



Policy Name: Acceptable Workstation and Mobile Device Use	
Policy Owner: Information Security Governance Council	Effective Date: 02/22/2023
Approved By: System Performance Alignment & Innovation (SPAN)	Last Reviewed Date: 02/22/2023
Page 1 of 9	

1.0 Scope:

1.1 Applicable Entities:

This policy applies to:

- Texas Health Resources (Texas Health) and its member entities
- 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 utilize Texas Health Workstations and Mobile devices to conduct Texas Health Confidential or Sensitive patient business.

2.0 Purpose:

- 2.1** The purpose of this policy is to outline the acceptable use of Workstations and Mobile devices at Texas Health. These rules are in place to protect the employee and Texas Health. Inappropriate use exposes Texas Health to risks including virus attacks, compromise of network systems and services, and legal issues.



3.0 Policy Statement(s):

- 3.1** Workstations and Mobile devices are to be used to conduct Texas Health business according to all applicable Texas Health policies and regulations.
- 3.2** When using a Workstation or Mobile device to Access a server or host application system, Users should expect variation in what constitutes acceptable use. Reasonable efforts should be made to learn the policies applicable to each system used. Questions about the permissibility of an action should be directed to the supervisor and/or system administrator before execution.

4.0 Policy Guidance:

4.1 Workstations and Mobile Device Use

- 4.1.1** Workstations and Mobile devices must only be used by authorized Texas Health Workforce or vendor representatives following the requirements defined in the approved Texas Health policies and standards.

- 4.1.2 Mobile devices must be used in accordance with Mobile Security, Photography and Secure Messaging policy.
- 4.1.3 Authentication to the Texas Health network requires a unique User ID and password. Users are required to follow good security practices in the selection and use of passwords according to the Password Management policy.
- 4.1.4 Screen savers are to be used on all Workstations, in accordance with Endpoint Security policy. Screen savers and Workstation lockouts will be configured in accordance with the Endpoint Security policy.
- 4.1.5 Anomalous or malicious behavior on a Workstation, Mobile device, or application must be reported to the ITS Service Desk immediately.
- 4.1.6 Users should be very cautious when opening email and clicking on website links within email.
- 4.1.7 Users must not respond to any emails that request personal or financial information. Users should report suspicious emails using the “Report Phish” button in Outlook or verify the message by directly contacting the person or institution requesting the information.
- 4.1.8 Workstations must be password protected where feasible. This protects Sensitive or Confidential Information from being inappropriately displayed should the User accidentally leave the Workstation without manually enabling the screen saver.
- 4.1.9 Users must lock their Workstations when they leave. The following can be used:
 -  +  (“Windows Symbol” key + “L” key)
 - Ctrl + Alt + delete, Lock this computer
- 4.1.10 For all Workstations that are not located in 24/7 departments, Users must log out of all applications, and log out of the network at the end of the business day or User workday.

Workstations dedicated to supporting a specific application or Information System (e.g., clinical Workstations) are not required to be logged out of the specific application or logged out of the network at the end of the business day.

4.1.11 Texas Health Resources workforce will only be issued one device to conduct business, regardless of how many locations they perform business. Exceptions must be approved by ITS CIO.

4.1.12 All managers/supervisors are responsible for returning all THR workforce IT provided equipment, within 3 business days after separation from THR to the nearest IT Field Service office.

4.2 Software and Operating System Configuration

4.2.1 All Workstations will be configured according to approved Texas Health policies and standards.

- Unauthorized changes to the desktop hardware, file structure, or system configuration are prohibited.
- Application features are not to be disabled (e.g., virus software or auditing capabilities).

4.2.2 Users are not permitted to download, install, or save any unauthorized software or applications to the network or hard drives without prior approval from ITS.

4.2.3 Users are not authorized to configure Workstations or Mobile devices to bypass security controls.

4.2.4 Mobile devices that are used to Access Texas Health systems and information must be configured in accordance with the Mobile Security, Photography and Secure Messaging policy.

