Point32Health

C&IS 002: CYBER & INFORMATION SECURITY INCIDENT MANAGEMENT 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, consistent methodology for defining the requirements associated with the identification, containment, eradication and recovery from Cyber & Information Security Events and Incidents. 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 in this document within their areas of responsibility.

3. SCOPE

This Standard applies to any information asset, system, application, or business process that may be or has been negatively impacted by a security threat.

4. ROLES AND RESPONSIBILITIES

a. **Cyber & Information Security** – Subject matter experts reporting into the Cyber & Information Security division of the IT Department who ensure that validation exercises (i.e., tabletop exercises, simulated incidents) with key stakeholders are conducted throughout the year – *target* quarterly.

b. **Crisis Management** – A structured, executive-level framework leveraged in times of a critical incident.

c. **Hazard-specific Event Lead** – An IT Department representative who is responsible for managing a Security Event. This person oversees, coordinates, and directs the response efforts being performed by one or more IT Department representatives and department-specific subject matter experts, as required.

d. **Security Event Logistics Coordinator (High and Critical)** – An authorized colleague who supports the Security Incident by coordinating meeting dates / times, scheduling conference lines, scheduling conference rooms and handling other logistics, as needed (i.e., food, drink, sleeping cots, "war room" coordination, equipment / software / license acquisition, etc.).

e. **IT Support Resources** – Individuals that 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 Admins, Software Engineers, App Dev/Analysts, Quality Analysts, Business Analysts, etc. IT Support Resources and/or their managers may be called upon during an incident to help assess the situation and remediate the exposure or provide recommendations to the Security Event Manager as needed.

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.

g. **IT Manager** – A Point32Health Manager with administrative responsibilities for one or more IT Support Resources. Responsible for ensuring that the technical security controls, as defined by the applicable Cyber & Information Security Standards and the Information Custodian, are appropriately implemented, and maintained.

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. **Security Event** – An event or act performed that negatively impacts or has a reasonable likelihood of negatively impacting, the confidentiality, integrity, or availability of Point32Health's Information Assets, systems, equipment, or operational practices because of a Cyber Threat or Trusted Insider, whether intentional or unintentional.

b. **Security Incident** – A Security Event that has been assigned a priority / criticality rating of "high" or "critical."

c. **Security Event Playbook** – Provides Hazard-specific Event Leads and participants with a vetted, consistent means by which to manage and communicate during the event/incident to identify, eradicate, and recover from Security Events efficiently and effectively.

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

e. **Asset** – Point32Health network, system, application, information, or business process that is owned or managed by Point32Health.

f. **Validation Exercise –** A process for evaluating the quality and accuracy of documented Security Event Playbooks. Helps familiarize key stakeholders with elements of the Playbook and reinforces basic knowledge of the response plan.

II. STANDARD

1. SECURITY EVENT MANAGEMENT STRUCTURE

a. IT Department representatives must be identified and authorized to lead all Low, Medium, and High Security Events and Incidents, both technical and non-technical. IT Department resources will triage all security events and assign a preliminary Security Event Priority Level as quickly as possible.

b. All Critical Security Incidents will be led by Point32Health's Crisis Management function.

c. The Hazard-specific Event Lead is the only individual authorized to communicate with business and technology stakeholders about the status and business impact of a Security Incident; authorization may be delegated and/or coordinated with other managers, as required.

d. The Security Event criticality level may only be modified once a successful knowledge transfer between the current and newly identified Hazard-specific Event Leads has occurred, if applicable.

2. SECURITY EVENT AND INCIDENT PRIORITY LEVELS

a. Security Event Criticality Levels are determined with consideration for the business impact, complexity of a given Threat/Hazard, and likelihood of a Threat/Hazard continuing to spread. The initial Security Event Criticality Level may increase but must never decrease. Characteristics and examples of Security Event Criticality Levels must be maintained in the accompanying procedure/playbook.

b. Security Event Criticality Levels must adhere to the following response and communication service level guidelines, unless otherwise noted within the accompanying procedure/playbook:

Security Event Criticality Level	**Security Event Manager Acknowledgment***	**Notification to Stakeholders After Strong Indication That Security Event Has Occurred**
Low	60 minutes	Not applicable
Moderate	60 minutes	2 hours
High	30 minutes	60 minutes
Critical	15 minutes	30 minutes

Hazard-specific Event Lead Acknowledgement refers to the assigned Event Lead's formal acceptance of responsibility for the Security Event either via the ServiceNow ticketing system or for high and critical priority events, live conversation with the IT Customer Support Desk ("IT Help Desk") representative or alternate resource.

