POLICY TITLE:	Workstation and Mobile Device Acceptable Use	POLICY # 3.3	REVIEW DATES	
Topic Area:	INFORMATION MANAGEMENT	ISSUED BY: Chief Executive Officer	9/1/2020	2/9/24
Applies to:	LRE Operations and Staff			
Developed and Maintained by:	CEO and Designee	APPROVED BY: Chief Executive Officer		
Supersedes:	N/A	Effective Date: 10/30/2017	Revised Date: 02/9/24	

I. PURPOSE

To comply with rules stated in the Health Insurance Portability and Accountability Act (HIPAA), as well as to protect the confidentiality and integrity of confidential information as required by law, professional ethics, and accreditation agencies.

II. POLICY

Lakeshore Regional Entity (LRE) shall protect the confidentiality and integrity of Protected Health Information (PHI) as related to workstation use and as required by law, professional ethics, and accreditation requirements. Violation of this or any other LRE policy may result in disciplinary action up to and including termination of employment.

General Expectations

1. LRE provides certain employees access to computer workstations (equipment). Every computer workstation in the agency is vulnerable to environmental threats, such as fire, water damage, power surges and the like.
2. Certain users will be granted access to LRE workstations. Use of electronic resources (equipment) at each workstation is limited by restrictions that apply to all LRE property and by constraints necessary for the reliable operation of electronic communications systems and services. The Information Technology (IT) department reserves the right to deny use of electronic services when necessary to satisfy these restrictions and constraints.
3. The primary function of the equipment is to perform LRE business functions.
4. Any computer workstation in the organization can access confidential customer information if the employee has the proper authorization. Care must be taken by all computer users to ensure they do not jeopardize LRE or customer information.
5. Non-Employees (persons and organizations that are not direct employees but are affiliated through program, contract, license relationships, etc.) may, as authorized by the Chief Information Officer, be eligible to use a LRE workstation or web portal for purposes of collaboration and communication.

6. Each computer will be setup to lock when the computer receives no input from a user for a specified period of time.

User Responsibility

1. Employees may, as authorized by the Chief Information Officer, be eligible to use LRE's electronic resources and services for purposes in this section.
2. All Users must review and sign this policy prior to use of LRE's workstations and electronic resources.
3. All computer users will monitor the workstation's operating environment and immediately report (to the Chief information officer or to the LRE IT Help Desk) potential threats to the computer and/or to the integrity and confidentiality of data contained in the computer system.
4. Personnel using the computer system will not write down their password and place it at or near the equipment or near their work area.
5. Users logging onto the system will ensure that no one observes the entry of their password. Personnel will neither log onto the system using another's account credentials nor permit another to log on with their credentials. Nor will personnel enter data under another person's credentials.
6. Each person using LRE's computers is responsible for the content of any data they input into the computer or transmits through or outside LRE's system. No person may hide their identity as the author of the entry or represent that someone else entered the data or sent the message (unless the activity is performed by an IT Admin in a role required as part of their job responsibilities such as, but limited to, launching fake phishing campaigns for end user testing and training purposes). All personnel will familiarize themselves with and comply with LRE policy 3.4 (Internet Acceptable Use).
7. No employees may access any confidential customer or other information that they do not have a need to know to perform their assigned job duties. No employee may disclose confidential customer or other information unless properly authorized.
8. Employees must not leave printers unattended when they are printing confidential customer or other information. This rule is especially important when two or more computers share a common printer.
9. Employees may not use LRE's system to solicit for outside business ventures, organizational campaigns or political or religious causes. Nor may they enter, transmit or maintain communications of a discriminatory or harassing nature or materials that are obscene or X-rated. No person shall enter, transmit or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language. For more information see LRE policy 3.4 (Internet Acceptable Use).
10. Users must lock or shut down their systems at the end of the day or whenever the user leaves his/her work area and is not keeping a "line of sight" proximity to their

computer/mobile device to ensure the security of the unlocked device.

Acceptable Use

LRE issued computer workstations and mobile devices may be used to access LRE's secure electronic resources under the following conditions:

1. LRE issued Workstations and electronic resources may be provided in support of the agency mission and of the administrative functions that support this mission.
2. Electronic resources shall not be provided to outside individuals or organizations except by approval of the Chief Information Officer. Such services shall support the agency mission.

