TRIHEALTH, INC.
CORPORATE POLICY

TITLE: Password Policy	
SECTION: 05	**POLICY NUMBER: IS06.00**
EFFECTIVE DATE: 03/2001	**REVIEWED/REVISED DATE(S):** **03/ 2002, 01/2004, 09/2007, 07/2011, 10/2013, 04/2017, 03/2018**
AFFECTED AREAS All TriHealth Entities including McCullough-Hyde Memorial Hospital This policy acknowledges that other relevant and applicable policies and procedures exist that have been drafted, approved, and adopted by entities (and departments) within TriHealth and are specific to those departments or entities. Interpretation of these other policies must comply with the principles adopted by Corporate Policy #12_01.00, "Corporate Policies, Development & Implementation".	
POLICY OWNER: Information Systems Security Manager	
APPROVED BY: **Sr. Vice President and Chief Information Officer** **Legal Services** **Corporate Policy & Procedure Committee** **President of Health Services and System COO** **President & CEO**	

PURPOSE

The purpose of this policy is to maintain confidentiality, availability and integrity of information that is consistent with the ethical standards and practices of TriHealth, Inc. In order to maintain the confidentiality and security of all computer passwords pertaining to TriHealth, Inc., requirements are provided to the employees; agency personnel; or other agents of TriHealth, Inc., who have access to TriHealth computer systems (specifically, all computers, mobile devices and its substitutes, computer networks, computer applications, telephone systems, and software developed by or licensed to TriHealth, Inc. (together, the "Infrastructure"). See Appendix A for a "quick list" of items covered in this policy.

BACKGROUND

- ☐ TJC Std: IM.02.01.01; IM.02.01.03
- ☐ Licensure
- ☐ Regulatory Agencies HIPAA C.F.R. 164.308
- ☐ Other

POLICY/PROCEDURE

The password security procedure must be initiated by the System or Access Administrators, which will allow employees or other agents of TriHealth, Inc., to access information as designated by their manager or sponsoring body. The sponsoring TriHealth employee must be responsible for ensuring all agents and employees under their supervision are provided with all TriHealth policies. Without an affirmative grant of authority, a TriHealth employee or other agents will not be considered to have access to any part of the TriHealth Infrastructure.

Passwords are established at the disk encryption, system and application levels. Disk encryption and/or system passwords enable access to the TriHealth network.
Once within the TriHealth network one can attempt to access certain applications; therefore application passwords provide a second level of authentication. Some network or application access will require the use of an additional PIN, biometrics, proximity card, challenge response questions and/or token to gain access.

Any system, agent or situation that cannot meet these policy requirements must be communicated to and signed off in writing by the Information Systems Security Manager.

Access authorization information for a particular user must be retained for so long as such user has access to the Infrastructure, and upon loss of such access, all information will be retained by TriHealth for a minimum of 7 years.

To prevent unauthorized access the number of consecutive attempts to enter a correct password is limited. After five (5) unsuccessful attempts to enter a password, the access code will be suspended until the Customer Support Help Desk or the appropriate System or Access Administrator resets the password. This will be implemented on all systems where technically possible.

At least annually, System or Access administrators must audit access rights against authorizations for such rights. Also, on an annual basis access administrators must audit access for inactive and terminated accounts. Any accounts that are found to be inactive for 180 days will be disabled either manually or automatically.

Passwords, PINs, biometrics, proximity cards and tokens should be treated as confidential information. No employee is to disclose or share in any way his or her password, PIN, biometrics, proximity cards or token to another person (including IT staff, administrators, clinicians, physicians and superiors) under any circumstances.

Passwords may be known only to the user or in exceptional cases the user and a TriHealth-Information Security Engineer as defined in the TriHealth Corporate Incident Response Policy. Use of software application (approved by TriHealth Information Security) that itself permits and tracks delegation of certain functions (e.g. an Administrator's ability to access a server) is not considered sharing a password for the purpose of the Password Policy. An example of such approved software is Cyber-Ark.

"One Time Use" passwords may be emailed to an employee's existing TriHealth email account, or to an agent's business account using secure email. Passwords may not be emailed to group accounts. These mailings shall have no markings indicating the nature of enclosure. A user id and password may never occupy the same message at any time. Only one time use passwords may be emailed, these passwords require the user to change the password at first logon.

