

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

I. PURPOSE

To prevent unauthorized access to any system resource, including the computer system, network, software applications, and data files.

To protect system resources against unauthorized use, disclosure, modification, and destruction.

To preserve the confidentiality of protected health information (PHI).

To define the <Company Name> standard for access requirements including applications supported by Information Systems throughout the organization and at the department level including the responsibility of individual department computer system administrators, data owners, and data custodians.

II. DEFINITIONS

Access – the ability to view or modify protected information in system resources, including a computer.

Access Controls – identifies and authenticates a user to allow access to confidential and private health information based on a business need to know. Access controls protect the computer systems and resources from unauthorized access as well as determine the type of access a user is entitled to have.

Authentication – identifies the user. The use of a userid and password provides authentication. It tells the computer that they are who they say they are. Confidential information is defined as information not freely disclosed and information protected by law or <Company Name> policy.

Data Custodians – the data custodian is usually a *department* which holds accountability in maintaining data integrity, assisting in the design of the security system to meet the needs of the data owner.

Data Integrity – refers that the data sent is the exact same data received and has not been modified in any way.

Data Owners – the data owner is the *individual* with primary accountability for the collection and accuracy of the data, determining who is allowed to access the data, the availability of data, and the ultimate outcome of the data.

Directory - A network service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers.

Network - A group of two or more computer systems linked together in a geographical area such as a Local area Network (LAN), or are linked together by telephone wire or radio waves such as a Wide Area Networks (WAN).

Protected Health Information (PHI) – is defined as information that's individually identifiable and created or received by a health care organization. This includes both clinical or payment information, which can reasonably be associated with a patient.

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

Root Access – allows authorized individuals unrestricted access to a system for administration and maintenance purposes.

Server - A computer or device on a network that manages network resources

User – a person or resource that is accessing a computer system.

User Id – A unique set of characters or a special code that is used to identify a specific user to a computer system.

III. POLICY

A. Types of Access Control

Access to any <Company Name> computer system or resource will be granted if it is expressly requested by the Operations Director or Designee of the department. See <Company Name> policy Requesting Computer Access for further information.

1. Identification and Authentication

Access requires a user identification, which answers the question, Who am I? The second step for access is authentication. Three elements exist for authentication, something you know, something you have, and something you are. Various types of access controls are now in use at <Company Name> and include one of the following.

a. Passwords

Identification = User ID (Who am I?)

Authentication = Password (Something you know)

This is the most common form of access control. Please see Section III(C) below for more detailed information.

a. Biometrics

Identification = User ID (Who am I?)

Authentication = Biometrics characteristic (Something you are)

i. Biometrics identification uses one or more unique human characteristics, fingerprint, retina of the eye, and the iris of the eye. One of these characteristics must be applied when using biometrics identification.

ii. There are very few departments at <Company Name> using biometrics. The use of biometrics does not negate the responsibilities of users and system administrators to enforce security policies and procedures on system not protected by this method.

2. Deviations from this practice require the <Company Name> Privacy Officer and Information Security Administrator approval.

B. Roles and Responsibilities

1. Data Owner

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

- a. Determines who has a business need to access information for which the data owner has accountability.
 - b. Assists in enforcing security rules.
 - c. Has primary accountability in auditing data integrity.
 - d. Assures that department level policy and procedures are developed and maintained to ensure compliance with the system wide security policies.
2. Data Custodians
- a. Information Systems is the primary on-site Data Custodian for <Company Name>.
 - b. For hosted applications outside the <Company Name> network, <Company Name> will obtain proper assurances that all equipment, software and/or services provided by the vendor will operate and be consistent with the requirements of any and all state and federal laws (including, but not limited to), rules establishing standards for security and electronic transactions.
 - c. The Data Custodians are accountable for developing procedures, standards, or policies for processing <Company Name> information maintaining security and the integrity of the information.
3. System Administrators
- a. The data owner or designee of department specific applications will assign a system administrator to oversee the security of the application within that department in addition to other departmental responsibilities.
 - b. Responsibilities of System Administrators include the following:
 - i. Adding, disabling, deleting, or modifying user access as indicated by changes in job responsibilities.
 - ii. Educating department staff on security policies and practices.
 - iii. Working directly with the <Company Name> Information Security Administrator to enhance security practices throughout the organization.
4. User
- a. Each user will protect their assigned password and will not share or post their password for others to see or use.
 - i. Sharing or posting of passwords is considered a breach of confidential information and grounds for disciplinary action.
 - ii. The disciplinary action taken will depend upon the severity of the breach. At a minimum, sharing or posting of passwords will be a Level I breach. Refer to Policy # 900.032, Breach of Confidential Information.
 - b. Role Based Access Controls (RBAC)
Identification = User ID (Who am I?)
Authentication = Password (Something you know)
- System Administrators are accountable to work directly with the data owner or designees to implement RBAC groups appropriate for the department workflow and computer access needs
- i. Limits access to protected information to those users who have a business need for access. See the policy *Workforce Limitations with Respect to Using, Requesting, or Disclosing Patient Information*.

