TRIHEALTH, INC.
CORPORATE POLICY

TITLE: Access to TriHealth Information Technology Resources	
SECTION: 05	**POLICY NUMBER: IS04.00**
EFFECTIVE DATE: 03/2001	**REVIEWED/REVISED DATE(S): 02/2001, 02/2002, 01/2004, 09/2007, 02/2011, 11/2014, 05/2017, 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 & Chief Information Officer** **Executive Vice President System Development** **TriHealth Corporate Policy & Procedure Committee** **President of Health Services & 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. This policy will define procedures on granting, changing, and removing access to TriHealth information technology resources pertaining to all employees, agency personnel; or other agents of TriHealth, Inc., who have access to TriHealth computer systems. This applies specifically to all computers, computer networks, e-mail systems, telephone systems, voicemail systems and software developed by or licensed to TriHealth, Inc.

BACKGROUND

- ☐ **TJC Std:** IM.02.01.01; IM.02.01.03; IM.02.02.03
- ☐ **Regulatory Agencies:**
- ☐ **Licensure**
- ☐ Other: C.F.R. 164.308

POLICY

Access:

Access to Information Technology (IT) resources must be controlled through access codes. Access codes and / or passwords must be compliant with Password Policy (#05_IS06.00)

All users of all TriHealth systems must have unique user identification, and a combination of one or more of the following: password, PIN, biometrics, challenge response questions, Tap 'N Go Employee Badges and/or tokens prior to using any Information Technology resources.

Users are responsible at all times for all activity performed with their personal access codes. Access codes must not be utilized by anyone but the individual to whom they are issued. Users must not allow others to perform any activity with their access codes.

User access will be verified annually by supervisors and/or managers of each user. System or Access Administrators will distribute a report to each Department Director, Manager, or Supervisor containing a list of employees, agency personnel, or agents of TriHealth, Inc., that have access to the network and applications and the level of their access. Each department will review the report and return the report with access modifications to the System Administrator. Access should only be permitted on a "need to know" basis. Changes in job category or job code require revocation of existing access privileges and re-authorization of access privileges.

Reasonable care shall be taken to ensure that unauthorized persons cannot view or access information displayed on the workstation monitor. All users must log off or lock unattended workstations, laptops, mobile devices, and other similar Information Technology equipment.

Remote Access:

Remote access allows TriHealth employees or other agents of TriHealth, Inc., to access the TriHealth network from outside of TriHealth's internal network. Remote access is available to authorized TriHealth employees or other agents of TriHealth, Inc.

Users requesting remote access must have their supervisor submit the Electronic Login Form found on LinkNet. The user is responsible for any cost associated with accessing TriHealth systems remotely and internet connection is needed for remote access. Users approved for remote access will receive appropriate installation documentation and access setup information. All remote access must use approved 2-factor authentication methods. The Remote Access Service Level Agreement (SLA) is signed at the time the packet is picked up and left with Corporate Security or the Information Systems Department. The SLA will be kept on file in the Information Systems Department.

When accessing TriHealth Systems from remote locations, users must access TriHealth systems via a computer or device that contains up-to-date anti-spyware, up-to-date antivirus, up-to-date software patches, and a firewall. Users utilizing TriHealth VPN or VDI (Virtual Desktop) will be subject to "access rejection" if these requirements are not met. Remote systems will be assessed upon attempt to connect. If the user's computer does not meet minimum TriHealth security requirements, the user will be denied access until the proper updates are performed.

Users who will be accessing sensitive information or PHI must not connect to TriHealth systems from areas where the public can view their screen. Accessing sensitive systems in unprotected viewing areas could expose TriHealth information and patient data.

Removing or Changing Access:

Human Resources and/or Managers will notify the Customer Support Help Desk of all TriHealth terminated and transferred employees. The Customer Support Help Desk will coordinate the procedure and notify the Outlook Distribution List called "/EA CIN IS Termination List" to change or revoke an individual's access to a system. Human Resources will directly communicate with the Information Systems Security Manager and TriHealth Corporate Security department if a terminated employee is considered to be a risk to security. Access will be removed in 2 business days or less upon notification from any authorized source.

Human Resources will send a Termination Report to the Outlook Distribution List called "/EA CIN IS Termination List" every pay period. This report will contain the employee's full name, employee number, department, title, and termination date and transfer/termination code. Each system security administrator will take appropriate action to change or revoke employee access to their system. Note that any access code which has not been used for 180 days will be disabled. The Termination List is maintained by the Information Systems Security Manager.

All Managers or Supervisors:

Access may be adjusted accordingly without notice to the user or user's manager if access is found to be inappropriate in conjunction with Corporate Security and / or Legal authorization.

Authentication and remote access:

Access to internal information assets requires at least one method of authentication.

There are three methods of authentication:

1) Possession based (something you have); examples include ID badge, Tap 'N Go Employee Badges, hardware authentication token
2) Knowledge based (something you know); examples include password, PIN, challenge response questions
3) Characteristic based (something you are); examples include biometric information

Remote access to TriHealth networks requires 2 of the above authentication methods (Two-Factor Authentication) or additional access control measures approved by Information Systems Security where feasible. Exceptions for Two-Factor Authentication will be reviewed by the Information Systems Security Manager. A hardware authentication token may not be shared.

Hardware Authentication Tokens (RSA Token) must be used with a corresponding personal identification number (PIN). The PIN must not be written on paper, any device or the computer used for access.

Hardware Authentication Tokens must not be stored in the same case/bag as portable computers used to remotely access TriHealth Information Systems.

Where tokens are required to access TriHealth infrastructure or information, TriHealth employees or other agent may only use tokens issued by TriHealth access administrators.

Tokens for agents or vendors requiring remote access (who are setup with the token 2-factor authentication) will be held and maintained by Information Systems Computer Operations. Vendors must pre-register with TriHealth providing accurate contact information. Access information including PIN will be provided at time of access need if correct verification is obtained and a return phone call can be made to the contact number of record.

Successful authentication DOES NOT imply authorization to access TriHealth information. Authorization access to information is the responsibility of the Information Owner.

Wireless Access:
TriHealth employees may not access the "TriHealth public wireless internet" from TriHealth owned Workstations or Laptops. The public wireless network is provided for patient use only. All access by employees to the public wireless internet must have a documented access request and approval from Information Security. Employees may connect mobile devices to the Bring Your Own Device (TH-BYOD) wireless network; personal devices cannot be connected to the internal network.

All laptops shall be configured to meet current minimum TriHealth standards and maintain compliance with all regulatory requirements.

Ad hoc wireless local area networks (WLAN) are not permitted without approval from Information Systems Networking and the Information Systems Security Manager.

Any employee or agent of TriHealth, Inc. found to have violated this policy, breached confidentiality or abused the privilege of TriHealth, Inc., access to information technology resources will be subject to the Performance Counseling policy.

OTHER AREAS/POLICIES OR PROCEDURES

Password Policy (#05_IS06.00)