The preferred method of providing user id's and one time passwords involves the System or access administrators to email the user id to the manager or user, and call the manager or user directly to provide the one time password.
User id's and password may be provided together in writing in the initial remote access packet which is picked up in Security by the user or hand delivered to the user by a designee and opened only by the user. This packet also contains a "token" or "key fob" which makes every password unique thereafter.

The display of passwords shall be masked, suppressed, or otherwise obscure so unauthorized parties will not be able to observe or recover them.

Where technically possible passwords must be entered on any TriHealth authorized device in a non-display mode.

No employee may leave a password written down in an obvious place, give an unauthorized user their password, or attempt to hack someone else's computer with the intention of obtaining access to their password, files or with a purpose of access elevation.

All vendor-supplied passwords must be changed before any computer system is used for TriHealth business.

Initially assigned passwords will be changed at or upon first usage.

Do not use the "Remember me on this computer" feature on where an application retains your password to automatically log you on in the future. Use secret password hints and reminders when available, but never type your whole password in these hints and reminders. See Access to TriHealth Information Technology Resources (#05_IS04.00) for policies pertaining accessing TriHealth Information Technology Resources. Applications support, Developers, Information Systems personnel or any System Owners are prohibited from building or deploying secret user IDs or passwords which have special privileges which are not clearly covered in system documentation.

All Network devices (routers, firewalls, access control servers, etc.) shall have unique user ids and passwords or other equivalent access control mechanisms where technically possible. A compromise in the security of one device shall therefore not automatically lead to a compromise in other devices.

TriHealth system application support, developers, information systems personnel, administrators and owners must consistently rely on the password access controls provided by an operating

system or an access control package that enhances the operating system. Separate mechanisms may not be constructed to identify or authenticate the identity of users without the advance permission of Information Systems Security.

Computer and communication systems shall be designed, tested, and controlled so as to prevent both the retrieval of and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

Passwords may not be "hardcoded" into any system unless advance permission and review has been granted by the Information Systems Security Manager.

Passwords and challenge response answers must always be encrypted where technically possible when held in storage or when transmitted over networks. This shall prevent them from being disclosed to wire tappers, technical personnel who are reading system logs, and / or other unauthorized parties.

Passwords or challenge response answers must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them, unless authorized by Information Systems Security.

Password Requirements:

Any system, agent or situation that cannot meet these policy requirements must be communicated to and signed off in writing by Information Systems Security.
System and application level passwords will be updated at least 180-days where technically possible. Services Accounts not managed by CyberArk will be updated annually where feasible. If the user has access to credit card information or have privileged access, then passwords will be updated every 90 days. Minimum password age for all passwords is 1 day. All passwords, where technically feasible, will be:

- set by the user and will be system forced to a minimum length of eight (8) characters (eight or more characters are preferred),
- Consisting of 3 of the following 5 options:
    1. upper-case alphabet (A-Z),
    2. lower-case alphabet (a-z)
    3. and numeric (0-9). Active Directory passwords must consist of at least a letter and a number.
    4. Special character such as !, @, #, $, etc.
    5. Unicode (not typically used)

.

Systems or situations where an exception is required must be assessed by Information Systems Security and have management approval.

Password parameters will be set to require that a user's account is locked out after 5 (five) invalid logon attempts where technically possible. Password parameters will be set to require that new passwords cannot be the same as the ten (10) previously used where technically possible. All users of TriHealth Infrastructure are responsible for the safekeeping of passwords which can be used to gain access to any TriHealth application. All users of TriHealth Infrastructure must log-off or secure their terminal when leaving it.

When technically possible, internal systems or applications should use Active Directory for authentication.

Passwords cannot be the person's first or last name or any other recognizable organization or department name or any variations thereof. Passwords should not be based on a user's personal information including but not limited to a spouse's name, automobile license plate, children's names, social security number, pets names, birthdays or any part of normal speech. Passwords must not be written or stored in a location in which personnel other than the password owner have access. Special Characters are encouraged but not required.

