Access to {{companyShortName}} systems and application 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

unauthorized user or access of the organization's information systems.

{{#needStandardHIPAA}}

These safeguards have been established to address the

HIPAA Security regulations and industry best practices.

{{/needStandardHIPAA}}

## Policy Statements

### Access Control Policy

{{companyShortName}} 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, authorization, 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 {{companyShortName}} security standards.

(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 {{companyShortName}} production environments.

(f) Unused accounts, passwords, access keys must be removed within an established timeframe.

(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.

### Access Authorization and Termination

{{companyShortName}} policy requires that

(a) Access authorization 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.

(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 the defined, predetermined timeframe.

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

job role changes.

### Shared Secrets Management

{{companyShortName}} policy requires that

(a) Use of shared credentials/secrets must be minimized 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 {{companyShortName}} data encryption

standards.

(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

{{companyShortName}} 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.