Event Criticality Level	Characteristics (Any of the Items Listed Individually or in Combination)	Hazard-specific Examples (Cyber & Information Security)	Hazard Specific Event Lead (Cyber & Information Security) ** Approved playbooks may override*	Minimum Stakeholder Notifications
Low	- Any event if priority level not clear (i.e., event validated and impact unknown) - Minimal user or business impact - Event is contained - Single (qualified) point of contact is able to resolve	- Lost or stolen laptop, fully encrypted hard disk - Limited individuals have received malware and opened (not spreading) - Vulnerability scan from an external source	IT Help Desk, Desktop Support, C&IS Threat Analyst	N/A
Moderate	- Active threat/hazard, limited potential for further impact - Individual users impacted, not broadly impacting department or operation - Impact to colleagues, property, or operations is minimal - Can recover reasonably quickly using existing procedures or technology - Multiple resources in same function or department involved in response efforts	- Denial of service attempt, limited impact - Malware email communicated to several users, some have opened - Any ransomware variant or similar threat type (limited impact) - Alert of files written to removable media or internet storage locations - Previously implemented key security control stopped working - Potential for data loss but unconfirmed	C&IS Sr. Threat Representative, C&IS Manager	Hazard /Policy Owner Impacted Business Leaders (VP, SVP) Supporting Expert Teams (IT, C&IS, Legal, HR etc.)
High (Incident)	- High likelihood of system or information compromise or of financial loss - One or more business operations or departments have been impacted - High likelihood that damage to physical property, equipment will be extensive - Colleagues will likely need to be displaced from current physical location - Difficult to recover from event; requires coordinated effort	- Lost or stolen laptop or portable media - medium not encrypted - Ransomware spreading, not well contained - Successful denial of service - Threat intelligence or law enforcement notification of attack, compromise - Unauthorized transfer of sensitive information to portable media device - Unauthorized transfer of sensitive information to Internet destination - Successful transfer of funds to unauthroized external party	C&IS Threat Manager, C&IS Director, CISO	Hazard /Policy Owner Impacted Business Leaders (VP, SVP) Supporting Expert Teams (IT, C&IS, Legal, HR etc.) Point32Health IMWG *** Defer to approved playbook ***
Critical (Incident)	- Physical harm to people - Extensive damage to property or equipment - High volume of sensitive information compromised (e.g., PII, PHI, M&A plans) - High likelihood of meaningful reputational, financial, legal, or regulator impact - Coordinated effort to notify partners, customers, members, employees, etc. - Facilities will be unavailable for use for an extended period of time - Disastery Recover and/or Business Continuity Plan invoked	- Successful data exfiltration by internal or external parties - Network, equipment, systems, or application compromised by threat actor - Large-scal unrecoverable data due to ransomeware attack - Sustained denial of service (failed mitigating)	Named head of Crisis Management and any identified delegates/backup resources	Applicable IMWG Members, executives of impacted business(es), CLO, Head of PR, Head of Internal Comms

3. INCIDENT RESPONSE PROCESS

a. The Hazard-specific Event Lead must ensure that all suspected Security Events are recorded within Point32Health's ticketing system using the approved Security Event template. Cyber & Information Security will define requirements for the Security Event Categories, Resulting Impact Categories and Root Cause Categories that will be available within the Security Event template. Requirements and categories will be reviewed and validated at least annually by Cyber & Information Security.

b. Common types of Security Event Categories must have an accompanying procedure included in the C&IS Security Incident procedures *("playbook")*. A playbook outlines specific procedures to be taken to respond to a Security Event and serve as a script to assist Hazard-specific Event Leads and other IT resources to gather pertinent information. A playbook contains an up-to-date Security Event notification list and contact information.
    i Cyber & Information Security must identify the need for, and ensure assignment of, ownership for the development and continued maintenance of the C&IS Security Event procedures/playbooks. The C&IS Security Event playbooks must be documented, maintained, and approved by Cyber & Information Security.
    ii The playbook owners must maintain the currency of the playbook, including contact names and contact information. Further, the playbook owner must formally review and validate information within the playbook at least annually.

c. The Hazard-specific Event Lead, or their delegate, is responsible for management of the Event throughout its lifecycle from inception to post-analysis. This includes the following:
    i Logistics (e.g., meeting minutes, decisions, communications, ticket creation, etc.)
    ii Event management (e.g., identify, eradicate, recover)
    iii Reporting
    iv Communication with business and technology stakeholders about the status and business impact of a Security Incident if applicable
    v Post-incident analysis, including root cause analysis

4. SECURITY EVENT EXERCISES AND PLAYBOOK VALIDATION

Validation Exercises (i.e., tabletop exercises, simulated incidents) with key stakeholders must be conducted quarterly to determine if incident response processes need to be improved and/or to validate the strength of the existing protocols.

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. REFERENCE DOCUMENTS

VI. 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.