All user-chosen passwords for computers and networks should be difficult to guess. Use misspelled words and substitute special characters for letters (5 or $ = S, 1 = I or L, 3 = E, 0 = O)

Examples of good passwords:

- Too late again = 2L8aga1n
- Music is for me = MusikS4m3
- Day after today = dayFter2day
- 15djoth! (15 dogs jumped over the house)
- Seashore = Se@shor
- Deadbolt = Ded&bowlt8
- Easy money = Ea$ymon3y!
- blaK4b0rD! = Blackboard

<u>Compromised Password, PIN, or Token:</u>

Upon notification of any compromised password, PIN, or token, the System or Access Administrator will immediately authorize a new password and contact Information Systems Security. Information Systems Security will make an assessment as to the security risk involved and determine the next steps.

All suspect passwords must be promptly changed if they are found to have been disclosed, or suspected to have been disclosed, to unauthorized parties.

Whenever a system is known to have been compromised by an unauthorized party, or a system administrator with privileged access to a particular system leaves the company, system managers must immediately change every password on the involved system(s).

All mobile devices accessing TriHealth email will be subject to TriHealth enforced security which includes the device to be password protected by a minimum of a 4 digit PIN, as well as a

maximum of 8 password attempts before the device is locked and wiped clean. These users must notify the help desk immediately if the phone is lost or stolen. A remote "wipe" of the device will be performed where technically possible.

Individuals who share a password, PIN, biometrics, proximity card or token will be subject to appropriate disciplinary action.

Removable Media:

Removable media (thumb drive, CD, flash drive, USB drive, etc.) must be used in compliance with the Portable Device and Removable Media Policies. If approved, the device must be encrypted and assigned a "public" key. This key may not be written down. If this key is forgotten, the drive is rendered useless. Removable media that is no longer needed or accessible must be returned to Client Technologies for proper destruction. Questions regarding this topic can be directed to Information Systems Security.

Emergency Passwords:

Passwords, PINs, biometrics and proximity cards may be issued in an emergency situation as authorized by a Department Director, Manager, or Supervisor upon a prior approval from Information Systems Security. Emergency access will be valid for no longer than 72 hours at which time access will be disabled until appropriate access forms are received.

Procedure:

New Employee:

Once registered for training Network logon access to the computer, Epic access, Cloudmail or Exchange email, as well as the Home directory (H drive) are granted automatically for the new employee. The Department Director, Manager, or Supervisor will submit the Electronic Login Form found on LinkNet as soon as the new employee start date is determined for any additional access needed. This will allow the new employee to have access established upon arrival the first day. The System or Access Administrators will assign the initial password and email this password to the employee's manager. Trainers will also have access to the one time code in order to validate access before leaving training to go to their job.

The user may be requested to pick up a keyfob / token from Corporate Security if such access is requested. Proper identification is always required in order to receive the password. Proper identification for employees is an employee badge or some other identifiable information. Proper identification for TriHealth, Inc., agents is a picture ID. When calling the Customer Support Help Desk proper identification is the last 4 digits of the employee's social security number. Only the employee themselves can call the help desk in order to verify identity.

Corporate Education will cover confidentiality and security policies and procedures in new employee orientation. Confidentiality and password acknowledgements will be signed by all new

employees or other agents of TriHealth, Inc., and will be retained by Human Resources in the compliance records.

Agents of TriHealth, Inc.

All agents not employed by TriHealth, Inc., who require access, must have a sponsoring body. A sponsoring body is a TriHealth staff (Director or above) who has authorized access and determined the level of access required by the agent to facilitate the duties assigned.

All agents must sign the TriHealth Information Technology Resources Agent Acknowledgement form, before any agency employees will be considered for access or the sponsor will place an electronic login request form from LinkNet.

The agent shall schedule agency employee training with Corporate Education of TriHealth, or an authorized agency trainer approved by Corporate Education and Information Systems. Upon successful completion of required training, Corporate Education or other Authorized Agency Trainer will have the agency employee sign the TriHealth Information Technology Agency Employee Access form. The individual will then receive the password from Corporate Education or Authorized Agency Trainer. If the password is received from Authorized Agency Trainer, the Information Technology Resources Agent Acknowledgment Form will be obtained.

When the agent and the agency employee sever the relationship, it is the responsibility of the agent to notify the TriHealth, Inc., Information Owner and/or Access Administrator to remove access. When a change in level of access is warranted, it is the responsibility of the agent to notify TriHealth Inc., Information Systems who will change the access level.

