

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

Department: Administration Services-Information Technology **Policy Number:** HHS-ADM-IT 3508

Policy Title: Password Policy

Attachments:

Revision History: 3/2013

Revised by/Date: Jan Manary/Abhi Devireddy/Holly Hunter 7/2021

Approved by: 
Jan Manary, Executive Director, Health Services

Date: 8.19.2021

Approved by: 
Nicole Anderson, Commissioner HHS

Date: 8-27-2021

POLICY STATEMENT: Passwords are one of the most important aspects of computer security. Missing or weak passwords may result in unauthorized access and/or exploitation of Mille Lacs Band of Ojibwe Health and Human Services (MLBO HHS) resources. This policy mandates the creation of strong passwords, the protection of those passwords, and the frequency of password change. All users, including contractors and vendors with access to MLBO HHS systems, are responsible for taking the appropriate steps to select and secure their passwords.

This policy applies to both the MLBO HHS network and all MLBO HHS applications. All MLBO HHS employees, and contracted resources are required to adhere to all elements of this policy. Any application or software that is acquired by MLBO HHS will be required to adhere to this policy as closely as possible. Updates may be made after major regulatory and/or environmental changes.

The Commissioner of HHS or designee must approve any exception to the policy in advance. 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, and may impact services or relationship contracted with a business associate, vendor or partner.

PURPOSE: The purpose of this Policy is to ensure that proper controls exist for the management of MLBO HHS secure authentication.

DEFINITIONS:

- **Bring You Own Device (BYOD):** The use of personally owned hardware, such as mobile phones and laptops, for accessing company owned resources.
- **Personal Identification Number (PIN):** Is a secure alphanumeric or numeric code used for authenticated access to a system. A PIN serves as a validation tool for users of various types of networks and systems, such as computer networks, credit/debit cards, and mobile phones.
- **Electronic Signature:** Computer data complication of any symbol or series of symbols executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's hand-written signature.

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

POLICY:

- **Administrative Safeguards:**
 - Users shall be made aware of password requirements.
 - Users shall sign the Computer Account Access User Agreement acknowledging their responsibility to keep all passwords confidential.
 - Passwords shall not be included in automated log-on processes.
 - Users will acknowledge receipt of passwords.
 - Third party or unprotected email messages shall not be used for the distribution of passwords.
- **Administrative Safeguards Process:**
 - When distributing a password to a user, it shall be delivered in person, through a protected channel or over the phone; verification of user identity will be done. Passwords will never be distributed via plain text/unprotected email.
 - For new employees, the Informatics Director or designee hand delivers the employee's temporary password in a paper format. The new employee is then required to log in with the temporary password in the presence of the Informatics Director or designee, thus indicating receipt of the password. If the employee is not able to login with the temporary password and select a permanent password at the time of delivery, the password is not supplied at that time.
 - All users at MLBO HHS are required to receive security training as part of their onboarding process.
 - ❖ This security training will include all password requirements of MLBO HHS as well as best practices. Best practices include not using automated log-on processes to include passwords, password complexity best practices, etc.
 - ❖ Training must be completed on the employee start date and are required to sign an attestation of agreement with policies and training.
- **Technical Safeguards:**
 - Quality passwords shall be used which contain at least eight (8) characters and meet three of the following four complexity requirements:
 - ❖ lower case characters
 - ❖ upper case characters
 - ❖ numbers
 - ❖ special characters/symbols
 - Passwords will be masked when being entered.
 - Passwords will be encrypted during transmission and at rest through the following controls:
 - ❖ Passwords shall only be transmitted when cryptographically-protected.
 - ❖ Passwords shall only be stored using an approved hash algorithm.
- **Technical Safeguards Process:**
 - MLBO HHS will utilize an automated system for its identity and password management solution to integrate with most systems/applications used by MLBO HHS.
 - The Informatics Director or designee will be responsible for configuring the passwords for new users and at the time of password resets as to not include them in automated log-on processes via automated options.

 - The Informatics Director or designee is responsible to ensure that passwords are configured to meet the complexity requirements.
 - For any system or application that does not integrate with the automated tools the Informatics Director or designee is responsible for ensuring that the system or application can meet the technical safeguards.
 - If the safeguards are not inherent in the system/application designated personnel and/or contract vendor will be responsible to add controls or third-party add-ons to meet these requirements.
- **Password Changes/Resets**
 - Passwords shall be changed:

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


- ❖ For default system accounts;
- ❖ At first login following the issuance of a temporary password;
- ❖ When it is believed the account has been compromised;
- ❖ Every 90 days for standard accounts and every 60 days for administrator accounts.
- Passwords that are changed shall differ from the last six passwords and will differ by at least one character.
- User identities will be verified prior to the password being reset.
- All temporary passwords shall be unique and not guessable
- **Password Change/Resets Process:**
 - The Informatics Director or designee will configure automated account passwords:
 - ❖ To expire after 90 days for standard Users and 60 days for administrator/privileged accounts
 - ❖ Differ from the previous six passwords and differ by 1 character.
 - Users can reset their passwords using the self-service feature in windows, or by using the password reset URL.
 - The password reset URL will ask security challenge questions to verify the user’s identity.
 - In the event a user cannot change their password using the self-service features, the Help Desk will assist. The Help Desk will verify a user’s identity by asking questions based on the security profile set up by the user, prior to resetting the user’s password.
 - Once the user has been verified the Informatics Director or designee will use the approved random password generator.
 - When resetting the password, the Informatics Director or designee will also configure the password to be changed upon the first logon using the temporary password.

Mobile Devices:

- Password policies for mobile devices will be documented and enforced through technical controls on all company devices (including devices approved for BYOD usage).
- MLBO HHS shall prohibit the changing of password/PIN lengths and authentication requirements for all mobile devices.

Mobile Devices Process:

- The Informatics Director will configure a 6-character length password/PIN for all mobile devices, and lock these options on the device so that a user cannot change these requirements.

Internal and/or External References	
Compliance - Posting Date	8/27/2024 
Replaces – Policy Number	HHS-ADM-IT 3504 Password Requirements
Next Review - Due Date	