4.3 Storing Documents and Files

4.3.1 Work-related documents, including Confidential and Sensitive Information, must be stored on appropriate network drives and not locally on a Workstation.

4.3.2 Data must not be stored on, transferred to, or transferred from, hard drives or removable media like USB devices, and diskettes unless there is a legitimate business purpose.

4.3.3 Sensitive Information stored on removable media, for legitimate business purposes, must be encrypted.

4.3.4 All data shall be cleared from removable media when no longer needed.

- 4.3.5 Data stored on network drives are backed up and available for restoration in the event of data loss.
- 4.3.6 If the User's designated share on a network drive becomes full, the User should contact the ITS Service Desk for remediation.
- 4.3.7 Storing of Confidential or Sensitive Information within cloud-based file and photo sharing services (Dropbox, Google Drive, Instagram etc.) is not authorized unless the cloud service has been evaluated and approved by Texas Health ITS. Questions on which cloud services are authorized should be directed to the Texas Health ITS Service desk.
- 4.3.8 Texas Health SharePoint sites that store Sensitive Information need to be approved and authorized by ITS.

4.4 Physical Placement and Monitoring

- 4.4.1 Physical Workstation placement should minimize the possibility of unauthorized personnel viewing screens or data.
Physical devices, such as privacy guards, are used where needed to limit visibility of Confidential and Sensitive Information to unauthorized personnel.
- 4.4.2 Workstation use and activity is monitored.
- 4.4.3 Department managers are ultimately responsible for the physical placement and monitoring of Workstations in their areas.
- 4.4.4 Missing or stolen Workstations or Mobile devices must be immediately reported to the ITS Service Desk.

4.5 Asset Documentation

- 4.5.1 Workstations and Mobile devices designated for transfer within or between entities will comply with Supply Chain Management Asset Transfer, Disposal and Sale policy.
- 4.5.2 Workstations designated for external relocation, disposal, sale, or donation will be appropriately tracked according to Texas Health inventory management guidelines to ensure appropriate tracking, hardware sanitizing, and disposal.

4.6 Asset Management and Protection

- 4.6.1 All Workstations and Mobile devices purchased by Texas Health are considered company assets throughout the life of the asset.
- 4.6.2 Workstations must not be relocated or changed by anyone other than authorized Texas Health employees or vendors.
- 4.6.3 Workstations will be protected on and off Texas Health premises.
- Security locks, alarms, or tracking devices will be appropriately used to physically secure Workstations in areas that are accessible to the public. The User and department manager are jointly responsible for securing devices and ensuring compliance.
 - Workstations that will be sent offsite for vendor maintenance will require an appropriate entity asset tracking form or service agreement, with the asset tracking details documented with the appropriate ticket tracking tool.
 - Users of laptops and Mobile devices are expected to follow Texas Health policies, best practices, and industry standards to avoid laptop/Mobile device theft and/or breach of Sensitive or Confidential Information.
 - Workstations, Laptops and Mobile devices that store or process Sensitive or Confidential Information must be physically protected at all times.
 - Laptops and Mobile devices shall not be left unattended in vehicles.
 - Stolen or lost computers or Mobiles devices shall be reported to the employee's manager and ITS Service Desk immediately.
 - Good judgment and reasonable care is to be exercised to avoid damaging equipment (e.g., do not drop the device or spill liquids on equipment).

4.7 Workstation and Mobile Device Use

- 4.7.1 Appropriate use of resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, including Copyright and harassment laws. Workstations are to be used primarily for conducting Texas Health business.

- 4.7.2 Attempts to maliciously sabotage systems or networks using Texas Health resources are prohibited.
- 4.7.3 Attempts to make a computer impersonate other systems, particularly via forged email, talk, news, etc., are prohibited.
- 4.7.4 Users may not use their Texas Health accounts to attempt to gain unauthorized Access to Texas Health or non-Texas Health systems.
- 4.7.5 Users should limit personal use of the internet.
- 4.7.6 Unless the Information System is unavailable for maintenance or there is a specified business reason preventing routine User Access, Texas Health Users may not deliberately deny authorized Users Access to systems.
- 4.7.7 Users are not to interfere with, or alter the integrity of, the Information System at large by destruction or unauthorized alteration of data or programs belonging to other Users.