Current Employee:

The manager will schedule related application training as required through Corporate Education or a TriHealth authorized trainer. The Manager, Supervisor, or Corporate Education will submit the Electronic Login Form on LinkNet requesting the change in access. The System or Access Administrator(s) will update the applicable systems to reflect the new levels of access. If the employee requires additional training, the new password will be obtained from Corporate Education or a TriHealth authorized trainer upon successful completion of training. Training on the use of passwords, PIN, biometrics, Challenge Response Questions, proximity cards or tokens will be provided on an "as needed" basis.

Forgotten Password or PIN:

Staff or agents of TriHealth, Inc., who have been assigned a password or PIN, may obtain a new password by using the self-service password reset function or PIN by contacting the Information Systems Customer Support Help Desk. Passwords may be given over the phone to employees with proper identification (Last 4 of social, employee ID). If user identity cannot be determined, users must go to the TriHealth Security Department who will verify the user's identification to receive a password over the phone.

Termination/Transfer of Employee:

Terminations and transfers of employees will be accomplished in accordance with the Access to TriHealth Technology Resources Policy. TriHealth reserves the right to terminate the information access of any individual or entity that violates this policy, breaches confidentiality restrictions or abuses privileges granted in TriHealth's Access to Information Technology Resources. Employees breaching this policy will be subject to the TriHealth Performance Counseling policy up to and including termination.

APPENDIX A

Quick List of Do's and Don'ts

1. Individuals who share a password, PIN, biometrics, proximity card or token will be subject to appropriate disciplinary action. Passwords, PINs, biometrics, proximity cards and tokens should be treated as confidential information. No employee is to disclose or share in any way his or her password, PIN, biometrics, proximity cards or token to another person (including IT staff, administrators, clinicians, physicians and superiors) under any circumstances.
2. Any system, agent or situation that cannot meet these policy requirements must be assessed by the Information Security and have management approval..
3. All agents not employed by TriHealth, Inc., who require access, must have a sponsoring body. A sponsoring body is a TriHealth staff (Director or above) who has authorized access and determined the level of access required by the agent to facilitate the duties assigned.
4. The sponsoring TriHealth employee must be responsible for ensuring all agents and employees under their supervision are provided with all TriHealth policies.
5. Password parameters will be set to require that a user's account is locked out after 5 (five) invalid logon attempts. Password parameters will be set to require that new passwords cannot be the same as the ten (10) previously used where technically possible.
6. No employee may leave a password written down in an obvious place, give an unauthorized user their password, or attempt to hack someone else's computer with the intention of obtaining access to their password, files or with a purpose of access elevation.
7. All vendor-supplied passwords must be changed before any computer system is used for TriHealth business.
8. Do not use the "Remember me on this computer" feature on where an application retains your password to automatically log you on in the future. Use secret password hints and reminders when available, but never type your whole password in these hints and reminders.
9. All TriHealth users must have unique user id's representing the user's identity.
10. Passwords cannot be the person's first or last name or any other recognizable organization or department name or any variations thereof. Passwords should not be based on a user's personal information including but not limited to a spouses name, automobile license plate, children's names, social security number, pets names, birthday's or any part of normal speech. Passwords must not be written or stored in a location in which personnel other than the password owner have access. Special Characters are encouraged but not required.
11. System and application level passwords will be updated at least 180-days where technically possible. All passwords, where technically feasible, will be:
    a. set by the user and will be system forced to a minimum length of eight (8) characters (eight or more characters are preferred),
    b. Consisting of a combination of letters and numbers: upper-case alphabet (A-Z), lower-case alphabet (a-z) and numeric (0-9). Active Directory passwords must consist of at least a letter and a number.

c. Special characters may be used but are not required.

