

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

Department: Administration Services-Information Technology **Policy Number:** HHS-ADM-IT 3505


Policy Title: Configuration Policy

Attachments:

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

Approved by: 
Jan Manary, Executive Director, HHS Health Services

Date: 7.14.2021

Approved by: 
Nicole Anderson, Commissioner HHS

Date:
7-17-2021

POLICY STATEMENT: Mille Lacs Band of Ojibwe Health and Human Services (MLBO HHS) is committed to utilizing information systems designed and configured using controls sufficient to safeguard data. Failure to protect systems against threats can result in the loss of data integrity, unavailability of data, and/or unauthorized use of data or other MLBO HHS assets.

PURPOSE: This policy is in place to support and ensure Mille Lacs Band assets are configured to industry standards and have safeguards from threats or breach in place.

SCOPE: This policy applies to all MLBO HHS employees, contracted resources, and vendor partners. All employees and contracted resources are required to read and adhere to all elements of this policy. MLBO HHS Commissioner and department leaders will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) is suspected, the company may report such activities to the applicable authorities.

POLICY:

Baseline Configurations:

- MLBO HHS will maintain information systems according to current baseline configurations, configures system security parameters, and implements supporting technical controls such as antivirus, file integrity monitoring, host-based firewalls or port-filtering tools, and logging as a part of this baseline to prevent misuse.
- MLBO HHS will not utilize automated updates on critical systems.

Security Audit:

- Annual compliance reviews, including checks on technical security configuration of systems, shall be conducted by security or audit individuals using manual or automated tools; if non-compliance is found, appropriate action is taken.
- Automated compliance tools are used when possible

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

- The result and recommendations of compliance reviews shall be documented and approved by the Commissioner of HHS, or designee.
- Technical compliance checks are used to help support technical interoperability.

Technical Security:

- MLBO HHS shall ensure vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application.
- MLBO HHS configuration control program shall maintain control of all implemented software and its system documentation and archive prior versions of implemented software and associated system documentation.
- Where development is outsourced, change control procedures to address security are included in the contract(s) and specifically require the developer to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.
- MLBO HHS has developed a continuous monitoring strategy and implemented a continuous monitoring program.
- Operational systems only hold approved programs or executable code.

Technical Controls:

- MLBO HHS shall identify unauthorized (blacklisted) software on its information systems, including servers, workstations and laptops, employ an allow-all, deny-by-exception policy to prohibit the execution of blacklisted software, and reviews and updates the list of blacklisted software at minimum of annually. MLBO HHS must prevent program execution according to the blacklist of software and rules authorizing the terms and conditions of software use.
- Physical or logical access is only given to suppliers for support purposes when necessary, with appropriate approval and such access is monitored.
- MLBO HHS employs assessors or assessment teams with a level of independence appropriate to its continuous monitoring strategy to monitor the security controls in the information system on an ongoing basis.

Asset Management:

- If the developer, vendor, or manufacturer no longer supports systems or system components in production, MLBO HHS shall show evidence of a formal migration plan approved by management to replace the system.

Creation of Baseline Configurations:

- Baseline configurations for all systems are established utilizing industry best practices for secure configurations.
- All baseline configurations must contain the following controls:
 - Anti-virus software
 - Logs sent to a centralized logging server
 - Restriction on automatic updates
 - Update and Patch validation
 - Restriction of application execution
 - File-integrity monitoring
 - Alerts for changes to the environment

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

- Implementation of Baseline Configurations
 - All systems within MLBO HHS will be configured in accordance with the developed baseline by the System Administrator
 - Systems that are maintained by a third-party vendor will configure systems in accordance with their developed baselines.
 - Exception to these baselines will follow the process outlined in the “Maintenance of Baseline Configuration” subsection.
 - System administrators must verify that any newly installed system’s logs are sent to the centralized logging server.

- Maintenance of Baseline Configurations
 - Any exceptions to configuration baseline must go through the MLHS HHS Change Management Process.
 - After baseline configurations are established, the System Administrator will configure all systems using this configuration.
 - Annually the designated personnel or contracted services will review and update baseline configurations. As part of this task, the prior versions of implemented software and associated documentation will be archive prior to production implementation.

