MILLE LACS BAND OF OJIBWE
HEALTH AND HUMAN SERVICES POLICY & PROCEDURE

Department: Administrative Services–Information Technology **Policy Number:** HHS-ADM-IT 3501

Policy Title: Acceptable Use

Attachments: Computer Account Access User Agreement

Revision History: 2021 **Revised by/Date:** Cassie Brown/Holly Hunter 1/2022

Approved by:	**Date:**
Cassie Brown, Director of Clinical Informatics and IT — Cassie Brown, RN	1/24/22
Approved by:	**Date:**
Nicole Anderson, Commissioner HHS	1-28-22

POLICY STATEMENT: Mille Lacs Band of Ojibwe Health and Human Services (MLBO HHS) provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. Users of information assets are required to comply with the acceptable and unacceptable use of electronic devices and network resources, as defined in this policy.

Any violation of this policy may result in immediate disciplinary action, up to and including termination of employment.

PURPOSE: The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources for MLBO HHS in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

SCOPE: All employees, contractors, consultants, temporary and other workers (collectively referred to as "Staff") at MLBO HHS, including all personnel affiliated with third parties with access to MLBO HHS computing systems and equipment must adhere to this policy. This policy applies to information assets owned or leased by MLBO HHS, or to devices that connect to a MLBO HHS network or reside at an MLBO HHS site. This policy and its supporting procedures shall be reviewed and updated annually. Updates may also be made after major regulatory and/or environmental changes.

DEFINITIONS:
Acceptable Use - Acceptable Use requires the user to only access assigned resources and to use these resources in accordance with their duties and responsibilities. Any use without proper assignment, in violation of company policy, or in an unlawful manner is considered inappropriate use and is prohibited.

Bring You Own Device (BYOD). The use of personally owned hardware, such as mobile phones and laptops, for accessing company owned resources.

Protected Health Information (PHI). Any information about health status, provision of health care, or payment of health care that can be associated with a specific individual, and is held by a covered entity.

POLICY:

1. General

a. All employees, contractors, will sign a Computer Account Access User Agreement. Third-party users must also sign attestation that they understand and agree to all rules of behavior set forth by MLBO HHS before access to the information system and its resources is granted.
b. All use of the corporate networks, emails systems, texting and access to the internet will be used for business operations only.
c. The information systems of MLBO HHS will be used in a professional and responsible manner. No abusive, profane, offensive or harassing material shall be accessed, transmitted or stored.
d. The management of MLBO HHS approves the use of all information assets and takes appropriate action when unauthorized activity or a violation of the Acceptable Use Policy occurs.
e. All workforce members shall promptly report the theft, loss or unauthorized disclosure of equipment or information to their supervisor.
f. Workforce members may only install approved software/applications on MLBO HHS owned/leased devices. All other software/applications are prohibited and require a memorandum requesting approval from the Commissioner of HHS.
g. Covered or critical business information will not be left unattended or available for unauthorized individuals to access including on desks, printers, copiers, fax machines, and computer monitors.
h. Workforce members who have access to MLBO HHS Electronic Resources which contain Protected Health Information (PHI) have a responsibility to apply Acceptable Use best practices to protect PHI.
i. Potential PHI security incidents and/or violations should be reported to the Compliance Officer. Examples include sending an email to incorrect email address, unexplained system lockout, inadvertently accessing a malicious Website.
j. MLBO HHS management shall approve the use of all assets hosting confidential data prior to deployment, and following deployment, shall continuously monitor for unauthorized use.
k. Workforce members must cooperate with federal and state investigations or disciplinary proceedings. Should an individual fail to cooperate with investigations, MLBO HHS shall take disciplinary action.

2. Security and Proprietary Information / Protected Health Information

a. All Protected Health Information (PHI) and Personally Identifiable Information (PII), confidential case notes or other confidential information contained on MLBO HHS systems will be classified as confidential. All information that is not clearly classified is assumed confidential.
b. Protected Health Information (PHI), Personally Identifiable Information (PII), or other Confidential Information will be encrypted in transit.
c. Confidential information will be stored on company owned storage systems unless permission from system owners, managers, and MLBO Band Assembly for offsite storage, such as cloud storage.
d. Confidential Information will not be transmitted to personal accounts such as email, texting applications, or virtual cloud storage.

e. If Confidential Information is transmitted to outside entities, it must be for approved business purposes.
f. Confidential Information shall not be stored on personally-owned or controlled virtual "cloud" storage, flash drives, USB devices, CD-ROM or other types of storage media

3. Systems Monitoring and Auditing

a. All information systems at MLBO HHS are the property of MLBO HHS, are subject to monitoring, and review by designated Information Technology or Security Personnel. This shall include but is not limited to email and internet usage or any other electronic process that utilizes MLBO HHS software or equipment.
b. Workforce members shall have no expectation of privacy of usage as MLBO HHS reserves the right to audit networks and systems on a periodic basis to ensure compliance.

