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

Department: Administration Services-Information Technology **Policy Number:** HHS-ADM-IT 3502

Policy Title: Access Control

Attachments:

Revision History: new policy **Revised by/Date:** Jan Manary/Abhi Devireddy/Holly Hunter 7/2021

Approved by: Jan Manary **Date:** 7.14.2021
Jan Manary, Executive Director Health Services

Approved by: **Date:**
Nicole Anderson, Commissioner HHS 7-16-2021

POLICY STATEMENT: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions of Mille Lacs Band of Ojibwe Health and Human Services (MLBO HHS). MLBO HHS limits access to only those authorized and maintains the ability to audit such access. User registration and de-registration, at a minimum, will formally address establishing, activating, modifying, reviewing, disabling, and removing accounts, including activities involved in termination and transfer.

This policy applies to all MLBO HHS systems managed internally or hosted by third-party vendors that manage, store, and/or transmit protected health information. 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 define rules and requirements for user access to all MLBO HHS assets.

POLICY:

1. Authorization and Account Activation
   a. All MLBO HHS users shall be subject to an authorization process prior to being granted access to any MLBO HHS workstation, application, or system. The authorization process will include the following:
   b. Prior to gaining access, all MLBO HHS users will sign and acknowledge the Acceptable Use form which outlines in written format all users' responsibilities, rights, and conditions of access.
      - All users will be assigned a defined role. All assigned access will be role-based, include the minimum necessary access, and have a defined account type (individual, administrator, security, system, etc.).
      - The role-based access will be capable of mapping each user to one or more roles, and each role to one or more system functions.
   c. The type and level of access will be based on the user's job function, responsibilities and business needs.

d. Approval will be required of employee supervisors prior to individuals' privileges being assigned to a business role. The authorization and minimum level of access will be checked prior to granting access.
e. If the user's role changes within the organization, access will be evaluated and changed accordingly.
f. Details of user ID, access, authorization, and termination requests will be recorded.
g. Any non-MLBO HHS employees or processes requiring access will be verified by the MLBO HHS Administrators and approved by MLBO HHS leadership prior to establishing access.
h. Every user, both organizational and non-organizational, will have a unique user ID which will provide MLBO HHS the ability to audit all user activities. All users will be uniquely identified and authenticated for both local and remote access to information systems.
i. MLBO HHS Administrators will review all user's IDs prior to creating new access to ensure there are no duplicate users IDs on any MLBO HHS systems.

2. Identification & Authentication
   a. Help desk support will require user identification for any transaction that has information security implications.
   b. MLBO HHS IT staff will verify the identity of every individual prior to establishing new or updated accounts/access to MLBO HHS systems.
   c. User IDs must be individually identifiable (assigned to or owned by only one person).
      - MLBO HHS will not allow generic/group user ID's on the MLBO HHS network.
      - Exceptions may be granted only when specifically authorized by the MLBO HHS Commissioner or designee for business purposes such as training IDs or multiuser clinical workstations.
        - Authorization will only occur when user functions do not need to be traced, and additional accountability controls are implemented.
        - These accounts will be strictly monitored.
        - MLBO account credentials will be modified when users are removed from the group.
   d. Multi-factor authentication methods will be used in accordance with organizational policy.
      - MLBO HHS will implement strong authentication and identification, with two-factor authentication, when MLBO HHS workforce requires remote access to the MLBO HHS network resources.
      - MLBO HHS will require encryption and multi-factor authentication for all remote access to the network connections.
   e. Access to non-public systems must be authenticated. Authentication must be enforced by automated means. Authentication mechanisms must be configured so that they:
      - Validate sign-on information only after all information is entered.
      - Log successful and failed sign-on attempts including date and time of the attempt.
      - Deactivate or lock out the user after five (5) failed sign-on attempts.
      - Reactivate locked users after user notifies IT/helpdesk
      - Encrypt the password during transmission.
   f. When PKI-based authentication is used, the information system will validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; will enforce access to the corresponding private key; will map the identity to the corresponding account of the individual or group; and will implement a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

g. Actions that can be performed without identification and authentication will be permitted by exception.

3. Privileged Access
   a. Administrative access rights will be formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role, and documented for each system product/element.
   b. Elevated privileges will be assigned to a different user ID from those used for normal business use, all users will access privileged services in a single role, and such privileged access will be minimized.
   c. Administrators will use separate accounts when performing administrator activities versus user activities.
   d. Network access for privileged accounts will be secured using replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps.
   e. MLBO HHS will restrict privileged access functions and security related functions and information. This access is explicitly authorized for the MLBO HHS Commissioner or designated administrator.
   f. MLBO HHS will promote the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.