4.8 Policy Violations and Sanctions

- 4.8.1 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.
- 4.8.2 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 Access - The ability to read, write, modify, or communicate data/information or otherwise use any system resource.
- 5.2 Authentication - Verification of a person or entity identity via password, biometrics, challenge/response, token cards, and other methods.
- 5.3 Authorization - Granting of privileges to use a Workstation, application, or program for Texas Health business purposes.
- 5.4 Confidential Information - 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.

- 5.5 Copyright - A form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of original works of authorship including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works.
- 5.6 Innovative Technology Solutions (ITS) - A Texas Health department responsible for information technology systems and services.
- 5.7 Mobile - The ability to use technology untethered to allow Access to information or applications from occasionally connected, portable, or networked computing devices.
- 5.8 Personally Identifiable Information (PII) - Any data that can be used to distinguish or trace an individual's identity. Any information that can be used to distinguish one person from another and that can be used for de-anonymizing anonymous data can be considered PII. For example, the individual's name, social security number, biometric records, etc., either alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- 5.9 Protected Health Information (PHI) - Individually Identifiable Health Information that is protected by the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Texas state law. Information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
- 5.10 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.
- 5.11 Users - Texas Health Workforce members, members of Texas Health facility Medical Staff, Trustees/Directors, contractors, vendors, or others who use the Texas Health Electronic Communication Systems.

5.12 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 or not they are paid by the entity.

5.13 Workstation - Information processing equipment, including desktop computers, laptops, wireless and Mobile devices.

6.0 Responsible Parties:

6.1 Device Engineering

6.1.1 Responsible for procuring, securing, supporting, managing, and maintaining Workstations and other devices connected to the Texas Health network.

7.0 External References:

7.1 ASU Information Technology. (n.d.). Acceptable Use and File Sharing Policies. Retrieved February 4, 2016, from

http://www.angelo.edu/services/technology/network/file_sharing.php

7.2 ASU Information Technology. (n.d.). Phishing Awareness. Retrieved February 4, 2016, from <http://www.angelo.edu/services/technology/support/phishing.php>

7.3 Lininger, R., & Vines, R. D. (2005, May). E-mail policies -- A defense against phishing attacks. Retrieved February 4, 2016, from <http://searchsecurity.techtarget.com/feature/E-mail-policies-A-defense-against-phishing-attacks>

7.4 Oracle. (2015). Best Practices for Hardware Configurations. Retrieved January 28, 2015, from http://download.oracle.com/otn_hosted_doc/timesten/1122/quickstart/html/best_practices/bp_hw.html.

7.5 SEC.gov. (2013, September 5). "Phishing" Fraud: How to Avoid Getting Fried by Phony Phishermen. Retrieved February 4, 2016, from <https://www.sec.gov/investor/pubs/phishing.htm>

8.0 Related Documentation and/or Attachments:

8.1 [Electronic Communications Acceptable Use - THR System Policy](#)

8.2 [Endpoint Security ITP-04 - THR System Policy](#)

Policy Name: Acceptable Workstation and Mobile Device Use

Page 9 of 9

- 8.3 [Information Privacy and Security Incidents, Inquiries, Complaints and Breaches - THR System Policy](#)
- 8.4 [Information Privacy and Security Sanctions - THR System Policy](#)
- 8.5 [Mobile Security, Photography and Secure Text Messaging ITP-14 - THR System Policy](#)
- 8.6 [Password Management - THR System Policy](#)
- 8.7 [Performance Management \(formerly Progressive Corrective Action\) - THR System Policy](#)
- 8.8 [Teleworking - THR System Policy](#)

9.0 Required Statements:

Not Applicable