Texas Health Resources®

Policy Name: Remote Access	
Policy Owner: Information Security Governance Council	**Effective Date:** 08/23/2019
Approved By: Alignment & Performance Team	**Last Reviewed Date:** 09/04/2023
Page 1 of 6	

1.0 Scope:

1.1 Applicable Entities:
This policy applies to:

- Texas Health Resources (Texas Health) and its member entities
- Texas Health Behavioral Health Virtual Visit
- Excludes the Texas Health joint venture entities (except those listed in the Formulation and Adoption of System-Wide Policies and Procedures in Section 4.1.6 or in Section 4.1.7)

1.2 Applicable Departments:
This policy applies to all Texas Health Workforce members, as well as members of Texas Health facility medical staff, trustees, Contractors, and Vendors who access the Texas Health network remotely.

2.0 Purpose:

2.1 This policy establishes a standard and secure protocol for Remote Access to Texas Health Information Assets.

3.0 Policy Statement(s):

3.1 Remote Access to Texas Health Information Assets should follow the requirements established in this policy to minimize security risks.

4.0 Policy Guidance:

4.1 Remote Access Services

4.1.1 Remote Access Services provide a gateway into the Texas Health network and application environment.

4.1.2 Remote Access Services can be used and supported on-premise (inside the Texas Health network) and off-premise (outside the Texas Heath network).

4.1.3 Remote Access Services can include, but not be limited to:

- Email communication services such as Microsoft Office 365 or Outlook Web Access

- External facing services, such as Texas Health eLink (Published Applications) and Texas Health Virtual Desktops
- Client Virtual Private Network or VPN

4.2 General Requirements

4.2.1 All Remote Access Service requests shall have a business justification.

4.2.2 Remote Access Services will be granted based upon organizational need and job requirements.

4.2.3 Remote Access Services are an extended offering, requiring management approval for all eligible employees.

4.2.4 Users of Remote Access Services shall adhere to the Teleworking policy.

4.2.5 Mobile devices must be used in accordance with Mobile Security, Photography and Secure Text Messaging policy

4.2.6 Remote Access Services must be controlled with Encryption and must be compliant with the Texas Health Encryption Policy.

4.2.7 Only ITS approved Remote Access Solutions are authorized. Please contact ITS for approved solutions.

4.2.8 Remote Access Services should be used for Texas Health business use only.

4.3 Authentication and Authorization

4.3.1 Remote Access Services will authenticate with a unique User ID and a strong password in accordance with the Password Management Policy.

4.3.2 Where applicable, Remote Access Services will use Strong Authentication, such as Multi Factor Authentication.

4.3.3 Only authorized and approved Texas Health employees, Vendors and Contractors are permitted to use Remote Access Services.

4.3.4 Vendor and Contractor Remote Access must have documented contract language specifying Remote Access requirements.

4.3.5 Any costs associated with Vendor or Contractor Remote Access shall be negotiated within the contract language.

4.3.6 Service Accounts are prohibited from using Remote Access Services.

4.3.7 Remote VPN access is not authorized for devices that are not owned and maintained by Texas Health.

4.4 Authorized Device Connectivity Requirements

4.4.1 Authorized devices must have the most current version of anti-virus software and operating system security patches installed.

4.4.2 Authorized devices must have reasonable security safeguards configured and implemented

4.4.3 Storage of Texas Health Confidential or Sensitive information on any personal device or personal storage media is prohibited.

4.5 Policy Exceptions, Violations and Sanctions

4.5.1 If there is a justifiable reason policy compliance is not possible, an exception may be granted. See the Policy Exception Procedure for additional information. Policy exceptions are processed through the IT risk management system.

4.5.2 Violations of this policy will be processed according to applicable Texas Health policies, including the Texas Health Performance Management Policy, as well as civil and criminal laws.

4.5.3 If you observe violations, you must promptly notify your supervisor, a representative of Human Resources, or the Compliance Hotline at 1-800-381-4728.

