Policy Name: Acceptable Workstation Use	
Originating Officer (Title), Council, or Committee: Information Security Governance Council	**Effective Date:** 03/15/2016
Approved By: System Leadership Council	**Last Reviewed Date:** 03/15/2016
Page 1 of 8	

1.0 Scope:

1.1 Applicable Entities:
This policy applies to Texas Health Resources and its member entities and excludes the Texas Health joint venture entities.

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.

2.0 Purpose:

2.1 The purpose of this policy is to provide requirements for Acceptable Workstation use.

3.0 Policy Statement(s):

3.1 Workstations are to be used to conduct Texas Health business according to appropriate Texas Health policies and applicable regulations.

3.2 When using a Workstation 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 must only be used by authorized Texas Health Workforce or vendor representatives following the requirements of the Texas Health Electronic Data Access Security Policy.

4.1.2 Mobility 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 To prevent getting phished, Users must not respond to any emails that request personal or financial information. Suspicious emails should be sent to Spam Review, or verified using one of the following methods:

- Calling the Service Desk
- Directly calling the person or institution requesting the information
- Typing the URL directly into a browser

4.1.8 Workstations must be password protected where feasible. This protects PHI 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:

-  +
- 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.

4.2 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 not allowed.

- 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 Mobility 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

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

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

4.3.2 Only Data stored on network drives are backed up and available for restoration in the event of Data loss.

4.3.3 If the User's designated share on a network drive becomes full, the User should contact IS customer service to have the disk space added.

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 Information to unauthorized personnel.

4.4.2 Workstation use 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 devices must be immediately reported to the Service Desk.

4.5 Asset Documentation

4.5.1 Workstations 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 at Texas Health.

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 general 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.
- Laptops and mobility device Users are expected to follow Texas Health policies, best practices, and industry standards to avoid laptop/mobile device theft and/or breach of Texas Health Confidential Information.
- Laptops and mobile devices that store or process Texas Health Confidential Information must be physically protected at all times.
- 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 Ethical 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 the conduct of 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 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 Classification and Category Audit

4.8.1 The Data owner will review the Data classification and category on an annual basis, at a minimum.

4.8.2 The Data owner will implement and review procedures and controls to ensure the handling of the Data is appropriate for the assigned classification.

4.9 Policy Violations and Sanctions

4.9.1 Violations of this policy will be processed according to applicable THR policies, including the THR Progressive Corrective Action Policy, as well as civil and criminal laws.

4.9.2 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, participants of Texas Health benefit plans and programs, customer information, physician credentialing, peer review, quality review, committee records, personnel records, payroll records, salary and compensation information, logon and password information, employee Health Information, and information related to operations and internal business affairs of Texas Health, that is not generally available to the public.

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 Health Information - Any information, whether oral or recorded in any form or medium, that is created or received by a provider, plan, employer, or clearinghouse; and that relates to the past, present, or future health condition of an Individual, as well as the provision of healthcare to the Individual.

5.7 Individual - The subject of Health Information. This includes patients, Group Health Plan participants, and their covered dependents. Legally Authorized Representatives will be accorded the same rights regarding Uses and Disclosures of Health Information as the Individual.

5.8 Individually Identifiable Health Information - Health Information that identifies the Individual or provides a reasonable basis for doing so, by virtue of containing one or more of the eighteen identifiers specified by the Privacy Rule.

5.9 Innovative Technology Solutions (ITS) - A Texas Health department responsible for information technology systems and services.

5.10 Legally Authorized Representative - (1) A parent or legal guardian, if the patient is a Minor; (2) a legal guardian, if the patient has been found by a court to be incapable of managing the patient's personal affairs; (3) an agent of the patient authorized under a Medical Power of Attorney for the purpose of making a health care decision when the patient is incompetent; (4) an attorney ad litem and/or guardian ad litem appointed for the patient by a court; (5) A person authorized to consent to medical treatment on behalf of the patient under Chapter 313 of the Texas Consent to Medical Treatment Act (6) a personal representative or heir of the patient, if the patient is deceased; (7) an attorney retained by the patient or by the patient's legally authorized representative; (8) a person exercising a power granted to the person in the person's capacity as an attorney-in-fact or agent of the patient by a Statutory Durable Power of Attorney that is signed by the patient as principal. (See Texas Health Policy on Health Information Uses and Disclosures for full definition).

5.11 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.

5.12 Shared Workstation - A Workstation that multiple Users routinely share through the course of a business day.

5.13 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.

5.14 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.

5.15 Workstation - Information processing equipment, including microcomputers, Personal Digital Assistants, laptops, and wireless 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 THR 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 HHS.gov (2013, July 26). Summary of the HIPAA Security Rule. Retrieved January 28, 2016, from http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/HIPAA Security

7.4 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

7.5 Mahoney, John. “Best Practices for the Content of IT Policies.” Best Practices for the Content of IT Policies. Gartner, 15 Nov. 2015. Web. 28 Jan. 2016. <https://www.gartner.com/doc/1469122/best-practices-content-it-policies>.

A Gartner account (or fee) is required to Access this article.

7.6 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

7.7 OWASP. (2009, April 14). OWASP Guide Project, Phishing. Retrieved February 4, 2016, from https://www.owasp.org/index.php/Phishing

7.8 Patton, Charles I., Jr., Kenneth R. Knouse, Jr., and Robert D. Malpass. “Defense Inventory Management.” U.S. Government Accountability Office. United States General Accounting Office, 14 Dec. 2015. Web. 28 Jan. 2016. <http://www.gao.gov/assets/230/225080.pdf>.

7.9 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 Computer Virus Management Policy

8.2 Confidentiality Policy

8.3 Electronic Communications Acceptable Use Policy

8.4 Electronic Data Access Security Policy

8.5 Information Privacy and Security Inquiries Complaints and Breaches Policy

8.6 Information Privacy and Security Sanctions Policy

8.7 Mobile Security, Photography and Secure Messaging Policy

8.8 Password Management Policy

8.9 Progressive Corrective Action Policy

8.10 Supply Chain Management Asset Transfer, Disposal and Sale Policy

8.11 Telecommuting Policy

9.0 Required Statements:

Not Applicable