Point32Health

C&IS 007 – IDENTITY, CREDENTIAL & ACCESS MANAGEMENT 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

Point32Health is committed to protecting the security and privacy of its customers and employees. To ensure that only authorized personnel have access to sensitive information, we have established an Identity and Access Management (IAM) Standard. The purpose of this Standard is to provide a documented baseline of Cyber & Information Security requirements for granting, managing, and monitoring access to our technology and information assets. It is designed to ensure that only those with the appropriate authorization can access the information and systems they require to perform their assigned job duties, while protecting the confidentiality, integrity, and availability of Point32Health’s assets.

3. SCOPE

This Standard applies to identities, either interactive or non-interactive, that meet at least one of the following criteria:

- Can create, read, update, or delete information Assets
- Can access, install, modify, maintain, or support technical Assets.
- Supports one or more Point32Health business operational processes
- Supports logical access to physical buildings or to physical locations within a building, e.g., data centers, wiring closets, executive areas, Human Resources.

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 environments.

4. ROLES AND RESPONSIBILITIES

a. **Cyber & Information Security** – Subject matter experts reporting into the Cyber & Information Security division of IT. 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 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, Technology Asset Owner.

c. **Information Asset Custodians –** An Information Asset Custodian is a Point32Health colleague that is responsible for the implementation and oversight of necessary safeguards to protect the Information Asset, as defined by the Information Asset Owner (by assigning its Information Classification). Information Asset Custodians may be a business application owner or owner an application, file share, Microsoft SharePoint site, Microsoft Teams site, etc.
   i. IT Managers with responsibility for application and access management are doing so at the direction and delegation of the corresponding Information Asset Custodian.
   ii. All third-party relationship owners are considered the Information Asset Custodian for all Point32Health information or systems/applications accessible by the third-party vendor/service provider.
   iii. There may be more than one Information Asset Custodian of an Information Asset. External parties, including trusted partners, contingent resources, and outsourced providers are not authorized to be a Point32Health Information Asset Custodian.
   iv. Responsibilities of Information Asset Custodians include:
      - ensuring that access is strictly limited to the roles, individuals, and permissions required for the colleague(s) to effectively complete their job responsibilities; and
      - notifying Information Asset Owners of security control deficiencies and associated recommendations. Information Asset Custodians must collaborate with Information Asset Owners to address identified security control deficiencies, in accordance with the Information Asset Owner's expectations.

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, Platform Engineers, Database Admins, Software Engineers, App Dev/Analysts, Quality Analysts, Business Analysts, etc.). IT Support Resources apply security controls to protect and maintain technical Assets. IT Support Resources 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 Resources. Responsible for ensuring that the technical security controls, as defined by the applicable Cyber & Information Security Standards and the Custodian, are appropriately implemented, and maintained.

a. 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 Managers are responsible for awareness of the Information Security Standards and ensuring that applicable requirements defined within these Standards are adhered to within their areas of responsibility.

Are responsible for entering colleague termination information into the centralized HR system IMMEDIATELY upon being made aware of the colleague's pending departure from Point32Health.

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.

f. **Security Administrator** – An individual that has been delegated responsibility by a Custodian to:
1. Document a process to grant access, modify access, remove access, and periodically coordinate user access and entitlement reviews (UERs) for authorized parties, e.g., managers and application owners, to review and approve or update access of others.
2. Ensure that access is granted only when a documented request has been received and approved by an authorized party.
3. Ensure access is adjusted or removed in a timely manner upon an employment status change, e.g., termination, leave of absence, role change, that requires different access needs

5. DEFINITIONS

Account – A unique identifier created within a system, application, or other resource. There are various types of accounts, i.e., user account – assigned to a specific individual (e.g., colleague), system account – assigned to a specific system (e.g., server, database, network device), application account – assigned to a specific application (e.g., TAHPMaster, OHI), service account – assigned to a specific service (e.g., application, FTP, Web), shared account – account that is not assigned to a specific asset and whose credentials may be shared by more than one individual, such as accounts created for the specific purpose of training new colleagues.

Application Programming Interface (API) – APIs are interfaces used within software, platforms, and network devices that help to define how pieces of software interact with each other, control requests made between programs, how requests are made, and the format of information used.

API Key – A code used to identify and authenticate an identity (individual, asset, process) to an API.

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 Technical Asset represents any technology used to transmit, host, use, store, or destroy Information Assets or services by or on behalf of Point32Health.
Authentication – The process or action of verifying the identity of an individual, resource, technical asset, or organization based upon the credentials provided.