4. Password

a. Workforce members shall ensure that their passwords are unique and not guessable.
b. Workforce members shall ensure that passwords are kept confidential and will not give their credentials to other employees, contractors or vendors for use.
c. Group, shared, generic, guest, or anonymous accounts and passwords (e.g., for first-time log-on) are prohibited.
d. Emergency or temporary accounts are allowed only for the minimum necessary time to perform their duties and shall have written preauthorization from department leadership and the Commissioner of HHS, or designee.
e. Changing password/PIN lengths and authentication requirements is prohibited. Circumventing any authentication measures of any host, network or service provided by MLBO HHS is also prohibited.
f. Workforce members are responsible for the security of their passwords and accounts. Workforce members shall not write their passwords on a piece of paper, store them with a software file, or save them for an automated logon.
g. Workforce members shall manually set strong passwords that are in accordance with the Password Policy of MLBO HHS. Workforce members will change passwords every 90 days for regular accounts, 60 days for privileged account, or if the password is believed to be compromised.

5. Internet and Social Media Use

a. MLBO HHS reserves the right to restrict access to any websites that are deemed inappropriate, and shall monitor and audit the use of all communication systems. MLBO HHS may view and disclose any data sent, received, and/or stored without the notice. Reports of employee network and email usage shall be available upon request by company management.
b. Employees are prohibited from disclosing any confidential or proprietary information, trade secrets or any other material that is considered sensitive.
c. Workforce members shall use corporate-approved versions and configurations of browser software.
d. Workforce members are required to obtain approval prior to using external public services, including instant messaging or file sharing.
e. Web content creation or social media activity by workforce members for business related purposes (whether using MLBO HHS property and systems or personal computer systems), is also subject to the terms and restrictions set forth in this policy.

6. **Email Use**
   a. All email accounts that are used on MLBO HHS systems shall be the property of MLBO HHS. All messages created, sent or received using MLBO HHs email system will also be the property of MLBO HHS.
   b. All messages created by a workforce member shall be professional and appropriate for a business environment.
   c. MLBO HHS has the right to monitor any email accounts for legitimate business reasons, including compliance with this policy, employee performance and where there is reasonable suspicion of activities that violate any policy.
   d. Workforce members shall not send unsolicited email messages that would be classified as jokes, "spam" or "junk mail", or advertising material.
   e. Workforce members are prohibited from using any third-party email service. All MLBO HHS business is to be conducted on the email system provided by MLBO HHS.
   f. Any email that is sent shall not contain confidential information to external entities unless one of the following conditions are met; 1) the external domain is an approved domain or 2) an approved encryption method is being used.
   g. Workforce members shall use extreme caution when opening e-mail attachments received from unknown senders, as it may contain malicious code such as viruses or spyware.
   h. All contracted and employed personnel will be assigned an (MLBO HHS) email account for information sharing and access to training and communication platforms.
   i. All personnel are responsible to check emails regularly and utilize email for training and communication platforms.

7. **Mobile Devices**
   a. When using a mobile device to conduct MLBO HHS business the mobile device shall utilize a passcode protected screen lock.
   b. When a mobile device is configured, it shall be configured to operate in a high-risk environment and checked for malware and physical tampering upon return. Workforce members of these mobile devices are prohibited from removing or tampering with any of the security measures in place.
   c. Mobile devices shall not be left unattended unless the device is secure. If the device is secure and unattended it must be locked and/or powered off.
   d. Workforce members shall be responsible for the physical integrity of all devices that are assigned to them. Regular checks of the devices should be performed to ensure the physical integrity of the device and that there is no evidence of tampering.
   e. Circumvention of built-in security controls on mobile devices is strictly prohibited (e.g., jailbreaking or rooting).
   f. Workforce members are required to perform backups of organizational and/or client data on their mobile devices
   g. Mobile devices must be managed in accordance with the Mobile Devices policy.

8. **Company Owned Devices**
   a. Company-provided computer devices must be used for business-related activities.
   b. Devices should not be shared with any unauthorized persons.
   c. Unauthorized software unrelated to the workforce member's responsibilities should not be installed.

9. BYOD

a. With supervisor approval, workforce members may be permitted to use and access company data from their personally-owned personal mobile devices.
b. Workforce members must agree to the Company Bring Your Own Device (BYOD) policy and complete a BYOD consent form.
c. BYODs must abide by the general rules for mobile devices outlined above.

10. Teleworking / Remote Users

a. Workforce members are responsible for providing suitable protections of the teleworking site are to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to the organization's internal systems or misuse of facilities.
b. Remote access is limited only to information resources required by to complete job duties.
c. Telework / remote access employees are only permitted to perform business appropriate work within the restricted MLBO HHS environment. Any restrictions on working hours or access to confidential data are negotiated with the telework employee's manager.
d. Appropriate systems and related office equipment (e.g., locked cabinets and cross-cut shredders, if not already available) will be provided for business use to telework / remote access employees.
e. Copy (including print screen), move, print, and storage of sensitive data is prohibited when accessed remotely without a defined business need.
f. Workforce members must permit MLBO HHS Information Technology Team to install encryption and security software to the mobile device, including their mobile phone, laptop, iPad or computer.
g. Personnel are required to follow the Telework Policy, and have an agreement in place with their supervisor.

