HSC OP: 56.02, Remote Work at Alternative Worksites

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 Every Year (EY) 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: .....................................................................................................................................................................3
1. Definitions .................................................................................................................................................................3
   a. Standard Remote Work ........................................................................................................................................3
   b. Regulated Information ........................................................................................................................................3
   c. Sensitive Information .......................................................................................................................................3

2. IT Division Remote Work Review ..........................................................................................................................3
   a. IT Solution Center (ITSC) Equipment Categorization ....................................................................................3
   b. Documenting Institutional Property to be Used at Alternative Work Locations .......................................4
   c. Hardware and Software Considerations for Alternative Work Locations .................................................4

3. Information Resource Compliance Requirements ..................................................................................................4
   a. Software License Restrictions .........................................................................................................................4
   b. Information Technology Policy and Procedure Compliance .......................................................................4
   c. Approved Remote Work Equipment ................................................................................................................4
   d. Networking and Connectivity Requirements ..................................................................................................5

4. Access Control ........................................................................................................................................................5
   a. Screen Positioning ...........................................................................................................................................5
   b. Logging Out ....................................................................................................................................................5
   c. Encryption .....................................................................................................................................................5
   d. Sharing Access Devices and Systems .............................................................................................................5

5. Backup and Media Storage ...................................................................................................................................5
   a. Backup Procedures and Media Storage ...........................................................................................................5
   b. Regulated and Sensitive Media Marking ........................................................................................................5

6. Remote Device Management ................................................................................................................................6
   a. Setting Date and Time ......................................................................................................................................6
   b. Changes to Configurations and Software .......................................................................................................6
   c. Changes to Hardware ..................................................................................................................................6
   d. Ownership vs. Possession ...............................................................................................................................6
   e. Liability for TTUHSC Property .......................................................................................................................6
   f. Liability for Team member-Owned Property ................................................................................................6
7. Physical Security
   a. TTUHSC Property at Alternative Worksites
   b. Secure Storage of Data
   c. Printers
   d. Transportation of Regulated and Sensitive Information to/from TTUHSC

8. IT Support

9. Violations
   a. Disciplinary Repercussions

10. Related Statutes, Policies, and Requirements

11. Document Details
POLICY:
Utilizing a work strategy other than traditional (i.e., an alternative work arrangement) is an agreement between the team member and their supervisor (or agency head for certain strategies) granted only when the strategy promotes administrative efficiency, improved productivity, business continuity, and the hiring and retention of highly performing values-based teams. Though potentially of great benefit to TTUHSC’s operations, it is essential that all remote work be performed in a secure computing environment. All TTUHSC policies, procedures, guidelines, and standards apply to remote workers, including those specific to information technology and information security.

1. Definitions
   a. Standard Remote Work
      The permanent performance of normal work duties at an alternative work location away from the regularly assigned place of work which may also be a hybrid schedule of on campus/remote work. The alternative off-site location is most often the team member’s home and requires a Standard Remote Work Agreement, completed through the online Remote Work application.
   b. Regulated Information
      Data that requires TTUHSC to implement specific privacy and security safeguards as mandated by federal, state, and/or local law, or university policy or agreement. Regulations or categories of data most applicable to TTUHSC include:
      (1) Family Educational Rights and Privacy Act (FERPA)
      (2) Health Insurance Portability and Accountability Act (HIPAA)
      (3) Social Security Numbers (SSNs)
      (4) Gramm Leach Bliley Act (GLBA)
      (5) Payment Card Industry Data Security Standards (PCI-DSS)
      (6) Sensitive Identifiable Human Subject Research
   c. Sensitive Information
      TTUHSC data routinely used in conducting business not covered by state or federal privacy law. It is protected to preserve the privacy, safety, or reputation of individuals and/or TTUHSC.