Authorization – The process or action of verifying that a successfully authenticated identity (through the authentication process) is approved to access a resource and which specific permissions the identity is approved (authorized) to perform.
Certificate – An electronic document that uses a digital signature to bind a public key with an identity. It is used to verify that a public key belongs to a certain individual, resource, technical asset, or organization and is applied in securing online communications, authenticating identities, and encrypting information.

Credential – Security principles used to authenticate a user or system before granting access to a system, network, application, or other resource. They may include account and password combinations, client ID and client secret pairings, API keys, security tokens, or digital certificates.

Dormant Account – An Information User's account that is enabled and accessible for use but has not been successfully logged on (authenticated) for a period of 45 calendar days.

Dormant Device – A Managed Device that has not been successfully logged into for a period of 45 calendar days.

Generic Account – Accounts that are not associated to a unique individual (e.g., system accounts, service accounts, application accounts, shared accounts, API keys, etc.).

Group Managed Service Account (GmSA) –Microsoft Active Directory domain accounts that provide automatic password management, simplified service principal name (SPN) management, and the ability to delegate management to other administrators.

Identity – A unique individual or technical Asset. An identity, e.g., colleague, must be unique but may have various properties or characteristics by which they may be identified, i.e., a colleague may have an account on the network that differs another account within an application, but the identity (colleague) does not change.

Just-in-Time Access – A security measure that allows an identity to access a system or application only when they need it, and for a limited amount of time. It is used to reduce the risk of unauthorized access to sensitive data or systems by limiting the amount of time a user has access to the system.

Local Administrator Password Solution (LAPS) – Manages the local Microsoft built-in account passwords of domain-joined Microsoft Windows based computers, e.g., laptop computers, virtual computers, servers. Passwords are stored in Active Directory (AD) and secured, allowing only authorized users to read or request a password (credential) reset.

Managed Device – Any device (e.g., laptop, server, firewall) that is configured and supported by or on behalf of Point32Health resources and provides a reasonable level of trust that Assets used or accessed by the device are secure.

Multi-factor Authentication (MFA) – Authentication of an identity via credentials that leverage more than an account and associated password, providing more confidence in the authentication process (supports the principle of nonrepudiation). Common examples of MFA include a unique, temporary code issued via an application such as Microsoft Authenticator and applied restrictions that permit an individual to login to a resource only from a Managed Device.

Passwords/Secrets – Authentication credentials, usually digital

Principle of Least Privilege – Requires that all identities be it user, program, and process be given the least amount of user rights and privileges necessary to complete an approved business process.

Privileged Account – (Also commonly referred to as an Administrator Account). account that has a level of access that allows it to perform actions that are beyond the scope of standard business users, including but not necessarily limited to:

- Override system or application controls
- Install or configure software, applications
- Override system or application files.
- Override or delete audit logs.
- Add/edit/delete user or permissions.
- Modify or delete critical business information

Rotation - The process of regularly changing credentials used to access assets or other resources.

Secrets Management– Secrets management refers to the tools and methods for managing credentials, including passwords, keys, APIs, and tokens for use in applications, services, privileged accounts, and other resources

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.

Access and Entitlement Review (AER) – The process of periodically reviewing access of accounts and their permissions to a given Asset (e.g., application, data repository, shared e-mail box, passwords), based on requirements of the identity (e.g., individual, system, application) to sufficiently perform the approved business function(s) of their job role or purpose (refer to Principle of Least Privilege).