11. Inappropriate Use

The following activities are, in general, prohibited. Under no circumstances is an employee of MLBO HHS authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing MLBO HHS-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use:

a. Workforce members must not tamper with, disable, or bypass MLBO HHS security and audit controls such as network connections, user accounts, security logs, security monitoring, software or devices.
b. Workforce members are prohibited from encrypting files on their computers or taking any steps that block access to files, other than the use of MLBO HHS passwords, or approved encryption programs.
c. Workforce members must not change their organization passwords or logon codes without notifying responsible management.
d. MLBO HHS Electronic Resources must not be used to access, create, transmit, print or download material that is derogatory, defamatory, obscene, or offensive, such as slurs, epithets, or anything that may be construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
e. MLBO HHS Electronic Resources must not be used to access, send, receive, or solicit sexually-oriented messages or images.
f. Workforce members must not share confidential or proprietary information about the MLBO HHS and or disclose unauthorized patient/client and employee PII on social networking sites or via unapproved electronic resources.

g. Workforce members shall not download or disseminate copyrighted material that is available on the Internet as this is an infringement of copyright law. Permission to copy the material must be obtained from the publisher. For assistance with copyrighted material, contact Compliance.
h. Without prior approval, software shall not be downloaded from the Internet, as the download could introduce a computer virus onto MLBO HHS's network. In addition, the software may be covered by copyright laws; downloading could be an infringement of copyright law.
i. MLBO HHS Electronic Resources shall not be used to send or participate in chain letters, pyramid schemes, or other illegal schemes.
j. MLBO HHS Electronic Resources should not be used to solicit or proselytize others for commercial purposes, ventures, religious or political causes, outside organizations, chain messages or other non-job-related purposes.
k. MLBO HHS Electronic Resources shall not be used to export software, technical information, encryption software or technology in violation of international or regional exports control laws.
l. MLBO HHS Electronic Resources shall not be used to introduce malicious programs or code into MLBO HHS's computing or networking resources.
m. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or attempting to access a network resource that the employee is not expressly authorized to access.
n. Port scanning or other security scanning. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job/duty.
o. Introducing honeypots, honeynets, or similar technology on the MLBO HHS network shall not be allowed.
p. Workforce members shall not circumventing user authentication or security of any host, network, or account.

Disclaimer: MLBO is recognized as a sovereign nation, and follows Federal laws and regulations. This document is intended as a guideline. Situations may arise in which professional judgment may necessitate actions that differ from the guidelines. Circumstances that justify the variation from the guideline should be brought to your immediate supervisor for clarity.

Non-Compliance: Failure to comply with any part of MLBO HHS's policies, standards, guidelines, and procedures may result in disciplinary actions up to and including termination of employment.

Internal and/or External References	
Compliance - Posting Date	1/28/22 AH
Replaces – Policy Number	
Next Review - Due Date	

Mille Lacs Band of Ojibwe Health and Human Services

Computer Account Access
User Agreement

As an authorized user of Mille Lacs Band of Ojibwe Health and Human Services (MLBOHHS) automated information systems (AISs) and having access to data stored in them, I will be given sufficient access to perform my assigned duties. I will use this access ONLY for its intended purpose and understand the following policies that apply to MLBOHHS data and computer systems:

I agree to safeguard all passwords (e.g. access/verify codes, electronic signature codes) assigned to me and am strictly prohibited from disclosing these codes to anyone, including family, friends, fellow workers, supervisor(s), and subordinates for ANY reason.

I understand that I may be held accountable for all entries/changes made to any government AIS using my passwords.

I am aware of the regulations and facility AIS security policies designated to ensure the confidentiality of all sensitive information. I am aware that the information about clients, patients, or employees is confidential and protected from unauthorized disclosure by law. I understand that my obligation to protect MLBOHHS information does not end with either the termination of my access to this facility's system or with the termination of my government employment.

I will exercise common sense and good judgment in the use of electronic mail. I understand that electronic mail is not inherently confidential and I have no expectation of privacy in using it. I understand that technical or administrative problems may create situations which require viewing of my messages. I also understand that the Commissioner of HHS may authorize access to my electronic mail messages whenever there is a legitimate purpose for such access.

I understand that violation of this agreement constitutes appropriate disciplinary action as defined in MLBO Personnel Policy and Procedure, as well as suspension/termination of access privileges.

I affirm with my signature that I have read, understand, and agree to fulfill the provisions of this User Access Agreement.

Signature_____ Date_____

Printed Name_____ Title_____