2. IT Division Remote Work Review
   The IT Division must review all requests for remote work before the team member is granted permission to work at an alternative worksite. In addition to the below policy requirements for remote work, team members must adhere to the guidelines set in the Remote Work application to initiate this process. Please note: While the IT Division can make recommendations on the best equipment setup for remote workers, the Division is not responsible for equipment purchases.
   a. IT Solution Center (ITSC) Equipment Categorization
      After assessing the equipment proposed to be used at the remote worker’s alternative work location, the ITSC will categorize the equipment in one of three categories:
      (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. Documenting Institutional Property to be Used at Alternative Work Locations

After the team member and their supervisor initiate the Remote Working Agreement process, the Institutional equipment and software to be provided to the team member at their alternative work location must be documented in the electronic request’s form. Provide the asset tag number, serial number, and description of the equipment/software.

c. Hardware and Software Considerations for Alternative Work Locations

Specifications have been provided in the IT Division’s Technology Specifications for Remote Workers standard and outline requirements for reliable performance and connectivity to facilitate remote worker productivity. Providing remote workers with equipment that meet the following minimum standards ensures they have the appropriate tools to perform their job duties and are eligible to receive Full support services from the TTUHSC ITSC. Equipment that does not meet minimum specifications may impede remote workers’ abilities to perform their job functions and will be subject to Best Effort support as indicated in the TTUHSC IT Service Level Agreement (SLA). In rare instances, remote worker equipment might not be eligible for any ITSC support—this would be evaluated and discussed with the supervisor.

The IT Division’s technology standards and recommendations are regularly reviewed and updated to reflect current industry standards. Adjustments to these standards and recommendations will be made as deemed necessary to ensure a successful remote work environment.

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 information technology security policies and procedures including, but not limited to, compliance with software license agreements, securing all hard copy and digital materials, including those with regulated and sensitive information, and use of shredders to dispose of regulated and sensitive hard copy information.

c. Approved Remote Work Equipment

Team members working on TTUHSC business at alternative worksites must use TTUHSC-provided computers and related equipment (e.g., webcam, computer headset, printer/scanner). 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. The only exception to this is for team members that require phone capabilities, their personal mobile device may be used to make calls, using the TTUHSC-provided Avaya IX soft phone product and, for accessing TTUHSC emails using approved mobile email clients. Approved mobile email clients include Microsoft Outlook and native email clients on the team member’s mobile device.
See the ITSC’s, Remote Worker Technology Standards web page for guidance on purchasing equipment for remote workers.

d. Networking and Connectivity Requirements

Remote workers must provide their own networking/internet connectivity equipment and are responsible for the cost of internet connectivity. Guidance for establishing at-home, stable, high-speed internet can be found at the ITSC’s Remote Worker Technology Standards web page. Ethernet connections are recommended.

Please note that any equipment that does not meet minimum specifications may impede the remote worker’s abilities to perform their job functions and will be subject to Best Effort support as indicated in the TTUHSC IT SLA.

4. Access Control

a. Screen Positioning

The display screens for all systems used to handle TTUHSC regulated or sensitive 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 computers, the team member must terminate their work session by logging off and locking their computer.

When applicable, team members that remote access TTUHSC assets 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 IT Division-approved encryption methods.

d. Sharing Access Devices and Systems

Remote workers must not share passwords or any other access devices or parameters with anyone. This also means that computers used for TTUHSC business must be used exclusively by the remote worker. Family members, friends, and any others unauthorized must not be permitted to use TTUHSC devices. Remote workers must never lend to others any computer or device that stores TTUHSC information.

5. Backup and Media Storage

a. Backup Procedures and Media Storage

It is recommended that remote workers backup their data on a regular basis, ensuring TTUHSC IT Division-approved encryption methods are utilized. Please reach out to the ITSC for recommendations on devices to use and for assistance with this process.