II. STANDARD

Account and Access Management

1. Security Administrators are responsible for documenting and maintaining procedures related to access provisioning, access modifications (e.g., job responsibility changes, transfers), and access deprovisioning when access is no longer required, i.e., colleague termination, leave of absence, third-party provider contract termination.
2. Security Administrators are responsible for implementing the principle of least privilege, allowing only the access necessary for an individual to perform their job responsibilities or assigned tasks.
3. Security Administrators must maintain the following information about the identities (e.g., user IDs, generic IDs) and authorization lists (e.g., Active Directory groups, security tables, authorization files) for which they are responsible:
    i. Owner of the account created within the technical asset for which they are responsible, e.g., operating system, network device, database, application.
    ii. The identity (e.g., individual, application, process) associated with the account
    iii. Intended purpose of the identity, including any pre-authorized/default assigned permissions and systems/applications that the identify may have access to (if applicable).
    iv. Owner of authorization lists, e.g., Active Directory groups, API Keys, and corresponding authorizations/permissions associated with each authorization list
4. There are three (3) approved methods to manage access:
    i. Deliberate access: a documented request for access by one or more individuals is requested and approved by authorized individuals on an “as-needed” basis.
    ii. Role-based access: previously authorized and documented access to applications, systems, or data repositories is assigned to an individual based upon one or more job characteristics, such as the individual’s job title, location, department, operation, or cost center.
    iii. Partner managed: External entities, e.g., customers, brokers, providers, are authorized with privileged access to add, modify, or remove accounts associated with information for which they own. This approach often comes with the paradigm of “federated access” or “bring your own identity”, where the external entity can leverage their own accounts and credentials to authenticate to approved resources within a Point32Health owned/managed environment.
5. Upon determination that access is no longer required (due to Information User departure, role change, contract expiration, etc.), access must be disabled/revoked within one (1) business day of the effective termination date to the following assets:
    i. Network access, including remote access (VPN)
    ii. Secondary accounts specifically assigned to the individual
    iii. Microsoft Active Directory, including Microsoft 365 (e.g., MS Teams, SharePoint, email, calendar)
    iv. Mobile access, including access obtained through bring-your-own-device (BYOD) methods
    v. Systems, applications, and resources that are accessible from the Internet that do not use Microsoft Active Directory or Microsoft Azure AD (Entra) to authenticate
    vi. Point32Health Buildings /facilities

6. All systems, applications, and resources not required to revoke access within one business day are required to have access effectively disabled within 180 calendar days of the effective termination date
7. Accounts, email, and information in personal folders (e.g., user home directory, OneDrive) and all account log activity must be retained for a period of no less than 13 full months.
8. Dormant (inactive) accounts must be disabled within 15 calendar days of the account becoming dormant unless satisfactorily justified and approved by the account owner, account owner's manager (for individually assigned user accounts), or custodian.
9. Dormant devices registered in Microsoft Active Directory or Microsoft Azure (Entra) must be disabled within 15 calendar days of the device becoming dormant unless satisfactorily justified and approved by the device owner or custodian.

Access and Entitlement Reviews

1. Custodians or assigned Security Administrators must ensure that access and entitlement reviews are documented and performed for the following types of Assets and within the defined frequency, includes all account types. Information provided to those responsible for periodically reviewing and approving access must ensure that role and access descriptions are accurate, clearly defined, and provide meaningful information to the reviewers about specific resources and permissions (entitlements).
    i. Privileged access, including systems, applications, resources, IT infrastructure, Ops IT, cloud environments, security products, facilities/areas: biennial review by asset owner.
    ii. Third-party remote access: biennial review by asset owner (third-party relationship owner)
    iii. Security access exceptions (e.g., media, firewall rules, websites): annual review by manager
    iv. Role-based access templates: annual review with custodians
    v. Applications and information repositories authorized to contain personally identifiable information (PII), protected health information (PHI), or financial information: biennial review by managers.
    vi. Databases: annual review by appropriate IT Managers if host restricted or highly restricted data
    vii. File shares: annual review by file share owners
    viii. SharePoint sites: annual review by identified SharePoint owners.
    ix. Microsoft Teams sites: annual review by identified MS Teams owners
    x. Microsoft Exchange Outlook (e.g., public folders, shared e-mailboxes): annual review by owners
2. Access change requests that occur as a result of the access review must be processed by the Security Administrator within 45 days upon completion of the access and entitlement review cycle.

Identification and Authorization

1. All accounts, devices, and services must be uniquely identified and authenticated.
2. Shared Accounts used in Point32Health production environments or to access restricted or highly restricted information are prohibited, unless used in conjunction with an approved credential management tool to provide auditability and non-repudiation of the credentials being used.
3. Generic accounts must only be used for their intended Point32Health business purposes. Any use of such accounts to bypass security controls is strictly prohibited.
4. Unless otherwise approved by Cyber & Information Security, all internal Point32Health Identities (employees, contingent workers, contractors, co-ops, interns) must conform to the following minimum user account authentication controls:
    i. User Accounts (Not applicable to generic accounts or secondary accounts for privileged access)
        1. Must conform to approved account naming standards, e.g., business email address
        2. Passwords must be no less than eight (8) characters long and be enrolled in an approved risk-based multi-factor authentication solution, e.g., MS Azure AD Identity Protection
        3. Passwords must not be easy-to-guess, commonly used, or known to have been previously compromised
        4. Accounts must be disabled ("locked out") for a period of no less than 10 minutes after incurring five (5) consecutive unsuccessful login attempts within a 24-hour period
        5. Password changes must not permit reuse of the last 10 used passwords and must not be changed for one (1) day after being successfully changed (minimum password age)
        6. Access to the corporate network requires the use of approved multi-factor authentication
        7. Direct access to systems, applications, or resources from the Internet requires the use of approved multi-factor authentication