4. Transfers and Termination
   a. MLBO HHS technical staff will notify department leadership to modify accounts when user access requirements change or when a user is terminated.
   b. MLBO HHS department leadership will provide approval for any access changes requested by MLBO HHS users to MLBO HHS IT team.
   c. Users' accounts will be modified:
      - Upon termination of an employee.
      - Upon termination of a contractor, vendor or third-party business relationship with MLBO HHS.
      - When an individual no longer requires access for business purposes.
      - Under any other circumstance deemed necessary by MLBO HHS Commissioner.
   d. Access rights to information assets and facilities will be reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors.
   e. Critical access rights of users who have changed roles or jobs will be removed or reduced as appropriate.
   f. Transferred users' access will be modified within 90 days of the transfer. Both physical and logical access of terminated user will be removed or restricted within 24 hours of notification.

5. Application Access
   a. MLBO HHS will maintain a current listing of all MLBO HHS employees and member organizations that have access to the MLBO HHS systems/applications.
   b. If there is a point person designated for organizations contracted with MLBO HHS, they will coordinate with HHS IT to ensure:
      - Informing all users of their access level to patient health information when using the MLBO HHS systems/ applications.
      - Verifying and attesting to the identity of all End Users who have systems/applications access every 90 days.
      - Notifying MLBO HHS when their End User's access rights change.

c. Each End User will need their unique user account. MLBO HHS has only one level of systems/application access.
d. When a User account is created, the End User will have 90 days to login to the account for the first time with their unique Username and Temporary Password. Upon logging in for the first time, End Users must create a new password of their choosing. It must contain all items required by the MLBO HHS Password Policy.
e. When a user is logged into MLBO HHS systems/applications, if there is no activity in the session for 15 minutes, the session will automatically timeout. The End User will need to log back in to continue.
f. MLBO HHS will require each member organizations point of contact to verify the identity of each user prior to having access created.
g. The point of contact will notify MLBO HHS of any changes to their organization's Active User List.

6. Audit
   a. MLBO HHS will remove all default system accounts prior to any system going into full production.
   b. MLBO HHS technical staff will review all access logs bi-weekly to ensure all expired, disabled or unnecessary accounts are removed from the system, made inactive, or reduced to the lowest level of access required.
      - All users with access to PHI will be reviewed and the appropriateness of the user's role will be examined.
      - Any discrepancies will be immediately remediated following the review.
      - Inactive accounts will be automatically removed or disabled.
   c. MLBO HHS will deactivate remote access of vendors and business partners when not in use.

7. Segregation of Duties
   a. Segregation of duties must:
      - Be designed to prevent malicious activity without collusion.
      - Define information system access authorization to support segregation of duties.

8. Session Time-out
   a. A time-out system will pause the session screen after 15 minutes of inactivity and will close network sessions after 30 minutes of inactivity.
   b. Users will be required to reestablish authenticated access once the session has been paused or closed.
   c. If the system cannot be modified, a limited form of time-out that clears the screen but does not close the application or network session will be used.
   d. As defined in the MLBO HHS Mobile Security Policy, MLBO HHS will require all bring your own devices (BYOD) and MLBO HHS issued devices have a configured lockout screen enforced through endpoint technical controls.

9. Critical Information Access Controls
   a. 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.
   b. MLBO HHS will, to the best of the organization's ability, protect any critical information being sent via internal or external mail services, including the USPS.
   c. In accordance with MLBO HHS Physical Security Controls Policy, MLBO HHS will physically secure network equipment to prevent unauthorized access.

d. Covered information will be encrypted when stored in non-secure areas and, if not encrypted at rest, the MLBO HHS will document its rationale.
e. The MLBO HHS IT team will authenticate users and devices prior to approving access to the MLBO HHS wireless network or allowing remote access from public networks to where sensitive data is maintained.
f. When accessed remotely, users shall not copy, move, store or print critical data without a previously approved business need.
g. MLBO HHS access control systems and MLBO HHS contractor systems and components will have a default setting of "deny all".
h. Access rights from an application to other applications will be controlled.
i. Access rights to applications and application functions will be limited to the minimum necessary using menus.
j. Outputs from application systems handling covered information will be limited to the minimum necessary and sent only to authorized terminals/locations.

