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

Department: Administration Services-Information Technology **Policy Number:** HHS-ADM-IT 3503

Policy Title: Auditing-Logging-Monitoring of IT Systems

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: It is the policy of Mille Lacs Band of Ojibwe Health and Human Services (MLBO HHS) to mandate audit standards and security log management for systems that manage MLBO HHS information resources. Furthermore, this policy establishes the requirements surrounding the collection, maintenance, and review of audit logs for MLBO HHS's information system and network resources. While the prevention of incidents such as intrusions and breaches is ideal, detection is critical, as is the implementation of an effective information security auditing and monitoring policy. Logging from critical systems, applications and services provides MLBO HHS with key information and potential indicators of compromise. Event tracking and monitoring are essential elements of our program because they enable us to enforce the policies and processes that comprise the program.

PURPOSE: This policy will ensure that information security events be monitored and recorded to detect unauthorized activities in compliance with all relevant legal requirements

SCOPE: This policy shall apply to MLBO HHS's Information Technology environment and to MLBO HHS employees and third-party contractors who operate computer systems on the corporate network. "Audit logs" or "logs" shall include network access logs, system logs, authentications logs, operating system logs, or any other data which correlate an activity with a user and a time.

POLICY:

1. Log Requirements
   a. Audit logs shall include the details necessary to perform a proper evaluation of the event.
   b. Audit logs shall be generated for events triggered by both standard and administrative (privileged) users.
   c. Logs generated for an event will include the following components (at a minimum and as applicable).
      - User ID or a unique user identifier
      - Function performed by the user (e.g. log-in, record creation, access, update, etc.)
      - Origin of the event
      - Date and time of the event
      - Event details

- Success or failure of event

d. Log Retention/Availability
   - Audit records will be backed up not less than weekly onto a different system or media than the system from which it originated.
   - Audit records will be retained for ninety (90) days and shall be immediately available for analysis.
   - Older records will be archived for one (1) year to provide support for after-the-fact investigations of incidents and/or to meet regulatory requirements.

e. Log Integrity
   - A technical solution (e.g., Network Time Protocol) will be implemented to ensure the integrity of time and date data to ensure that tracked and monitored events on all platforms, applications, and other systems are associated with an accurate chronology.

f. Access Requirements
   - Audit logs will be secured from unauthorized use/modification by access control mechanisms or other means of segregation.
   - Separation of duties will be used whenever possible to limit the risk of unauthorized or unintentional modification of information and systems.

g. Monitoring
   - MLBO HHS reserves the right to record, monitor, and audit the event logs of all systems and applications, especially those systems/applications designated as 'High' security sensitivity.
   - MLBO HHS shall inform all employees and contractors that their actions are subject to monitoring. Consent to said monitoring shall be gathered before the employee or vendor is granted access to MLBO HHS systems/applications.
   - Logs generated by both standard and administrator accounts shall be reviewed on a regular basis.
   - Audit trails/logs shall be reviewed regularly from those devices or components that handle Highly Confidential information and from those components that perform security functions (e.g., firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, etc.).
   - MLBO HHS shall monitor systems/applications to identify irregularities or anomalies that are indicators of malfunctions or failures.
   - Implemented auditing solutions shall be configured to display logs using filters and/or reports.
   - Routine and ad-hoc log analysis may be used for identifying inappropriate or unauthorized access as part of performing audits, forensic analysis, supporting internal investigations, establishing baselines, and to comply with Federal regulatory requirements.
   - MLBO HHS shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include authorized and unauthorized access.

h. Alerting will be required for those systems/applications designated as 'High' security sensitivity. Alerting will provide a method to notify systems or appropriate personnel of any event that requires follow-up or corrective action.

2. PROCEDURE

a. Log Requirements - Business owners and system admins should ensure that all logs are capturing the required level of detail outlined above.
b. Log Retention/Availability - In accordance with the policy requirements, auditing solution will be configured by the system administrator to exist indefinitely
c. Log Integrity – when server installation is configured an automated hardening playbook which installs and configures the *Server Hardening Baseline* is ran. Included as part of that is the installation and configuration of NTP, a *nix daemon that automatically keeps server time synced and runs continuously. This is critical in order to synchronize the chronology of all events across the system at all times.
d. Access Requirements
    - Only those personnel designated are allowed to access monitoring logs.
    - Access to auditing solutions shall never be limited to one administrator/user.
e. Monitoring and Alerting – solutions are in place to monitor the MLBO HHS environment and alert when appropriate.

3. RESPONSIBILITIES & ACCOUNTABILTY

a. All supervisors are responsible for ensuring that members of the workforce are familiar with this policy on MLBO HHS's logging and monitoring standards.
b. It is the responsibility of the supervisor and IT team leadership to routinely review audit logs generated by the various components of the overall IT environment.
c. It is the responsibility of MLBO HHS IT staff to ensure that all technical capabilities as applies to auditing are performing at the expected standard and that all logs generated capture all the required data fields.

4. COMPLIANCE, ENFORCEMENT & SANCTIONS

a. Members of MLBO HHS workforce who violate this policy will be subject to corrective disciplinary action, up to and including termination of employment or contract with MLBO. If necessary, MLBO also reserves the right to advise appropriate legal officials of violations of a possible illegal nature

Internal and/or External References	HITRUST Common Security Framework (CSF) v8, 06.j Protection of Information Systems Audit Tools HITRUST Common Security Framework (CSF) v8, 09.aa Audit Logging HITRUST Common Security Framework (CSF) v8, 09.ab Monitoring System Use HITRUST Common Security Framework (CSF) v8, 09.ac Protection of Log Information HITRUST Common Security Framework (CSF) v8, 09.ad Administrator and Operator Logs HIPAA Security Rule §164.308(a)(1)(ii)(D) HIPAA Security Rule §164.312(b)
Compliance - Posting Date	7/16/2021
Replaces – Policy Number	
Next Review - Due Date	7/2024