2024	Cyber & Information Security, Legal, Audit, ERM, Privacy, and other SMEs and stakeholders	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.