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

- i. Grants access based on the individual user roles, i.e. Physician, RNs, Lab Tech, etc.
 - ii. Users are placed into role groups. The groups are then given pre-defined access to information based on their business need to know.
5. Information Security Administrator
 - a. Holds primary responsibility for developing policies and procedures to protect PHI and confidential information, including access control.
 - b. Responds to security incidents and works directly with Privacy Officer, and leadership to eliminate or reduce associated risks.
 - c. Acts as a resource and works directly with departmental System Administrators to develop and enforce security practices.
6. Vendor Access
 - a. Vendors will not be allowed to access the <Company Name> network without a properly formatted userid and password.
 - b. Vendor userid(s) will be activated when needed and will be promptly disabled when not in use.
 - c. Vendor on-site access to applications or information containing PHI will be supervised at all times.
7. Remote Access

Individuals with remote access will retain accountability and responsibility for protecting the confidentiality of <Company Name>'s protected health information (PHI) and/or confidential information.

Current technology makes remote access "at risk access" with respect to security issues. Therefore, the user assumes full responsibility for the physical security of all computing devices and all PHI and/or confidential information printed, maintained, or stored on a remote computing device.

- a. Printed information will be protected from unauthorized disclosure at all times and shredded to be made unreadable before disposal.
- b. Documents unable to be shredded by a remote user will be returned to the individuals department for destruction.

C. Password Security

Information on a computer is only as secure as the weakest link. Poorly chosen password many times serve as the weak link that could allow an unauthorized individual access to computer information and resources. The following rules apply to all users when determining a password.

1. Do Use:

- Uppercase and lowercase combined.
- A minimum of 8 characters. If the application does not allow 8 characters, use the maximum length allowed by the application.
- Combination of letters, numbers, and symbols.
- A minimum of 3 letters (a through z) and 2 numbers (1 through 9).

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

- Do not use these or other example passwords found in literature. They have been published and considered to be poor choices
2. **Do Not Use:**
- Passwords less than 8 characters long.
 - Your userid in any form i.e., as-is, reversed, capitalized, doubled, etc.
 - Your first, middle, last, or nick name in any form i.e., as-is, reversed, capitalized, doubled, etc.
 - Names of your spouse, parent, child, pet, boss, co-worker, or friend or your favorite sport team i.e. GoHuskers.
 - Personal information easily obtained about you – license plate number, hobbies, telephone number, social security number, type of car, or your address or street you live on.
 - All numbers.
 - All the same letter.
 - Any word found in a foreign or English dictionary.
 - Dates, especially birthdays or anniversaries.
 - Letter sequences directly off the keyboard like QWERTY, MNBVCXZ.
 - Names of words with a single number in front or behind it.
 - Popular vacationing sites, like LakeTahoe, LasVegas, etc.
 - The name of the operating system the computer uses.
 - The hostname of the computer.
 - Proper nouns.
- 3 Password Management
- When applications have the capability, the following restrictions must be applied to individual passwords.
- a. Passwords will be set to expire every 6 months or less.
 - b. Individual users may reset their passwords at anytime.
 - c. Initial passwords assigned by the System Administrator will be set to expire with the very first log in by the user. The individual user must meet all of the above expectations when determining their private password.
 - d. If an application is limited in the ability to apply the above restrictions, the application security will be set to the highest possible restriction level available.
- 4 Password must never be shared.
- 5 Do not post a userid and password where it could be found by someone and used to access the computer.
- 6 All individuals are held accountable for all activity occurring with the use of their individual userid. Treat passwords as you would your PIN number for the bank.
- 7 Do not store passwords in software programs that will automatically log into another application or software program.
- D. Automatic Logoff Functions.
- 1. Automatic logoff functions will log a user out of an application or program after a pre-determined amount of time.

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

2. If Department specific applications have this function, it will be set to match the current defined auto logoff time set on the network. Contact the Information Security Administrator or the Help Desk to determine the defined time period.

E. Technical Considerations

1. Implementing Access Controls

Computer access to confidential information, PHI, and computer resources must be provided at four levels of access control. All four levels work together to provide security to <Company Name> computer equipment and resources. The four levels of access control are: Network, Server, Directory, and User.

- a. Network – Access to the network hardware is controlled by both the ENA and Network teams. This includes physical access as well as being password protected.
 - b. Server – Access to the Server software is controlled by the Network team with Network Administrator rights.
 - c. Directory – Directory security is controlled at the network level through an IS Network Analyst with network administrator rights.
 - d. Users - Users are required to have and use an individual user id and a secret password to access confidential information or PHI. See section III(C).
2. Default passwords shipped with servers, operating system software, or applications will be changed upon implementation.
 3. Root access will be granted to the smallest number of individuals required to support the system. Root passwords will be changed immediately upon arrival of the system and whenever necessary to protect system integrity.
 4. Passwords will not be transmitted over the network in clear text.
 5. Servers and network hardware will be locked in a physically secure room with access limited to authorized personnel only.
 6. Servers will be accessed only by the Network Administrators or Enterprise Network Analysts for the purposes of server administration.
 7. Cable connections will be in a secure location to avoid tampering and physical damage to equipment.
 8. Non-employee technical maintenance personnel will be supervised when providing maintenance to equipment containing PHI. The home department of the equipment being serviced is responsible for providing supervision of maintenance personnel.
- G. Violation of this policy could result in criminal prosecution as determined by local, state, or federal law. Members of the workforce in violation of this policy will be subject to disciplinary action up to and including termination of employment.

IV. REFERENCES

- A. Information Security, Policy # 903.004.

Computer Access Controls_Stripped_Alegent

<Company Name>

Computer Access Controls

DRAFT

SUBJECT: Computer Access Controls

DRAFT

- B. Information Technology Code of Practice For Information Security Management, ISO/IEC 17799, First Edition, December 2000.
- C. Breach of PHI and/or Confidential Information, Policy # 903.002.
- D. Requesting and Terminating Computer Access, Policy #903.003