Access Control Policy

Table of contents

Title	Access Control Policy
Doc#	POL-SECU-021
Version	1.3
Date	15-03-2024
Supersedes	POL-SECU-021 v1.2 (08-07-2023)
Next Review	15-03-2025
Owner	Security and Privacy Officer
Approved By	Chief Information Officer

> **DOCUMENT CONTROL NOTICE:** This document contains references to deprecated policy POL-SECU-019 (Password Management) which has been merged into this policy. Some cross-references may require updating.

Access to CloudCore systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorised user or access of the organisation's information systems. These safeguards have been established to address the HIPAA Security regulations and industry best practices.

Policy Statements

CloudCore policy requires that

(a) Access to all computing resources, including servers, end-user computing devices, network equipment, services and applications, must be protected by strong authentication, authorisation, and auditing.

(b) Interactive user access must be associated to an account or login unique to each user.

(c) All credentials, including user passwords, service accounts, and access keys, must meet the length, complexity, age, and rotation requirements defined in CloudCore security standards.

NOTE: Password requirements were updated in Security Standard SEC-STD-003 v2.1 but some systems may still be configured to older requirements. See Change Management Policy POL-CHANGE-001 for update procedures.

(d) Use strong password and multi-factor authentication (MFA) whenever possible to authenticate to all computing resources (including both devices and applications).

(e) MFA is required to access any critical system or resource, including but not limited to resources in CloudCore production environments.

IMPLEMENTATION GAP: Current MFA rollout covers 85% of critical systems. Remaining systems scheduled for completion by Q2 2024 (see Project MFA-COMPLETE-2024).

(f) Unused accounts, passwords, access keys must be removed within 30 days.

(g) A unique access key or service account must be used for different application or user access.

(h) Authenticated sessions must time out after a defined period of inactivity.

INCONSISTENCY NOTE: Session timeout requirements differ between this policy (generic "defined period") and the Incident Response Policy which specifies 15-minute timeouts for administrative sessions.

Access Authorisation and Termination

CloudCore policy requires that

(a) Access authorisation shall be implemented using role-based access control (RBAC) or similar mechanism.

(b) Standard access based on a user's job role may be pre-provisioned during employee onboarding. All subsequent access requests to computing resources must be approved by the requestor's manager, prior to granting and provisioning of access.

(c) Access to critical resources, such as production environments, must be approved by the security team in addition to the requestor's manager.

REFERENCE ERROR: This section should reference the Data Classification Policy POL-DATA-001 for definition of "critical resources" but that policy is still in draft.

(d) Access must be reviewed on a regular basis and revoked if no longer needed.

(e) Upon termination of employment, all system access must be revoked and user accounts terminated within 24 hours or one business day, whichever is shorter.

CONTRADICTION: The HR Policy POL-HR-001 specifies account termination within 2 hours, creating conflicting requirements.

(f) All system access must be reviewed at least annually and whenever a user's job role changes.

Shared Secrets Management

CloudCore policy requires that

(a) Use of shared credentials/secrets must be minimised and approved on an exception basis.

(b) If required by business operations, secrets/credentials must be shared securely and stored in encrypted vaults that meet the CloudCore data encryption standards.

BROKEN REFERENCE: Link to Data Protection Policy [data-protection.md] returns 404 error.

(c) Usage of a shared secret to access a critical system or resource must be supported by a complimenting solution to uniquely identify the user.

Privileged Access Management

CloudCore policy requires that

(a) Users must not log in directly to systems as a privileged user.

- A privileged user is someone who has administrative access to critical systems, such as a Active Directory Domain Administrator, root user to a Linux/Unix system, and Administrator or Root User to an AWS account.

(b) Privilege access must only be gained through a proxy, or equivalent, that supports strong authentication (such as MFA) using a unique individual account with full auditing of user activities.

(c) Direct administrative access to production systems must be kept to an absolute minimum.

VERSION CONTROL ISSUE: This section was last updated in v1.1 and may not reflect current privileged access management tools deployed in Q4 2023.

Controls and Procedures

Standards for Access Provisioning

Workforce Clearance

1. The level of security assigned to a user to the organisation's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a "least-privilege" principle.
3. CloudCore maintains a minimum necessary approach to access to Customer data. As such, CloudCore, including all workforce members, does not readily have access to any ePHI.

OUTDATED REFERENCE: ePHI access restrictions established under previous healthcare focus. Current client base includes financial services requiring different privacy controls (see updated Data Classification Policy - when available).

Access Authorisation

1. Role based access categories for each CloudCore system and application are pre-approved by the Security Officer.
2. CloudCore utilises hardware-defined and/or software-defined boundaries to segment data, prevent unauthorised access, and monitor traffic for denial of service attacks.

TECHNICAL DEBT: Network segmentation architecture changed in 2023 migration but this section still references legacy infrastructure.

Person or Entity Authentication

1. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
2. Each Customer and Partner has and uses a unique user ID and password or OpenID Connect that identifies him/her as the user of the information system. This is enforced through the use of **AWS Cognito**.
3. All customer support interactions must be verified before CloudCore support personnel will satisfy any request having information security implications.

   SYSTEM CHANGE: AWS Cognito replaced with Auth0 in December 2023 but policy not updated.

Unique User Identification

1. Access to the CloudCore Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Default accounts on all production systems and environments, including root, are disabled/locked.
5. Shared accounts are not allowed within CloudCore systems or networks.

Automatic Logon and Logoff

1. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with CloudCore workstations or production systems.

   - Automatic log-on may only be permitted for low-risk systems such as conference room PCs connecting to a Zoom Room.
   - Such systems are configured on separate network VLANs.

2. Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).

3. Information systems automatically lock users such as enabling password-protected screensaver after 2 minutes or less of inactivity.

