IS-7 SYSTEM ACCESS POLICY

**7.1 System Access Policy**

Access to <COMPANY NAME> systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized use or access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations including the following:

**7.2 Access Establishment and Modification**

Requests for access to <COMPANY NAME> Platform systems and applications are made formally using the following process:

1. A <COMPANY NAME> workforce member initiates the access request by creating an Issue in the <COMPANY NAME> ticketing system
	1. User identities must be verified prior to granting access to new accounts.
	2. Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
	3. For new accounts, the method used to verify the user's identity must be recorded on the Issue.
2. The Security Officer or Privacy Officer will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
3. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the request. If the request is rejected, it goes back for further review and documentation.
4. If the review is approved, the Security Officer or Privacy Officer then marks the request as Done, adding any pertinent notes required. The Security Officer or Privacy Officer then grants requested access.
	1. New accounts will be created with a temporary secure password that meets all requirements from [§7.12](#7.12-password-management), which must be changed on the initial login.
	2. All password exchanges must occur over an authenticated channel.
	3. For production systems, access grants are accomplished by adding the appropriate user account to the corresponding LDAP group.
	4. For non-production systems, access grants are accomplished by leveraging the access control mechanisms built into those systems. Account management for non-production systems may be delegated to a <COMPANY NAME> employee at the discretion of the Security Officer or Privacy Officer.

Access is not granted until receipt, review, and approval by the <COMPANY NAME> Security Officer or Privacy Officer.

The request for access is retained for future reference.

**Access Reviews**

All access to <COMPANY NAME> systems and services is reviewed and updated on a bi-annual basis to ensure proper authorizations are in place commensurate with job functions. The process for conducting reviews is outlined below:

1. The Security Officer initiates the review of user access by creating an Issue in the <COMPANY NAME> Ticketing System
2. The Security Officer is assigned to review levels of access for each <COMPANY NAME> workforce member.
3. If user access is found during review that is not in line with the least privilege principle, the process below is used to modify user access and notify the user of access changes. Once those steps are completed, the Issue is then reviewed again.
4. Once the review is completed, the Security Officer approves or rejects the request. If the request is rejected, it goes back for further review and documentation.
5. If the review is approved, the Security Officer then marks the request as Done, adding any pertinent notes required.

**Access Modifications**

1. Any <COMPANY NAME> workforce member can request change of access using the process outlined 7.2-access-establishment-and-modification).
2. Access to production systems is controlled using centralized user management and authentication.
3. Temporary accounts are not used unless absolutely necessary for business purposes.
	1. Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
	2. Accounts that are inactive for over 90 days are removed.
4. In the case of non-personal information, such as generic educational content, identification and authentication may not be required. This is the responsibility of <COMPANY NAME> Customers to define, and not <COMPANY NAME>.
5. Privileged users must first access systems using standard, unique user accounts before switching to privileged users and performing privileged tasks.
	1. For production systems, this is enforced by creating non-privileged user accounts that must invoke `sudo` to perform privileged tasks.
	2. Rights for privileged accounts are granted by the Security Officer or Privacy Officer using the process outlined in 7.2-access-establishment-and-modification).
6. All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
7. Generic accounts are not allowed on <COMPANY NAME> systems.
8. Access is granted through encrypted, VPN tunnels that utilize two-factor authentication.
	1. Two-factor authentication is accomplished using a Time-based One-Time Password (TOTP) as the second factor.
	2. VPN connections use 256-bit AES 256 encryption, or equivalent.
	3. VPN sessions are automatically disconnected after 30 minutes of inactivity.
9. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access.
10. Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.

**7.3 Workforce Clearance**

1. The level of security assigned to a user to the organization'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-access principle."
3. <COMPANY NAME> maintains a minimum necessary approach to access to Customer data. As such, <COMPANY NAME>, including all workforce members, does not readily have access to any ePHI.

**7.4 Access Authorization**

1. Role based access categories for each <COMPANY NAME> system and application are pre-approved by the Security Officer, or an authorized delegate of the Security Officer.
2. <COMPANY NAME> utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

**7.5 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 that identifies him/her as the user of the information system.
3. All Customer support desk interactions must be verified before <COMPANY NAME> support personnel will satisfy any request having information security implications.
	1. <COMPANY NAME>'s current support desk software, requires users to authenticate before submitting support tickets.
	2. Support issues submitted via <COMPANY NAME>'s dashboard require that users authenticate with their <COMPANY NAME> account before submitting support tickets.
	3. Support issues submitted by email must be verified by <COMPANY NAME> personnel using a phone number that has been registered with the corresponding account.

**7.6 Unique User Identification**

1. Access to the <COMPANY NAME> 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, including root, are disabled.
5. Shared accounts are not allowed within <COMPANY NAME> systems or networks.
6. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with <COMPANY NAME> workstations or production systems.

**7.7 Automatic Logoff**

1. 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).
2. Information systems automatically log users off the systems after 15 minutes of inactivity.
3. The Security Officer pre-approves exceptions to automatic log off requirements.

**7.8 Employee Workstation Use**

All workstations at <COMPANY NAME> are company owned, and all are laptop products running Windows, Mac OSX or Linux.

