TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER SCHOOL OF MEDICNE PSYCHIATRY DEPARTMENT POLICY AND PROCEDURE		REVIEW NO: 1	NUMBER:
PREPARED BY: BLAIR TORRES	APPROVED BY: SARAH WAKEFIELD, MD CHAIR	ORIGINAL APPROVAL DATE: September 2023	MOST RECENT REVIEW APPROVAL DATE: December 4, 2023
TITLE: Departmental Remote Work Policy			PAGE: 1of 10

A. GENERAL STATEMENT OF POLICY:

a. Statement of Purpose: The Department of Psychiatry to establish policies for remote work for non-faculty employees. Psychiatry recognize the potential mutual benefits that remote work may afford in creating a flexible, safe, and supportive work environment for certain employees and employee positions.

B. SCOPE: This policy covers the entirety of the Psychiatry Department.

C. Important HSC OP Policies:

a. HSC OP 56.02.3(d): Remote workers are responsible for providing their own networking/internet connectivity equipment and for the costs associated with service.

b. HSC OP 56.02.1(b): All team members who request permission for remote work, must demonstrate that they have a secure work environment at the remote location. A secure work environment is one where all of the requirements for acceptable use are followed. This includes the requirements outlined in all relevant policies, standards, and procedures related to network connectivity and the access, use, transfer, storage and disposal of TTUHSC information and information systems.

c. HSC OP 56.02.2(b): Team members requesting a remote work arrangement are required to use a TTUHSC-issued computer or other electronic device. The specifications for approved equipment are listed in the IT Division's Technology Specifications for Remote Workers standard. Full support services from the TTUHSC ITSC are provided for approved, TTUHSC- owned equipment.

d. OP 70.49: System Remote Work

D. ADMINISTRATION & PROCEDURE:

a. Immediate supervisors will have the responsibility for monitoring employees remote work and may revoke work from home benefits if deemed necessary.

b. Zoom Chat

  i. Unless discussed with your immediate supervisor, all employees working remotely must log into their Zoom Chat business account during business hours. If you have issues with this application please submit a work order request to Psychiatry IT.

c. CXOne Workplace

  i. Team members working remotely will need to setup their office number to be reached remotely through their work approved equipment (e.g., laptop).

d. Virtual Meetings Expectations

i. Names will be displayed (first then last or Dr. Last name)
ii. Professional head shot will be uploaded to the image place holder in Zoom Web camera will be turned on for meetings
iii. Exceptions exist. However, team member camera should be on the majority of the meeting.
iv. Business attire is to be worn during meetings (business casual is appropriate) Always be aware of camera angles and standing up in front of the webcam
v. Angle webcams away from the ceiling; camera should face straight ahead to reduce distractions of fans and light fixtures Limit settings with back-light
vi. Do not attend video meetings with an open window behind you, visibility becomes difficult in these settings
vii. Make sure you are in a well-lit area for all Zoom meetings, this may require team members to use a Lumecube to provide additional lighting
viii. Have a clean and clutter free background to limit distractions Use an approved Zoom background

E. **DISTRIBUTION:** This policy will be distributed to the Psychiatry department and made electronically accessible to all relevant personnel.

F. **APPROVAL AUTHORITY:** This policy shall be recommended for approval through the department Faculty and Chair.

G. **RESPONSIBILITY AND REVISIONS:** It is the responsibility of the department Faculty and Chair to review and initiate necessary revisions based on collaboration and input by and through department leadership, Risk Management and the Office of Institutional Compliance.

H. **RIGHT TO CHANGE POLICY:** TTUHSC Psychiatry Department reserves the right to interpret, change, modify, amend or rescind this policy in whole or in part at any time to reflect changes in policy and/or law.

I. **CERTIFICATION:** This policy was approved September 2023 and will undergo biennial reviews thereafter.

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 56.02, **Information Resources for Remote Work**

PURPOSE: This Texas Tech University Health Sciences Center Operating Policy (TTUHSC OP) outlines the requirements for secure access to TTUHSC information, networks, and computing resources by team members authorized for remote work at alternative worksites.

REVIEW: This OP will be reviewed annually in July by the Vice President of Information Technology and Chief Information Officer (CIO), the Assistant Vice President of Information Security and Information Security Officer (ISO), and the Managing Director of the IT Solution Center.

TABLE OF CONTENTS

POLICY:

This policy outlines requirements for TTUHSC Information and Information System use for remote work. Remote work constitutes an agreement between the team member and their supervisor (or department head) granted only when the remote work promotes administrative efficiency, improved productivity, business continuity, and the hiring and retention of highly performing values-based teams. In order for remote work agreements to be finalized, a secure remote work environment must be established in accordance with the requirements outlined in this policy as well as in all related procedures and guidelines.