- Implementation of Approved Upgrades
 - Only authorized administrators will implement approved upgrades to baseline software, applications, or system libraries.
 - All changes, including those to information systems, networks, and network services need to be tracked and approved following the MLBO HHS Change Management process prior to implementation. As part of the implementation, the administrator will archive the current settings or software, prior to updating any system.

Security Audit:

- Compliance Review
 - The MLBO HHS Security Risk team will initiate a yearly compliance review by assigning the task to the designated personnel or contract services.
 - All security policies and processes are in the scope of review and are evaluated for effectiveness and non-compliance.
 - If non-compliance is found, the HHS Compliance Officer will initiate an investigation.
 - Results and recommendations are documented, the Compliance Officer and designated team will provide an updated briefing to the Commissioner of HHS and personnel Commissioner invites into the process, analysis, remediation, and implementation of corrections.

- Technical Security Reviews
 - Annually the HHS Security Risk team is responsible for ensuring a technical security review is conducted.
 - The HHS Security Risk team will determine if the review shall be conducted internally or by a qualified third-party vendor.
 - If third-party assessors are chosen:
 - ❖ The third-party must be vetted by the Compliance Officer and approved by the Commissioner of HHS, or designee.
 - ❖ The third-party must execute a Business Associate Agreement (BAA) with MLBO HHS.

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

- Identify the scope of the review and the following must be covered:
 - ❖ Information system will be scanned for compliance with baseline configurations.
 - ❖ Baselines will be reviewed for vulnerabilities.
- Upon completion of the review, all findings will be documented in a report to be reviewed by the Commissioner of HHS and designated personnel.
 - ❖ Non-compliance and gaps will be addressed.
 - ❖ A corrective action plan is created for non-compliance/gap and submitted to the Commissioner of HHS for approval.
 - ❖ Once remediation is completed, including testing, the report is updated/amended to show completion and the update is sent to the Commissioner of HHS.
- Security Review of Application Changes
 - ❖ Designated personnel or selected vendor will ensure that all application changes to any MLBO HHS environments are reviewed, tested, and checked prior to production implementation so they do not compromise the security of the system nor the operating environment.
- **Technical Controls:**
 - Third-Party Access
 - ❖ Suppliers will only be given access with Commissioner of HHS approval.
 - ❖ Physical access to facilities for all suppliers will be monitored in accordance with the MLBO HHS *Physical Environmental Security Policy*.
 - ❖ Remote access monitored.
 - ❖ A signed agreement must be on file before remote access is granted.
 - Application Execution
 - ❖ All devices shall have deny-all for non-approved applications.
 - ❖ Using manual or automated tools, designated personnel will create and maintain a list of approved applications and software that are authorized to execute in the MLBO HHS environments.
 - ❖ User accounts will be restricted from installing applications that are not on the approved applications list.
 - ❖ Exceptions for not approved applications must go through the exception process utilizing the MLBO HHS *Exception Policy*.
 - Installation of approved applications not installed with the baseline must follow these steps.
 - ❖ Send request to identified personnel to have application added to device
 - ❖ Designated personnel verifies application is authorized; if so approval given and the application is installed.
 - ❖ Use of the application does not change user access level regarding PHI.
 - Identification and Monitoring of Authorized Software
 - ❖ Designated personnel/ contract service vendor will utilize manual or automated tools, such as installation checklists and vulnerability scans to validate the configurations of the MLBO HHS systems, including servers and endpoint devices for unauthorized software.

Asset Management:

- If a system or system component in production becomes unsupported by developer, vendor, or manufacturer, then designated personnel will utilize the Change Management program to phase out systems/applications.
 - ❖ Phase out process will include leveraging project management principles to ensure successful migration of systems/applications to supported systems.

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

Internal and/or External References	
Compliance - Posting Date	7/17/2021 18
Replaces – Policy Number	
Next Review - Due Date	7/2024