8. Registration of a new computer devices or systems, including registration of a new phone or tablet to support the bring-your-own-device (BYOD) capability, requires the use of approved multi-factor authentication

ii. Privileged Access
1. Must be avoided
2. Privileged Access must not be assigned to a colleague's primary user account. A secondary user account assigned specifically to the individual with assigned required privileged access must be created
3. Privileged access should be used on a limited basis (only when absolutely required) and access should be able to be correlated to a corresponding change request or incident/event or similar unique activity to have triggered the need to use privileged access credentials

iii. Secondary User Accounts assigned to individuals to perform privileged access functions
1. Must conform to approved account naming standards
2. Passwords must be managed by the approved privileged access management (PAM) solution including automated password selection and rotation, where possible
3. Passwords must be set to at least 24 characters and be changed within eight (8) hours of being accessed within the PAM solution and no less frequency than once per day
4. Passwords must not be easy-to-guess, commonly used, or known to have been previously compromised
5. Access to credentials within the PAM solution must be limited to only the individual for whom the secondary account has been created and must never be shared with others.
6. Access to obtain the password within the PAM solution requires the use of MFA by the individual assigned to the account (account owner)
7. Accounts must be logged off by the authorized colleague immediately after the task/activity has been completed

iv. Generic Accounts
1. Must conform to approved account naming standards
2. Generic Account must leverage MS LAPS (preferred) or MS GmSA, if feasible
3. If LAPS and the use of GmSA are not feasible options, passwords must be managed by the approved privileged access management (PAM) solution, including automated password selection and rotation
4. Passwords must be set to at least 24 characters and be changed within eight (8) hours of being accessed within the PAM solution and no less frequency than once per day
5. Passwords must not be easy-to-guess, commonly used, or known to have been previously compromised
6. Credentials must not be used directly on the colleague's assigned laptop/workstation but in a secure computing environment that is not directly accessible to the Internet and is closely monitored for suspicious and unauthorized activities
7. Access to credentials within the PAM solution must be limited to only the individual(s) approved for use by the corresponding asset owner or custodian
8. Access to obtain the password within the PAM solution requires the use of MFA by the authorized individual(s)
9. Accounts must be logged off by the authorized colleague immediately after the task/activity has been completed

v. Accounts created by the Security Administrator must have an assigned password that is unique to the account, conforms to all the password requirements, and securely communicated to the authorized owner or person(s) responsible for configuring the account within the PAM solution.

vi. Accounts must be technically forced to change their passwords immediately upon an administrative change (a change made by someone other than the user, e.g., IT Help Desk, Security Administrator)

5. Credentials, including passwords must:
i. Never be displayed in clear-text while being entered.
ii. Be securely stored (encrypted)
iii. Encrypted while being transmitted between identities, e.g., systems, applications, services
iv. All default or assigned credentials by vendors or external support resources to systems, applications, services, or resources must be changed prior to being implemented.
v. Must not be stored within application custom code or configuration files

vi. Credentials must never be stored outside of approved repositories, e.g., spreadsheet, MS Word documents, email, contacts lists, written down

6. Official Point32Health Social Media Accounts
   i. All social media accounts representing Point32Health in an official way, where postings are made to the public, shall implement Multi-factor Authentication.
   ii. The primary administrator-level social media account(s) shall be managed by the approved PAM solution
   iii. Must be associated with a Point32Health employee using their approved business email address, not a personal account with a personal email address
7. Authenticating identities via phone, text, and email
   i. Where leading technology used to authenticate individuals is not available, Point32Health service desk, IT Help Desk, and customer support functions must ensure that industry-leading practices are applied to confidently authenticate the identity of individuals before resetting passwords, granting system access, or sharing any non-public information with requestors.

III. EXCEPTION MANAGEMENT

Inability to meet the requirements set forth in this Standard poses a potential risk to the Point32Health organization. As such, all exceptions must be shared with Cyber & Information Security. Cyber & Information Security will assess the risk and recommend an appropriate course of action (e.g., eliminate, correct, mitigate, or accept the risk).

IV. CONTACT INFORMATION

For all inquiries / questions regarding the Cyber & Information Security Policy and Standards, 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.