1. Definitions

a. Remote Work

The performance of normal work duties at an alternative work location away from the regularly assigned place of work. Permission to work remotely may be granted through the team member's supervisor and TTUHSC HR based on the submission of a Standard Remote Work Agreement, completed through the online Remote Work application.

b. Secure Remote Work Environment

All team members who request permission for remote work, must demonstrate that they have a secure work environment at the remote location. A secure work environment is one where all of the requirements for acceptable use are followed. This includes the requirements outlined in all relevant policies, standards, and procedures related to network connectivity and the access, use, transfer, storage and disposal of TTUHSC information and information systems.

c. Data Classification

All TTUHSC data requires the implementation of privacy and security safeguards classifying it as Public, Sensitive, Confidential, or Regulated as mandated by federal, state, and/or local law, or university policy or agreement. A full explanation of TTUHSC data classification can be found in the Security Categorization of Information and Information System Impact Standard.

2. IT Division Remote Work Review

Before a team member is granted permission to work at an alternative worksite, the IT Division must review the Remote Work Application to assess the equipment to be used and the TTUHSC data that will be managed under the agreement.

Please note: *TTUHSC IT determines appropriate equipment specifications but equipment purchases are the responsibility of the team member's department.*

a. IT Solution Center (ITSC) Equipment Assessment

The ITSC will assess the proposed equipment to be used at the remote worker's location. Equipment will be categorized according to the service support levels outlined in the ITSC Appendix to the TTUHSC IT Service Level Agreement (SLA). Those levels are summarized as:

(1) Recommended for remote work (*Full Hardware and Software Support provided*)

(2) Not Recommended for remote work (gaps in readiness of equipment being assessed for remote work; *Best Effort Hardware and Software Support provided*)

(3) Not Supported for remote work (*ITSC support not provided*)

For equipment categorized as Not Recommended and Not Supported, the ITSC will work with the team member's supervisor to resolve issues in order to meet the requirements of the Recommended category.

b. **Hardware and Software Requirements for Alternative Work Locations**

Team members requesting a remote work arrangement are required to use a TTUHSC-issued computer or other electronic device. The specifications for approved equipment are listed in the IT Division's Technology Specifications for Remote Workers standard. Full support services from the TTUHSC ITSC are provided for approved, TTUHSC-owned equipment.

c. **Documenting Institutional Property to be Used at Alternative Work Locations**

All institutional equipment and software approved for the team member for remote work must be listed in the Remote Work Application. That information must include:

- the asset tag number
- the serial number
- a description of the equipment/software to be provided

3. **Information Resource Compliance Requirements**

a. **Software License Restrictions**

Remote workers must follow software licensing restrictions and agreements on all software used to process TTUHSC information at alternative worksites.

b. **Information Technology Policy and Procedure Compliance**

Remote workers must follow all TTUHSC IT policies and procedures for securing information and information systems. Shredders must be used to dispose of hard copies of Sensitive Information or higher.

c. **Approved Remote Work Equipment**

The team member's department is responsible for the purchase of all needed equipment and should work with the IT Solution Center to purchase equipment with recommended specifications.

Team members **MUST NOT** use their own mobile computing devices, computers, computer peripherals, or computer software for TTUHSC remote work-related business.

Exception: personal devices may be used when using Remote Desktop Connection to access a TTUHSC-owned computer or device to perform TTUHSC-related business.

However:

- personal mobile devices may be used for TTUHSC-provided Avaya IX soft phone product for phone calls, and
- personal mobile devices may be used for approved mobile email clients (Microsoft Outlook, native email clients) for TTUHSC mail.

d. **Networking and Connectivity Requirements**

Remote workers are responsible for providing their own networking/internet connectivity equipment and for the costs associated with service.

Remote workers should follow the guidelines for appropriate internet connectivity found in the Home Network and Internet Service Provider for Remote Workers standard.

4. **Access Control**

Access Control for TTUHSC devices is covered in HSC Operating Policy 56.01 Acceptable Use and

TTUHSC IT Policy 56.08 Access Control. Elements of Access Control related to remote work include the following:

a. **Screen Positioning**

The display screens for all systems used to handle TTUHSC information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

b. **Logging Out**

After a team member has completed a work session with TTUHSC equipment, they must terminate their work session by logging off and locking their computer.

When applicable, team members who remotely access TTUHSC networks, must terminate their session after their tasks are completed and remote access is no longer needed.

c. **Encryption**

All computers used for remote work must be encrypted using TTUHSC-managed encryption methods.

d. **Access to Devices and Systems**

Remote workers must **not** share passwords or any other access to TTUHSC devices with anyone. Computers used for TTUHSC business must be used exclusively by the remote worker. Family members, friends, and any other unauthorized persons are not permitted to use TTUHSC devices. Remote workers must never lend to others any computer or device that contains. TTUHSC information.

5. **Data Storage**

Remote workers must store TTUHSC information in accordance with the TTUHSC IT Data Storage Standard.

a. **Encryption of Data on External Media**

For approved business cases, Sensitive Information or higher written to external storage media (e.g., CDs/DVDs, USB drives, etc.) must be encrypted using TTUHSC-approved encryption methods.

6. **Remote Device Management**

a. **Configuration**

Team members must **not** change the operating system configuration or download and/or install unauthorized software.

All software changes and updates must be performed by the ITSC or authorized departmental IT staff.

b. **Changes to Hardware**

Team members must **not** alter TTUHSC hardware without the prior knowledge and authorization of the TTUHSC IT Division.

c. **Liability for TTUHSC Property**

Team members are responsible for any and all equipment and software used at the remote worksite, and accept financial responsibility for any equipment that is lost, stolen, or damaged as the result of negligence, misuse, or abuse.

TTUHSC retains title, rights, and interest to any TTUHSC assets supplied for remote work. Remote worker use does not convey ownership or any implication of ownership of TTUHSC assets.

d. Liability for Team Member-Owned Property

TTUHSC will not be responsible for the operating costs, home maintenance, or any other incidental costs (e.g., utilities, telephone, insurance) associated with the use of an alternative worksite for remote work.

e. Return of Property

All TTUHSC-supplied assets for remote work must be promptly returned to TTUHSC when a remote worker separates from TTUHSC, or when so requested by the remote worker's manager.

7. Physical Security

a. TTUHSC Property at Alternative Worksites

Equipment must be protected from environmental threats and hazards, and opportunities for unauthorized access.

Reasonable precautions must be taken to protect TTUHSC hardware, software, and information from theft, damage, and misuse.

b. Printers

When allowed, only TTUHSC-provided printers can be used by team members to print out work-related documents. Team members must either submit a work order to the ITSC or request that their departmental IT set up a printer equipped to work with TTUHSC-approved computers. Please see the Technology Specifications for Remote Workers standard for equipment recommendations.

c. Transportation of TTUHSC Assets to/from TTUHSC

Regulated and Sensitive Information or higher should not be stored or transported on removeable media without prior TTUHSC IT approval.

The following requirements must be followed for transporting TTUHSC assets:

(1) All TTUHSC assets to be transported must be encrypted using TTUHSC-managed encryption;

(2) Where feasible, all TTUHSC assets to be transported should be placed in the trunk or an inconspicuous location in the vehicle when in transit—do not place the equipment or device on the vehicle's seat.

8. IT Support

Remote worker equipment will be subject to the support outlined in the ITSC Appendix in the TTUHSC IT SLA.

9. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. TTUHSC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

a. Disciplinary Repercussions

Misuse of TTUHSC Information or Information Systems is a violation of the policies contained herein and can result in disciplinary action in accordance with, but not limited to, TTUS Regulations 07.07 Employee Conduct, Coaching, Corrective Action, and Termination and HSC OP 77.05 Suspension and Retention, as well as the Student Handbook.

10. Related Statutes, Policies, and Requirements

Digital Millennium Copyright Act
Digital Millennium Copyright Act of 1998

Health Insurance Portability and Accountability Act
HIPAA, Title 45, Subchapter C, Part 164

Payment Card Industry (PCI) Data Security Standard (DSS)
PCI-DSS: 12.3 Acceptable Usage

Texas Administrative Code
TAC 202, Subchapter C, 70-76

Texas Public Information Act
Texas Public Information Act

Texas Security Control Standards Catalog
Texas DIR Security Control Standards Catalog

TTUHSC IT Areas of Responsibility
Areas of Responsibility

11. Document Details

Approval and Ownership

Approved By	Vince Fell
Title	Vice President for Information Technology and Chief Information Officer
Approval Date	7/10/2020
Owner(s)	IT Executive Management Team

Revision History

Version	Description	Date Reviewed	Date Submitted for Publishing	Reviewer(s)
1.0	Initial version.	7/10/2020	7/13/2020	VP for IT and CIO, AVP of Information Security and ISO, Managing Director of the ITSC, Director of IT GRC, Director of IT Security Operations, and Director of IT Policy and Planning.
2.0	Revision	7/29/2022	08/12/2022	IT GRC, Managing Director of ITSC