b. Regulated and Sensitive Media Marking

When sensitive information is written to external storage media (e.g., CDs/DVDs, USB drives, etc.), the media must be externally marked with the highest relevant regulated or sensitivity data classification (e.g., PHI, PII, Confidential).
6. Remote Device Management
   a. Setting Date and Time
      Remote workers must keep their remote computers’ internal clocks synchronized to TTUHSC local date and time (Central Standard Time/Central Daylight Time).
   b. Changes to Configurations and Software
      On TTUHSC-supplied computer hardware, workers must not change the operating system configuration nor download and/or install unauthorized new software. If such changes are required, they must be performed by ITSC personnel with remote system maintenance software. Changing the font defaults for a word processing program, or otherwise altering the templates provided with an application is permissible without ITSC assistance or advance approval.
   c. Changes to Hardware
      Remote computer equipment supplied by TTUHSC must not be altered or added to in any way without prior knowledge and authorization from the IT Division.
   d. Ownership vs. Possession
      If TTUHSC supplied a remote worker with software, hardware, furniture, information or other materials to perform TTUHSC business remotely, the title to, and all rights and interests to these items will remain with TTUHSC. In such instances, remote worker possession does not convey ownership or any implication of ownership.
   e. Liability for TTUHSC Property
      The remote worker is responsible for any and all equipment and software that is used at the remote worksite, and accepts financial responsibility for any equipment that is lost, stolen, or damaged because of negligence, misuse, or abuse.
   f. Liability for Team member-Owned Property
      TTUHSC is not liable for damages to the remote worker’s personally-owned equipment resulting from remote working. TTUHSC will not be responsible for 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.
   g. Return of Property
      If TTUHSC supplied a remote worker with software, hardware, furniture, information or other materials to perform TTUHSC business remotely, all such items 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 should be located in an area to best protect from and reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The security of TTUHSC property at an alternative worksite is just as important as it is at the central office. At alternative worksites, reasonable and prudent precautions must be taken to protect TTUHSC hardware, software, and information from theft, damage, and misuse.
   b. Secure Storage of Data
      Workers who must handle and store regulated and sensitive information at their homes in order to do their work must have a secure method of storing and protecting data. For information related
to appropriate regulated and sensitive data disposal, data storage options, and shredders, please refer to the TTUHSC Office of Institutional Compliance’s *HIPAA Considerations When Working from Home* document for detailed guidance.

c. **Printers**

When allowed, only TTUHSC-provided printers will be used by team members to print out work-related documents. Team members must submit a work order to the ITSC to have the printer set up and equipped to work with TTUHSC-approved computers. Please see the *Technology Specifications for Remote Workers* standard for equipment recommendations.

d. **Transportation of Regulated and Sensitive Information to/from TTUHSC**

Computers, and removable media with regulated and sensitive information should not be transported between the regular TTUHSC worksite and the remote worksite unless instructed by the remote team member’s supervisor. The following requirements must be followed for transporting equipment and devices with regulated and sensitive information:

1. Regulated and sensitive information stored on computers and removal media devices (e.g., USB drives, external hard drives, CDs/DVDs) must be encrypted using TTUHSC’s approved methods;

2. Place equipment and devices in the trunk or an inconspicuous location in the vehicle when transporting—do not place the equipment or device on the vehicle’s seat;

3. Avoid running errands or making stops that result in the vehicle being left unattended, even for short periods of time. Best practice is to go directly from the remote work location to the TTUHSC campus, and vice versa.

8. **IT Support**

Remote worker equipment will be provided the same support outlined in the TTUHSC IT SLA, with the level of support provided dependent upon the categorization determined during the IT Division Remote Work Review.

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 IR is a violation of the policies contained herein and can result in disciplinary action in accordance with, but not limited to, TTUHSC OPs 70.31 *Employee Conduct, Coaching, Corrective Action, and Termination* and 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**

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Vince Fell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Vice President for Information Technology and Chief Information Officer</td>
</tr>
<tr>
<td>Approval Date</td>
<td>7/10/2020</td>
</tr>
<tr>
<td>Owner(s)</td>
<td>IT Executive Management Team</td>
</tr>
</tbody>
</table>

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Date Reviewed</th>
<th>Date Submitted for Publishing</th>
<th>Reviewer(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version.</td>
<td>7/10/2020</td>
<td>7/13/2020</td>
<td>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.</td>
</tr>
<tr>
<td>1.1</td>
<td>Minor updates.</td>
<td>7/29/2020</td>
<td>7/31/2020</td>
<td>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.</td>
</tr>
</tbody>
</table>