10. Electronic Signatures
    a. MLBO HHS will utilize electronic signatures when deemed appropriate. Each electronic signature will be unique to one individual and not shared. Electronic signatures can never be re-assigned.
    b. MLBO HHS may verify the identity of the requesting party prior to establishing, assigning, or certifying the electronic signature.
    c. Electronic signatures based upon biometrics will be designed to ensure that they cannot be used by any individual other than their genuine owners.
    d. Electronic signatures and handwritten signatures executed to electronic records will be linked to their respective electronic records.
    e. Signed electronic records shall contain information associated with the signing in human-readable format.

11. Information Sharing
    a. MLBO HHS will facilitate information sharing by enabling authorized users to determine a business partner's access when discretion is allowed as defined by the organization and by employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.

12. Exceptions
    a. Any exception to these access control policies will require the approval of the MLBO HHS Commissioner or designee with a documented business justification for the exception.

PROCEDURE:

1. Authorization and Account Activation
   a. Organizational Users:
      - Background checks are performed by the MLBO Human Resources as part of the hiring process.
      - MLBO Human Resources notifies the department leadership via email of the new hire's start date and job role.
      - The department leadership or designee sends the new employee the Acceptable Use Policy (AUP) as part of the onboarding information package.

- After receiving the executed AUP from the new employee, department leadership or designee submits a new user request ticket to the MLBO HHS IT support (Network Access form). The request should include the following information:
    - The signed AUP or attestation form
    - The job role and function
    - The systems to which the user needs access
    - The requested account types
- The department leadership is responsible for reviewing the access request and confirming that the privilege levels, account types and roles are appropriate based on the new user's job. All privileged accounts must be explicitly signed off on.
- The MLBO HHS IT team will then provision the user's account in Active Directory and the systems /applications pertinent to the employee job description.
- The MLBO HHS IT team assigns accounts in Active Directory the roles of MLBO HHS User, Administrator, Contractor User or System.
    - They will assign the security groups and file access based on the job role.
    - User IDs will be assigned according to the formula: "Firstname.lastname."
    - Privileged User IDs will be assigned according to the formula: "lastname_ADMIN."
    - Accounts in systems/applications are assigned to either the ADMIN User role with full access to the system or the User role with more limited functionality.
- Account managers are provisioned with Delegated User accounts while the IT TEAM is given Cache User accounts.
    - User IDs will be assigned according to the formula "first initial last name" to ensure that they are unique.
- During onboarding, the MLBO HHS IT team will distribute temporary account passwords to the new employees either verbally or through secure email according to the process established in the Password Policy. If the user was determined to require a privileged account, they will be trained by the MLBO HHS Compliance Officer and Informatics Director on when to use the privileged vs the non-privileged accounts.

b. Non-Organizational Users

- The process for establishing non-organizational user accounts will be the same as the process for establishing organizational accounts.
- Non-organizational accounts created must include a specific end date in use or the vendor/business partner must notify the MLBO HHS IT staff once remote access is no longer needed.
    - When possible, the account will be configured by the IT team to time out once the end date is reached.
    - If an extension is required, a request must be sent to the MLBO HHS IT staff for approval with a new end date. If approved, the IT team reconfigures the account with the new end date.
    - MLBO HHS IT team when no longer needed, the MLBO HHS Informatics Director will verify that the account has been deactivated and will deactivate the account manually if necessary.

c. Other Types of Accounts as needed:

- The MLBO HHS Informatics Director or designated administrator, will establish access only after the member contracting process has been completed.
- The MLBO HHS IT team provisions access within systems and applications based on role and group membership.

- Initial passwords will be distributed in accordance with the process established in the Password Policy.

d. Secure File Transfer Protocol (SFTP)

- SFTP is used for PHI data transfers.
- The IT Informatics Director and Health Information Management Coordinator will approve all SFTP use between MLBO HHS and a Third-Party after ensuring that all legal and contractual requirements are met.
- When large amounts of PHI need to be transferred, a request will be sent to the Health Information Management Coordinator, who will set up the SFTP servers.
    - When configuring these accounts, the Health Information Management Coordinator will utilize a random password generator to ensure that passwords are unique and not guessable.
    - Passwords will then be distributed to the user in encrypted email and sent only to the email account associated with the user.

2. Shared Accounts

a. Shared or group accounts are prohibited by MLBO HHS unless an exception has been made.

b. If there is a need for a shared, guest, emergency or temporary account, the user will request the creation of an account through the exceptions process which is submitted to the MLBO HHS IT team and the MLBO HHS Compliance Officer.

- The request must contain the business justification, duration that the account is needed, and the system access required.
- The request will be reviewed and approved or denied by the stakeholders including the application owner, Compliance Officer on behalf of the Security Risk Team.
- The MLBO HHS Security Risk Team will be responsible for monitoring the use of all accounts.
- Once the account reaches the end of the proposed duration period, the Compliance Officer, Informatics Director and the Security Risk team will either re-approve the account or de-activate the account.
- If membership to the group changes, the MLBO HHS IT team is notified and will initiate a password change. This password will then be distributed to the other group members according to the process established in the Password Policy.

3. User Lists

a. Asset Owner List

- The Informatics Director will be responsible for creating a current list of all owners of information assets. This list will take the form of a spreadsheet stored in on the T-Drive and accessible by the IT team. The list will be updated annually or as needed when assets are assigned or re-assigned. The list will include:
    - The name of the asset
    - The name of the asset owner
    - Date the asset was assigned
    - IP address
    - Operating System

b. Access List Documentation

- The MLBO HHS Informatics Director will be responsible for creating a current list of all users authorized to access PHI.
- This list will take the form of a spreadsheet stored in the T-drive and accessible by the IT team. The list will include:

- The account username
- The name of the user's connected to the account
- The worker type (contractor, third-party, employee)
- The account type (admin, user, shared, temporary etc.)
- The names of the system
- PHI/ No PHI access

c. Access List Review

- The Informatics Director will review the list every 90 days to ensure that it is up to date and the access rights are appropriate.
- After any employment, changes (change in privilege level, change of role, termination) or system the Security Risk team will review the access list to ensure that all accounts are set to the appropriate access level. If the Security Risk team determines that access rights need to be reallocated, they will submit a request to IT team.

d. Updates

- If new accounts are made or if existing accounts are modified or removed, MLBO HHS department leadership will reach out to the Informatics Director via email and let them know that the access list needs to be changed.

4. Privileged Access

a. Only the MLBO HHS Informatics Director or designated administrator are authorized to have access to specific security relevant functions deployed and security-relevant information such as:

- Hardware (Firewalls, Physical Equipment)
- Software (IPS/IDS, A/V, SIEM or other security tools)
- Firmware (Operating Systems of security tools or underlying infrastructure)

b. If additional privileged access is needed outside of the initial account set up, a request must be sent to the Informatics Director and the Security Risk team for authorization.
c. This request should include the business justification for the privilege level.
d. Once approved, the MLBO HHS IT team will be notified to create the account.
e. When a privileged account is created, the Compliance Officer will advise the user to only use the privileged account when necessary. Normal business functions should be done using the non-privileged account.

5. Modification of Access

a. If the role is the same but the access rights have changed, the department leadership is responsible for and sending a Network Access form to the IT team notifying of the change.
b. If the role is changing, the same process is followed as initial credentialing, although additional training may be required in accordance with the Training Policy.
c. The department leadership approves and sends it to the IT team who will configure the account.

6. Termination

a. For any termination initiated by the receipt of a letter/email announcing an employee's resignation:
b. The MLBO HHS department leadership will notify the IT team to begin the termination process. The Informatics Director will deactivate all accounts on the individual's last day.

c. For high-risk terminations, termination is effective immediately and the Informatics Director will remove access immediately.
d. During off boarding the MLBO HHS department leadership will fill out appropriate termination paperwork, including the Network Access form (requesting deactivation).
   - As part of this process, the MLBO HHS department leadership will collect all physical access items (keys, keycards, badges, employee IDs), and notify the IT team to remove the employee from the physical access list.

The MLBO HHS department leadership will maintain evidence of the completion of off boarding.

7. Equipment Deployment

a. The MLBO HHS will follow the Change Management Policy when issuing new equipment.
b. The MLBO HHS Informatics Director or designee will obtain equipment from storage or procure new equipment.
c. The MLBO HHS Informatics Director or designee will remove all default and system accounts. If system or default account cannot be removed, they will:
   a. Change the default password of the account.
   b. Rename the account.
   c. Remove the access rights of the account.
d. After creating a user id and provisioning equipment, the Informatics Director will notify the application owner as appropriate
e. If device has been re-purposed it will be fully sanitized ahead of time.