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through the organization's system.
3. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
4. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
5. Transmitted messages may not contain material that criticizes the organization, its providers, its employees, or others.
6. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
7. Workstation hard drives will be encrypted using Butlocker, FileVault 2.0 or equivalent.
8. All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.
9. All workstations are to have the following messages added to the lock screen and login screen: \*This computer is owned by <COMPANY NAME> , Inc. By logging in, unlocking, and/or using this computer you acknowledge you have seen, and follow, these policies (https://policy.<COMPANY NAME>.com) and have completed this training (https://training.<COMPANY NAME>.com/). Please contact us if you have problems with this - privacy@<COMPANY NAME>.com.\*

**7.9 Wireless Access Use**

1. <COMPANY NAME> production systems are not accessible directly over wireless channels.
2. Wireless access is disabled on all production systems.
3. When accessing production systems via remote wireless connections, the same system access policies and procedures apply to wireless as all other connections, including wired.
4. Wireless networks managed within <COMPANY NAME> non-production facilities (offices, etc.) are secured with the following configurations:
	1. All data in transit over wireless is encrypted using WPA2 encryption;
	2. Passwords are rotated on a regular basis, presently quarterly. This process is managed by the <COMPANY NAME> Security Officer.

**7.10 Employee Termination Procedures**

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
	1. The user has been using their access rights inappropriately;
	2. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
	3. An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
3. The Security Officer will terminate users' access rights immediately upon notification, and will coordinate with the appropriate <COMPANY NAME> employees to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

**7.11 Paper Records**

<COMPANY NAME> does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against <COMPANY NAME> policies.

**7.12 Password Management**

1. User IDs and passwords are used to control access to <COMPANY NAME> 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 <COMPANY NAME> environment, password configurations are set to require:
	1. a minimum length of 12 characters;
	2. a mix of upper case characters, lower case characters, and numbers or special characters;
	3. a 90-day password expiration, or 60-day password expiration for administrative accounts;
	4. prevention of password reuse using a history of the last 6 passwords;
	5. where supported, modifying at least 4 characters when changing passwords;
	6. account lockout after 5 invalid attempts.
4. All system and application passwords must be stored and transmitted securely.
	1. Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent).
	2. Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in 17.8-production-data-security.
	3. Transmitted passwords must be encrypted in flight pursuant to the requirements in [§17.9](#17.9-transmission-security).
5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database.
6. Passwords are inactivated immediately upon an employee's termination (refer to 7.10-employee-termination-procedures).
7. All default system, application, and partner 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 Officer.
12. In cases where a user has forgotten their password, the following procedure is used to reset the password.
	1. The user submits a password reset request to password-reset@<COMPANY NAME>.com. The request should include the system to which the user has lost access and needs the password reset.
	2. An administrator with password reset privileges is notified and connects directly with the user requesting the password reset.
	3. The administrator verifies the identity of the user either in-person or through a separate communication channel such as phone or Slack.
	4. Once verified, the administrator resets the password.

The password-reset email inbox is used to track and store password reset requests. The Security Officer is the owner of this group and modifies membership as needed.

**Access to ePHI**

1. Employees may not download ePHI to any workstations used to connect to production systems.
2. Disallowing transfer of ePHI to workstations is enforced through technical measures.
	1. All production access to systems is performed through a bastion/jump host accessed through a VPN. Direct access to production systems is disallowed by <COMPANY NAME>'s VPN configuration.
	2. On production Linux bastions, all file transfer services are disabled including file-transfer functionality of SSH services (SCP/SFTP).
	3. On production Windows bastions, local drive mappings are disabled by Group Policy settings.
	4. Configuration settings for enforcing these technical controls are managed by <COMPANY NAME>'s configuration management tooling, TOOL NAME.

**7.14 Customer Access to Systems**

<COMPANY NAME> grants customers secure system access via VPN connections. This access is only to Customer-specific systems, no other systems in the environment. These connections are setup at customer deployment. These connections are secured and encrypted and the only method for customers to connect to <COMPANY NAME> hosted systems.

In the case of data migration, <COMPANY NAME> does, on a case by case basis, support customers in importing data. In these cases <COMPANY NAME> requires that all data is secured and encrypted in transit, such as by using SFTP or SCP for transferring files.

In the case of an investigation, <COMPANY NAME> will assist customers, at <COMPANY NAME>'s discretion, and law enforcement in forensics.

**Purpose**

The purpose of this procedure is to provide a policy and guideline for creating, modifying, or removing access to the company’s network and data by creating, changing or deleting the network account configuration for a User.

**Scope**

This policy and defined process is used to allow access to the company’s data and systems to individuals who meet the requirements defined in this policy. This policy governs individuals who are granted access that is necessary to support the business. This policy relates to all data used, processed, stored, maintained or transmitted in and through the company’s systems.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 01.d - User Password Management
* 01.f - Password Use
* 01.r - Password Management System
* 01.a - Access Control Policy
* 01.b - User Registration
* 01.h - Clear Desk and Clear Screen Policy
* 01.j - User Authentication for External Connections
* 01.q - User Identification and Authentication
* 01.v - Information Access Restriction
* 02.i - Removal of Access Rights
* 06.e - Prevention of Misuse of Information Assets

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(4)(ii)(C) Access Establishment and Modification
* 164.308(a)(3)(ii)(B) Workforce Clearance Procedures
* 164.308(a)(4)(ii)(B) Access Authorization
* 164.312(d) Person or Entity Authentication
* 164.312(a)(2)(i) Unique User Identification
* 164.308(a)(5)(ii)(D) Password Management
* 164.312(a)(2)(iii) Automatic Logoff
* 164.310(b) Workstation Use
* 164.310(c) Workstation Security
* 164.308(a)(3)(ii)(C) Termination Procedures

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |