Point32Health

C&IS 001- CYBER AND INFORMATION SECURITY POLICY AND STANDARD FRAMEWORK

VERSION 1.0

I. INTRODUCTION 2
1. AUTHORITY 2
2. PURPOSE 3
3. SCOPE 3
4. ROLES AND RESPONSIBILITIES 3
5. DEFINITIONS 3
Figure 1: Cyber & Information Security Policy and Standard Framework 4
II. STANDARD 5
1. GOVERNANCE 5
2. STANDARD FORMAT 5
3. OVERSIGHT AND COMPLIANCE 5
III. EXCEPTION MANAGEMENT 6
IV. CONTACT INFORMATION 6
V. REFERENCE DOCUMENTS 6

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 define the Cyber & Information Security Policy and Standard Framework and approach for the creation, maintenance, communication and implementation of the Cyber & Information Security Policy and Standard Framework as part of Point32Health's system of internal control.

3. SCOPE

This standard identifies the components of the Cyber & Information Security Policy and Standards Framework, influencing factors, oversight, and governance.

4. ROLES AND RESPONSIBILITIES

a. **Cyber & Information Security** – A team of subject matter experts reporting into the Cyber & Information Security department. Reviews and revises the policy framework, including the development of new standards, and recommends material modifications of existing standards to the Enterprise Security, Privacy, and Resilience Committee. 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. **Enterprise Security, Privacy, and Resilience Committee** – Approves and implements the non-technical Cyber & Information Security Standards, recommends standard effective dates, and ensures that the departments or divisions they represent develop implementation plans. Ensures that departments or divisions represented are adhering to Cyber & Information Security Standards.

c. **Point32Health Managers** – All employees with a job title referencing the term "manager" or having one or more colleagues reporting directly and/or indirectly to them. Point32Health's managers are responsible for driving awareness of the Cyber & Information Security Standards and ensuring that requirements defined within these Standards are adhered to within their areas of responsibility, as appropriate.

   If unable to comply with the published standards, the responsible Point32health manager must notify Cyber & Information Security of any variance per the published Risk Assessment Standard.

d. **IT Support Resources** – Individuals who work in a technical capacity to design, install, configure, develop, QA, support, or maintain technical assets. This includes, but is not limited to 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. They may create and publish procedures, technical baselines, or implementation specifications that detail specific processes and steps necessary to comply with Cyber & Information Security Standards within areas of responsibility.

5. DEFINITIONS

a. **Policy –** Formal, high-level mandatory control goals, objectives, and expectations applicable to the entire organization.

b. **Standards –** Specific, mandatory control requirements and behaviors to ensure uniform control effectiveness across the organization.

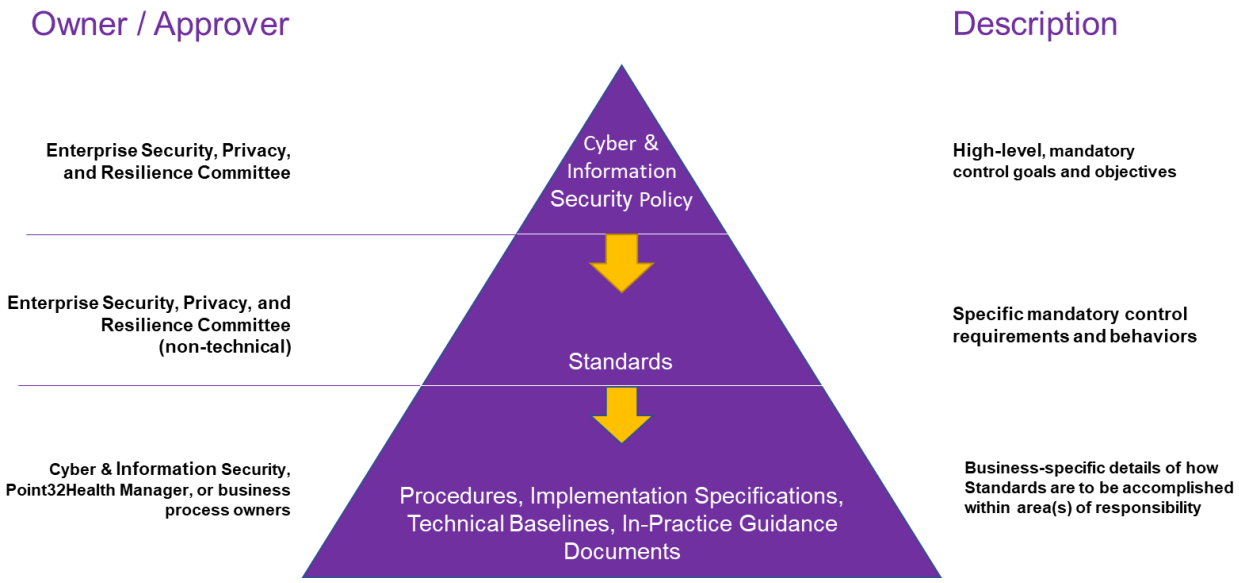
c. **Procedures –** Step-by-step instructions detailing how a particular control or standard is to be implemented, e.g., configuration steps, installation issues, business operating practices, and incident response playbooks.