8. System Access

a. All access to the MLBO HHS network is configured using the same methodologies. This includes access from within the MLBO HHS offices and from remote locations.
b. To request remote access, the employee's department leadership or designee should complete an access request form. The request should include the business justification for remote access.
   - Once the employee is approved for remote access, the request should be forwarded to the IT team.
   - The Informatics director or designee will configure access using the following guidelines:
     - Multi-factor authentication will be used for any users provisioned with remote access and for all MLBO HHS accounts. The Informatics Director will work directly with the user onsite to establish the multi-factor authentication. The preferred method is to utilize the user's mobile phone to send a one-time password which is replay resistant.
     - Multi-Factor authentication will only be installed for a user while the user is on-site.
   - Remote access through an SSL VPN is to be configured with the following:
     - IKE Algorithm AES 256
     - IKE Authentication Algorithm SHA2 256
   - The MLBO HHS Informatics Director will establish the initial SSL VPN connection for the user on their device. SSL VPN set-up instructions will also be provided to the employee.
     - Split Tunneling is to be disabled for all VPN access.
   - The Informatics Director will configure endpoints to prevent the use of USBs.
   - Where possible, technical controls such as Group Policy Objects or controls should be implemented to prevent copying, moving, printing, or storing sensitive data when accessed remotely.
   - The MLBO HHS Informatics Director ensures that when PKI-based authentication is used:
     - The information system validates certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information;
     - Enforces access to the corresponding private key;

- Maps the identity to the corresponding account of the individual or group; and implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

9. Authentication Procedures
   a. The firewall settings will be configured through the network/host-based access rules with a default deny all setting by designated personnel.
   b. The designated personnel is responsible for initially configuring systems to ensure that:
      - Role-based access is used to control access to system components storing, processing or transmitting covered information for all systems and applications.
      - No action can be performed without identification and authentication.
      - Access rights from application to application are restricted based on role.
      - Outputs are limited to the minimum necessary and sent only to authorized terminals.
   c. The Informatics Director or designee conducts periodic audits of all systems to:
      - Remove/disable inactive accounts.
      - Ensure that the role-based access is configured correctly.

10. Time-Out Settings
    a. The Informatics Director or designee will implement the following timeouts for different systems.
       - Workstations (Windows) - All workstations are configured with a 15-minute timeout out which will require a password to unlock. A Group Policy Object or similar technical control will configure the timeout policy.
       - Mobile Devices - All personnel devices (BYOD) or MLBO HHS owned mobile devices will be configured with a screen lock after 15 minutes which is enforced through device settings.
       - Servers - All remote desktop remote sessions will disconnect after an idle timeout after 30 minutes enforced by Group Policy Object or other technical control.

11. Software Development Procedures
    a. Developers should control functionality by utilizing role-based access which limits menu options.
    b. Developers will prevent the need of elevated access privileges to execute the normal functioning of internally-developed applications.
    c.. When acquiring off-the-shelf programs to be used as part of a MLBO HHS solution, the designated personnel will perform a thorough evaluation of the software's security. The investigation will include whether the application will require elevated access privileges to run.

12. Information Sharing Procedures
    a. When information residing on the MLBO HHS system needs to be shared with a business partner, the appropriate business owner must provide approval.
       - Requestor submits an email to the business owner outlining the information to be shared and the Business Partner receiving the information.
       - Once the business owner approves the request, the IT TEAM is notified to share the information.

13. Clean Desk
    a. Workers are trained on the clean desk requirements as part of onboarding as described in the MLBO HHS Education Policy.
    b. The Compliance Officer or designee will perform periodic, random walkthroughs regularly to verify users are adhering to the Clean Desk Policy as outlined in the Acceptable Use Policy. Goals for the walkthrough is to test locked cabinets/drawers and check desks, printers, shredders and trash

cans to verify that no sensitive information or passwords are visible or stored in an unsecure location.

c. If violations are discovered, it will be noted and a follow up meeting will be scheduled to discuss the clean desk violation. Depending on the severity or frequency of violations, re-training or other disciplinary actions in accordance with the sanctions policy may take place.

14. MAIL/ SHIPPING

Prior to shipment of devices, the Informatics Director of designee will ensure that devices are wiped or encrypted as appropriate.

15. Network

a. All servers are securely hosted by contracted vendors that provide assurance equipment is maintained through contracts and ongoing relationships. All other network equipment is stored securely in a locked room.

b. The onsite IT team will provide access to the network closet to roles requiring physical access to the network equipment. More information is available in the MLBO HHS Physical Environmental Security Policy.

c. Covered information is always encrypted, in accordance with the Data Classification Policy.

d. MLBO HHS prohibits use of dial-up technologies for all network connectivity.

16. Wireless Configuration

a. MLBO HHS will implement protections for the wireless access systems which have access to any covered information.

16. Help Desk Support

a. If help desk support is required, the identity of the individual must be verified.

- Account configurations will follow the procedures laid out in the Password Policy.
- For all other transactions, identity verification will be done through the use of passwords, security codes sent to email accounts or answering security questions.

Internal and/or External References	
Compliance - Posting Date	7/16/2021 HH
Replaces – Policy Number	
Next Review - Due Date	7/2024