[Insert Company Name and Logo]	
Title: Technical Safeguards – Access Control	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: The purpose of this policy is to ensure that all members of the workforce have access to the systems and information appropriate to their job functions, and to ensure that inappropriate access is prevented under cybersecurity best practices, herein referred to as "sensitive and regulated data." This Policy pertains to the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to all sensitive and regulated data.

Scope: This policy applies to all employees and other members of the workforce (whether paid or volunteer) with access to our organization's information systems, applications and/or network.

Procedure:

1) Unique User Identification and Password:
    a. Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores sensitive and regulated data, must be provided with a unique username.
    b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores sensitive and regulated data, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.
    c. Each user's password should meet the minimum requirements as outlined below:
        i. Must be a minimum of eight characters in length.
        ii. Must contain a unique character.
        iii. Must contain a number.
        iv. May not contain your user-name or any part of your full name
        v. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
        vi. If a system does not support the minimum structure and complexity as detailed in the previous guidelines, one of the following procedures must be implemented:
            1. The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.

2. The legacy system must be upgraded to support the requirements as soon as administratively possible.
3. All sensitive and regulated data must be removed and relocated to a system that supports the foregoing security password structure.

vii. Users must not allow another user to use their unique username or password.

d. Users must ensure that their username and password is not documented, written, or otherwise exposed in an insecure manner.
e. Each user must ensure that their assigned username is appropriately protected and only used for legitimate access to networks, systems, or applications.
f. If a user believes their username or password has been comprised, they must report that security incident to their manager, who will contact the organization's Security Officer.

2) Emergency Access (This section may depend upon the Company. These are examples to work with.)

a. The HIPAA Security Rule requires organizations to establish procedures to allow access to sensitive and regulated data during an emergency. During an emergency or disaster, covered entities must remember that protecting sensitive and regulated data is of utmost importance. Emergency procedures may be very different from standard operating procedures, but they are necessary because the normal methods for obtaining access may fail. Emergencies include, but are not limited to, the following:
   i. Natural disasters – Floods, earthquakes, tornadoes, tsunamis, hurricanes, etc.
   ii. Man-made disasters – Hacking attacks, thefts, vandalism, terrorist attacks, etc.
   iii. Unforeseen disasters – Power outages, internal failures, etc.
b. When developing this policy and procedure, a covered entity should:
   i. Determine the type of situation that may require emergency access to sensitive and regulated data.
   ii. Determine who will need access to sensitive and regulated data in case of an emergency
c. In the case of emergency, a computer account may be temporarily shared with another individual. The requirements for emergency access sharing are:
   i. There must be a true emergency.
   ii. The sharing must be temporary.
   iii. The emergency incident must be reported to the managing authority of the computer account being shared.
   iv. In no case should this emergency access sharing exceed 30 days.
   v. The Emergency access procedure must be used in case a terminated employee's computer account must be maintained for business reasons.

Unless the Emergency Access procedure is implemented, all terminated employee computer accounts will be deleted immediately upon notification of the termination to all relevant parties.

d. Servers with sensitive and regulated data are maintained off-site in order to reduce potential damage during a disaster at the facility.
e. The organization has established an off-site disaster recovery location, [Insert Specified Location]. Provisioning and maintenance of this location have been arranged through external contractors. In the event of its activation, it will be staffed by a combination of the Covered Entity and these contractors. The data and applications on the systems resident at the location are either actively synchronized with the corresponding systems in the Covered Entity or will be brought up-to-date from data backups when the site is activated. The system is tested and exercised on a [Insert Time Frame].
f. Critical personnel have been issued emergency response cards for access to the facilities in the event of an emergency or disaster.
g. In the event of power outage, a backup generator will be utilized.
    i. In the event the backup generator doesn't work, remote access will be utilized by the designated personnel. Information will be printed or transmitted via phone (cell, sat) for critical business continuity.
h. If facility is under a pre-evacuation, print only necessary documents to maintain critical business continuity.