d. **Implementation Specifications** – Approved implementation methods for supporting a specific standard, i.e., list of approved encryption algorithms, appropriate use of OneDrive, approved network-connected printer models, etc.

e. **Technical Baselines** – Minimum level of security configuration settings that technical assets (e.g., operating system, database, platform, network devices) must adhere to. Technical baselines take into consideration Cyber & Information Security requirements and are mapped to industry standards, such as the National Institute of Standards and Technology (NIST) or Center for Internet Security (CIS), if available.

f. **In-Practice Guidance Documents –** Provide recommended course of action related to the implementation of a specific control, as well as additional details or further context related to standards and procedures.

Figure 1: Cyber & Information Security Policy and Standard Framework



II. STANDARD

1. GOVERNANCE

    a. The Cyber & Information Security Policy must align with the organization's overall business objectives and is applicable across the entire organization. The Cyber & Information Security Policy is owned by the Enterprise Security, Privacy, and Resilience Committee, who is required to approve any recommended modifications to the policy.

    b. Cyber & Information Security Standards represent information security requirements that:
        i. Support the Cyber & Information Security Policy
        ii. Are applicable across the entire organization
        iii. Align to industry best practices
        iv. Respond to findings associated with corporate and solution risk assessments
        v. Includes required changes driven by legal and/or regulatory requirements

    c. Cyber & Information Security or the Enterprise Security, Privacy, and Resilience Committee must determine the need for a new Cyber & Information Security Standard.

    d. All Cyber & Information Security Standards must be communicated and published in a central repository that is accessible by all impacted stakeholders.

    e. Each Cyber & Information Security Standard must be reviewed annually by Cyber & Information Security to ensure its continued suitability, relevancy, and adequacy.

    f. All material changes reflected in the latest revision of the standard will become effective, on a go-forward basis, three (3) months after publication, unless otherwise noted. During the three (3) month period, impacted technical and business stakeholders must complete a gap analysis and a recommended target to the CISO of when material security changes will be applied to the existing environment to adhere to the current security requirements, where applicable.

2. STANDARD FORMAT

    a. All standards must be available in a format that is clearly understood by the intended audience.

    b. Each published standard must contain the last reviewed and approved date.

3. OVERSIGHT AND COMPLIANCE

    a. Point32Health's managers are responsible for ensuring the implementation of security requirements defined within the standards. When a business process, function or area is unable to comply with the published standards, the responsible Point32Health manager and/or IT support resource must notify Cyber & Information Security of any variance per the published Risk Assessment Standard.

    b. In support of providing oversight and governance, Cyber & Information Security is responsible for providing visibility of key issues and risk indicators to executive stakeholders.

III. EXCEPTION MANAGEMENT

The inability to meet the requirements set forth in this Cyber & Information Security Standard poses a potential risk to Point32Health. As such, any variance must be shared with Cyber & Information Security, who will then 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, Standards, please contact: CyberInformationSecurity@point32health.org.

V. REFERENCE DOCUMENTS

VI. REVISION HISTORY

Version	Approved Date	Published Date	Changed By	Change Description
1.0	April 1, 2024	April 1, 2024	Cyber & Information Security, various internal SME stakeholders	Initial publication