Personal (non-LRE issued) computer workstations and mobile devices may be used to conduct LRE business ONLY as described here:

1. Messages (whether via text message, email, twitter, etc.) which DO NOT contain secure/confidential information (including but not limited to Protected Health Information (PHI)) may be sent from personal accounts to a contact inside the LRE domain if such communication is needed and supports one of LRE's business operations. Regular use of personal devices to conduct LRE business is strongly discouraged.

Unacceptable Use

LRE issued computer workstations and mobile devices may NOT be used for:

1. Unlawful activities.
2. Downloading or transmission of any communications where the meaning of the message or its transmission could reasonably be construed as being offensive to the recipient or recipients. These would include, but not be limited to, messages that contain profanity, sexually explicit content, race, national origin or gender specific comments, threats, or harassment. Receipt of such information from an unsolicited source will not be cause for sanction.
3. Purposes that violate any applicable laws or regulations or are for personal profit or benefit. These would include, but are not limited to:
    a. Unencrypted transmission of Protected Health Information (PHI) - sending person-served specific PHI over the Internet (web, file transfer, email, etc.) that has not first been encrypted is strictly prohibited.
    b. Improper Release of Information - sending information that is confidential without first having the appropriate authorization
    c. Improper or Unauthorized transmission – sending or transfer of Protected Health Information (PHI) to personal accounts or unapproved file shares outside the secure LRE domain, or to unapproved/unregistered removeable storage devices.
    d. Purposes other than business of the organization, commercial or otherwise
    e. Copyright infringement, plagiarism, forgery, vandalism, and software piracy
    f. Circumventing the Open Meetings Act
    g. Lobbying
    h. Religious or political advocacy

i. Gambling, betting pools
j. Chain letters, Ponzi schemes
k. Use which involves misrepresentation of one's identity to compose, send and/or intercept messages
l. Any other uses that may create liability for the organization or harm its professional image

4. Port scanning or security scanning is expressly prohibited unless this activity is a part of the employee's normal job/duty.
5. No personnel may download or install any software without express permission from the Information Systems team. This rule is necessary to protect against the transmission of computer viruses and other malicious software into LRE's systems.
6. Executing any form of network monitoring which will intercept data not intended for the employee unless this activity is a part of the employee's normal job/duty.
7. Monopolizing computer resources through excessive use shall be expressly prohibited. Such use detracts from the productivity of others. (i.e., streaming video/audio, web TV, etc.)
8. Personal use
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
11. Improper use of thumb/flash drives

Personal (non-LRE issued) computer workstations and mobile devices may NOT be used to connect to LRE's secure electronic resources. This requirement is necessary to protect against the transmission of computer viruses and other malicious software into LRE's systems.

Personal (non-LRE issued) computer workstations and mobile devices may NOT be used to either transmit or store Protected Health Information (PHI) - this prohibition includes associated or augmented storage such as (though not limited to) flash drives, memory chips, and cloud-based file storage areas. This requirement is necessary to ensure that private and confidential data are kept encrypted and secure both during transmission and "at rest", so that HIPAA security protocols will be comprehensive and effective.

It is impossible to outline every example of acceptable or unacceptable use. The LRE IT Department reserves the right to allow for exceptions to the above guidelines on an as-needed basis. Requests for exceptions to any of the guidelines listed in this policy must be submitted in writing (email or memorandum) to the Chief Information Officer, or his/her designee, for approval.

III. APPLICABILITY AND RESPONSIBILITY

This policy applies to LRE Operations and Staff.

IV. MONITORING AND REVIEW

The CEO and designee will review the policy on an annual basis.

V. DEFINITIONS

HIPAA: Health Insurance Portability and Accountability Act
HITECH: Health Information Technology for Economic and Clinical Health

VI. RELATED POLICIES AND PROCEDURES

A. LRE Information Management Policies and Procedures
B. LRE Human Resource Policies and Procedures
C. LRE Compliance Policy and Procedures
D. LRE Compliance Plan

VII. REFERENCES AND LEGAL AUTHORITY

A. Balanced Budget Act 1997
B. HIPAA Act 1996
C. HITECH Act 2009
D. MDHHS Medicaid Specialty Supports and Services Contract

VIII. CHANGE LOG

Date of Change	Description of Change	Responsible Party
12/16/21	Added references, separated policy/procedure	CEO
02/09/24	Language updates, definitions added	CEO