3) Automatic Logoff
    a. Servers, workstations, or other computer systems located in open, common, or otherwise unsecure areas, that access, transmit, receive, or store sensitive and regulated data, or that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms. These systems must terminate a user session after a maximum of 15 minutes of inactivity.
    b. Applications and databases using sensitive and regulated data, such as electronic claims records, must employ inactivity timers or automatic session logoff mechanisms. These application sessions must automatically terminate after a maximum of 30 minutes of inactivity.
    c. Servers, workstations, or other computer systems that access, transmit, receive, or store sensitive and regulated data, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
    d. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
        i. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.
        ii. The system must be moved into a secure environment.
        iii. All sensitive and regulated data must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.

e. When leaving a server, workstation, or other computer system unattended, users must lock or activate the system's automatic logoff mechanism (e.g. CTRL+ALT+DELETE and Lock Computer) or logout of all applications and database systems containing sensitive and regulated data.

4) Encryption and Decryption
   a. Encryption of sensitive and regulated data as an access control mechanism is not required unless the custodian of said sensitive and regulated data deems the data to be highly critical or sensitive. Encryption of sensitive and regulated data is required in some instances as a transmission control and integrity mechanism.
5) Firewall Use
   a. All networks housing sensitive and regulated data repositories must be appropriately secured. To ensure that all networks that contain sensitive and regulated data-based systems and applications are appropriately secured, each connection to outside the network must follow the steps outlined below. Networks containing sensitive and regulated data-based systems and applications must implement perimeter security and access control with a firewall.
   b. Firewalls must be configured to support the following minimum requirements:
      i. Limit network access to only authorized users and entities.
      ii. Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
      iii. Console and other management ports must be appropriately secured or disabled.
      iv. Implement mechanism to log failed access attempts.
      v. Must be located in a physically secure environment.
   c. [Insert Company Name] must document its configuration of firewalls used to protect networks containing sensitive and regulated data-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.
   d. The configuration of firewalls used to protect networks containing sensitive and regulated data-based systems and applications must be submitted to and approved by the Information Security Officer.
6) Remote Access
   a. Dial-up connections (if allowed), directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.
   b. Authentication and encryption mechanisms are required for all remote access sessions to networks containing sensitive and regulated data via an ISP (Internet Service Provider) or dial-up connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.

c. The following security measures must be implemented for any remote access connection into a secure network containing sensitive and regulated data:
    i. Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications, such as GoToMyPC.com, are not permitted.
    ii. Remote access workstations must employ a virus detection and protection mechanism.
d. Users of remote workstations must use multi-factor authentication and comply with cybersecurity best practices outlined here.
e. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 256-bit encryption.
f. Any user requesting remote access to a secure network containing sensitive and regulated data-based systems and applications must be approved by the Security Officer. The owner of the secure network (IS or managing department) must ensure that the previous requirement has been satisfied before access is granted.
g. [Insert Company Name] must establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their users to remotely access secure networks containing sensitive and regulated data-based systems and applications continue to meet strict security measures

7) Wireless Access
    a. To ensure that all networks that contain sensitive and regulated data-based systems and applications are appropriately secured, [Insert Company Name] must follow the wireless access policies and procedures outlined below.
    b. Wireless access to networks containing sensitive and regulated data-based systems and applications is permitted so long as the following security measures have been implemented:
        i. Encryption must be enabled.
        ii. MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
        iii. All console and other management interfaces have been appropriately secured or disabled.
        iv. Unmanaged, ad-hoc, or rogue wireless access points ARE NOT PERMITTED on any secure network containing sensitive and regulated data-based systems and applications.
        v. All wireless LANs do not utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit sensitive and regulated data may not allow encryption of that data stream. It has been determined that this is

low risk because this implementation of infrared is very short distance and low power.

vi. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 256-bit encryption.

c. Any user requesting access to a secure wireless network containing sensitive and regulated data-based systems and applications must ensure that the wireless device being used by said user meets the security measures detailed, for example, in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security. The owner (managing entity) of the secure wireless network must ensure that the previous requirement has been satisfied before access is granted.

d. [Insert Company Name] must establish a formal, documented procedure to ensure that wireless devices used by their users to access secure networks containing SENSITIVE AND REGULATED DATA-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security.

Violations: Any individual found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Attachments: None

Related Policies: None