12. All mobile devices accessing TriHealth email will be subject to TriHealth enforced security which includes the device to be password protected by a minimum of a 4 digit PIN, as well as a maximum of 8 password attempts before the device is locked and wiped clean. These users must notify the help desk immediately if the phone is lost or stolen. A remote "wipe" of the device will be performed.
13. Removable media (thumb drive, CD, flash drive, USB drive, etc.) must be used in compliance with the Portable Device and Removable Media Policies. If approved, the device must be encrypted and assigned a "public" key must be assigned. This key may not be written down. If this key is forgotten, the drive is rendered useless. Removable media that is no longer needed or accessible must be returned to Client Technologies for proper destruction. Questions regarding this topic can be directed to the Information Systems Security Manager.
14. All access requests for new employees: The Department Director, Manager, or Supervisor will submit the Electronic Login Form found on LinkNet as soon as the new employee start date is determined. This will allow the new employee to have access established upon arrival the first day.
15. All access requests for Agents of TriHealth: All agents must sign the TriHealth Information Technology Resources Agent Acknowledgement form, before any agency employees will be considered for access. All agents not employed by TriHealth, Inc., who require access, must have a sponsoring body. A sponsoring body is a TriHealth staff (Director or above) who has authorized access and determined the level of access required by the agent to facilitate the duties assigned
16. When technically possible, systems or applications should use Active Directory for authentication.
17. Systems may not be purchased or used for TriHealth business purposes holding confidential or patient information without an Application Security Review approval from Information Systems Security (purchased, subscription / hosted, or web application, etc.):
18. Systems or situations where an exception is required must be submitted in writing to the Information Security Manager and a response must be provided to requestor.

TRIHEALTH, INC.

INFORMATION TECHNOLOGY RESOURCES

AGENT ACKNOWLEDGEMENT

We, in doing business with TriHealth understand that TriHealth, Inc., computer, e-mail, Internet and voice mail systems (the Infrastructure) is to be used by our employees for the purpose of conducting authorized TriHealth, Inc., business only. We are aware that TriHealth, Inc., reserves and intends to exercise the right to review, audit, intercept, access, and disclose all matters on TriHealth, Inc., information technology at any time, with or without user notification and that such access may occur during or after working hours.

We understand that use of these resources for unauthorized and private purposes is strictly prohibited. We agree that our employees will not access any information other than where authorized. We are aware that use of a TriHealth, Inc., provided password does not imply any right of privacy expectation and does not restrict TriHealth, Inc., right to access information technology resources.

We acknowledge that we have read, understand, and agree to comply with the following policies governing the use of TriHealth, Inc., Information Technology resources and services.

Password Policy
Access to TriHealth Information Technology Resources
Protection from Malicious Software
E-Mail
Portable Devices and Removable Media
Internet / Intranet Acceptable Use
HIPAA Portable Devices Storing Protected Health Information

We understand that our employees must complete any required training prior to accessing any TriHealth, Inc., owned or operated resources.

We agree to promptly notify TriHealth, Inc., Information Systems Security of any terminations/transfers of our employees that have been granted access to any TriHealth, Inc., computer systems and/or networks.

We understand that a violation of this policy may result in an employee having access permanently revoked and/or legal action.

Human Resources Representative: _____

Printed Name: _____

Company: _____

Date Signed: _____

TRIHEALTH, INC.

INFORMATION TECHNOLOGY RESOURCES

CONTRACT / AGENCY USER ACCESS

As an employee of _____, I, _____, in doing business with TriHealth Inc., understand that TriHealth, Inc., computer, e-mail, Internet and voice mail systems (the infrastructure) are to be used for business purposes only. I am aware that TriHealth, Inc., reserves and intends to exercise the right to review, audit, intercept, access and disclose all matters on TriHealth, Inc., Information Technology at any time, with or without user notification and that such access may occur during or after working hours.

I agree not to access any information other than where authorized. I agree not to give anyone else access to my password. I am aware that use of a TriHealth, Inc., provided password does not imply any right of privacy expectation and does not restrict TriHealth, Inc., right to access electronic communications.

I acknowledge that I have read and understand the following TriHealth Inc., policies:

Password Policy
Access to TriHealth Information Technology Resources
Protection from Malicious Software
E-Mail
Portable Devices and Removable Media
Internet / Intranet Acceptable Use

HIPAA Portable Devices Storing Protected Health Information

I agree to comply with the above policies governing the use of TriHealth, Inc., Information Technology resources and services. I understand that I must complete training prior to accessing any TriHealth, Inc., owned or operated resources.

I understand that a violation of this policy may result in having access permanently revoked, removal from doing business with TriHealth, Inc., and/or legal action.

_____ _____
Signature Date Signed

_____ _____
Company Trainer

_____
Printed Name