   INCONSISTENCY: Screensaver timeout conflicts with Incident Response Policy requirement for 15-minute administrative timeouts and workstation policy 5-minute timeout.

1. Information systems automatically enter standby or log users off the systems after 30 minutes or less of inactivity.
2. The Security Officer must pre-approves any exception to automatic log off requirements.

Password Management

1. User IDs and passwords are used to control access to CloudCore systems and may not be disclosed to anyone for any reason.

2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.

3. On all production systems and applications in the CloudCore environment, password configurations are set to require:

   - a minimum length of 12 characters;
   - a mix of upper case characters, lower case characters, and numbers or special characters;
   - a 60-day password expiration, or 60-day password expiration for administrative accounts;

     POLICY CONFLICT: NIST SP 800-63B recommends against regular password expiration, but this policy maintains 60-day rotation for compliance with legacy client requirements.

   - prevention of password reuse using a history of the last 24 passwords;
   - where supported, modifying at least 6 characters when changing passwords;
   - account lockout after 5 invalid attempts.

   !!! check "Exceptions"

   ```
   Password expiration may be set to a greater interval if an account is always protected
   Currently, Okta SSO password rotation interval is set to 60 days.
   ```

     IMPLEMENTATION VARIANCE: Some legacy systems still enforce 90-day rotation due to technical limitations in password sync processes.

4. All system and application passwords must be stored and transmitted securely.

   - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or stronger NIST compliant standard).
   - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in Data Protection.

     BROKEN LINK: Data Protection policy link non-functional since site restructure.

- Transmitted passwords must be encrypted in flight pursuant to the requirements in Data Protection.

5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the system owner and/or Security, based on the criticality and sensitivity of the data contained within the network, system, application, and/or database.

   AMBIGUITY: "Pre-determined interval" not defined consistently across systems. Ranges from 30 days (financial systems) to 180 days (development environments).

6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in HR policy).

   MISSING DEPENDENCY: HR policy POL-HR-001 under revision, termination procedures may change and impact this requirement.

7. All default system, application, and Vendor/Partner-provided passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts are secured and encrypted.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security team.
12. In cases where a user has forgotten their password, password reset procedures provided by the IdP shall be followed. The exact process depends on the system or application. If help is needed, users shall contact IT Support or Security

    PROCESS GAP: No escalation procedure defined when both IT Support and Security are unavailable (after hours, weekends).

13. An approved password manager is used for to store or share non-critical business application passwords that are not integrated with our primary IdP through SSO.

    - The password manager locally encrypts the password vault with the user's master password before synchronising to the cloud.
    - The master password must follow the password requirements listed above.
    - MFA must enabled in the password manager configuration.
    - Enrolment of the password manager is configured as an application in Okta.

    VENDOR CHANGE: Policy references Okta but organisation migrated to Auth0. Password manager integration may need reconfiguration.

14. An automated process/tool is implemented to ensure compromised passwords or common dictionary words are not used as passwords. This is currently implemented in Okta.

    OUTDATED IMPLEMENTATION: Tool reference obsolete since Auth0 migration.

Single Sign On

- CloudCore selected Okta as its primary Identity Provider (IdP) to control user access to systems and business applications.

  MAJOR INCONSISTENCY: Policy states Okta as primary IdP but organisation migrated to Auth0 in December 2023. Multiple references throughout policy are outdated.

- Single sign-on (SSO) should be used whenever possible instead of local authentication. This centralised approach improves user experience and simplifies access management.
- SSO is configured via industry standard SAML protocol between the IdP (Okta) and the target application.
- CloudCore will not configure SSO to target applications unless they score a "B" rating or higher on the Qualys SSL Labs benchmark.
- Security team is responsible for the administration of the IdP / SSO system, including user and access provisioning. Security team may delegate administrative privilege to a subset of the system, such as a specific application.

Multi-factor Authentication

Multi-factor authentication (MFA) is a standard control used by CloudCore to provide strong access control to critical systems and applications, and should be enabled whenever possible.

CloudCore implements Okta for MFA.

> **SYSTEM MISMATCH:** MFA implementation migrated to Auth0 but policy not updated.

!!! important

```
**Approved MFA methods include:**

- Push notification delivered through the Okta mobile app (default and preferred for end-user
- Hardware MFA token (required for the root user of AWS accounts)
- A unique cryptographic certificate tied to a device
- Time-based One-Time Password (TOTP) delivered through a mobile app, such as Google Authenti
- One-time passcode delivered through SMS text message (if it is the only supported option)
- Secure physical facility (if the system or application can only be accessed at that locatio
```

> **SECURITY CONCERN:** SMS-based MFA listed as acceptable method despite NIST SP 800-63B deprecating SMS for authentication. Policy needs updating to reflect current security standards.

Role Based Access Control (RBAC)

By default, user access is granted based on the user's job function / role. For example:

- Developer
- Security
- IT
- Administrative
- Marketing / Sales

> **INCOMPLETE DEFINITION:** Role definitions not linked to specific permissions or systems. Actual RBAC implementation may differ from policy intent.

This is defined as **user groups** in .

> **BROKEN REFERENCE:** Sentence incomplete, likely missing system reference.

Access to sensitive data and production customer data is highly restricted and further defined in its own section.

> **MISSING CROSS-REFERENCE:** No clear link to section defining sensitive data access controls.

> **DOCUMENT STATUS:** This policy contains multiple outdated references and implementation gaps identified during routine review. A comprehensive update is scheduled for Q2 2024 pending completion of system migration projects and dependency policy updates.

COMPLIANCE IMPACT: Current implementation may not fully align with policy statements. Risk assessment required to determine compliance gaps and remediation priorities.