5.0 Definitions:

5.1 Confidential - Information, including patient information, protected information of participants in Texas Health benefit plans and programs, customer information, physician credentialing, peer review, quality review, business intelligence, privileged committee records, logon and password information, employee health records Protected Health Information, social security numbers, financial account information, or credit card information.

5.2 Contractor - Individual representative of third-party service provider with Texas Health Workforce responsibilities

5.3 Data - Any information in any medium including, but not limited to, desktop computers, laptop computers, telephones, fax machines, pagers, mobile

phones/smart phones, and tablets, as well as variations, such as multi-function fax/printer/copiers, and paper.

5.4 Encryption - A method used to convert Data from a readable clear text form to an unreadable format. This method is achieved by using an Encryption algorithm that combines plaintext with other values called keys, or ciphers, so that Data becomes unintelligible.

5.5 Information Assets - An interconnected set of information resources that shares common functionality. A system normally includes hardware, software, information, Data, applications, communications, and people.

5.6 Multi Factor Authentication - A method of confirming a User's claimed identity in which a User is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something they and only they know), possession (something they and only they have), and inherence (something they and only they are).

5.7 Published Applications - The process of delivering Published Applications is known as application remoting, where the application is physically installed on a separate device, such as a server in a data center, and virtualization software displays it on an endpoint.

5.8 Remote Access Services - The uses of telecommunications to allow authorized Access to the Texas Health Network, Data, Reports and Applications.

5.9 Sensitive Information - A subcategory of Confidential Information that identifies Protected Health Information (PHI), payment card Data, personally identifiable information (PII) or other Data that is required by federal/state law or industry mandated standards to apply security controls to protect Confidentiality, integrity, and availability.

5.10 Strong Authentication - Please see Multi Factor Authentication definition.

5.11 Service Account - A Service Account is a special user account that an application or service uses to interact with the operating system. Services use the Service Accounts to log on and make changes to the operating system or the configuration. Through permissions, you can control the actions that the service can perform.

5.12 Users - Texas Health Workforce members, members of Texas Health Facility Medical Staff, Trustees/Directors, Contractors, Vendors, or others who use the Texas Health information systems.

5.13 Vendor - An access management user Account and password dedicated to a specific vendor to perform application or system installation or maintenance.

5.14 Virtual Desktop (VDI) - Software technology that separates the desktop environment and associated application software from the physical client device that is used to access it.

5.15 Virtual Private Network (VPN) - A way to securely communicate over the Internet to a corporate network through a dedicated server that uses Encryption or other secure mechanisms.

5.16 Workforce - Employees, volunteers, persons involved in Texas Health training programs or those sponsored by its wholly owned or wholly controlled entities, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether they are paid by the entity or not.

6.0 Responsible Parties:

6.1 IT Risk Management and Assurance

6.1.1 Manages and participates in the development of Information Security policies and standards; identifies Security risks; performs risk-based assessments to ensure that Information Security risks are maintained at levels that are acceptable to Texas Health management.

6.2 Innovative Technology Solutions

6.1.2 The Texas Health department responsible for information technology systems and services. Participates in the development and maintenance of IT policies and standards; addresses risks and compliance requirements; develops operational procedures to support IT policies and standards.

6.3 Texas Health Information Security Officer

6.1.3 Provide completed audit document to Information Security; performs periodic audits for ITS systems used at their entities.

7.0 External References:

Not Applicable

8.0 Related Documentation and/or Attachments:

8.1 Encryption - THR System Policy

8.2 Confidentiality - THR System Policy

8.3 Information Privacy and Security Sanctions - THR System Policy

8.4 Password Management - THR System Policy

8.5 Safeguarding Health Information and Sensitive Personal Information - THR System Policy

8.6 Teleworking - THR System Policy

8.7 Performance Management (formerly Progressive Corrective Action) - THR System Policy

8.8 Acceptable Workstation Use and Mobility Device Use - THR System Policy

8.9 Endpoint Security ITP-04 - THR System Policy

8.10 Access Management - THR System Policy

8.11 Mobile Security, Photography and Secure Text Messaging ITP-14 - THR System Policy

9.0 **Required Statements:**

Not Applicable