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

Department: Administration Services-Information Technology **Policy Number:** HHS-ADM-IT 3512

Policy Title: Transmission Policy

Attachments:

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

Approved by: Jan Manary **Date:** 8.19.2021
Jan Manary, Executive Director HHS Health Services

Approved by: **Date:**
Nicole Anderson, Commissioner HHS 8.27.2021

POLICY STATEMENT: Technical controls must be in place for the transmission of covered information due to the sensitive nature of this information. The improper transmission of covered information can result in the loss of confidentiality, integrity or availability of this information; which can also result in legal ramifications for Mille Lacs Band of Ojibwe Health and Human Services (MLBO).

This policy applies to both the MLBO HHS networks and all 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.

Failure to comply with any part of MLBO HHS 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. In addition, state and/or federal agencies may act in accordance with applicable laws, rules and regulations.

PURPOSE: The purpose of this policy is to ensure the controls outlined within the Data/Information Classification Policy are implemented for the transmission of covered information by MLBO HHS.

POLICY:

- **Information System / Allowed Services**
  - Multiple safeguards must be addressed prior to the use of information systems for information exchange.
  - Prior to using an external public service (instant messaging, file sharing, etc.) not listed in the approved application list, approvals much be obtained.
  - Prior to using an external public service (instant messaging, filesharing, etc.) the user must obtain approval..

1.1. Information System Remote Access

1.1.1. The information system prohibits remote activation of collaborative computing devices and provides an explicit indication of use to users physically present at the devices.

1.1.2. Remote (external) access to the information assets and access to external information assets (for which MLBO HHS has no control) is based on clearly defined terms and conditions.

1.1.3. Cryptography is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.

1.1.4. Use of controlled portable storage media by individuals on external information systems is limited (or prohibited).

1.2. Information Protection

1.2.1. Strong levels of authentication must be used for granting access to internal information systems over a public network.

1.2.2. Stronger controls are implemented to protect certain electronic messages, and electronic messages are protected throughout the duration of its end-to-end transport path using cryptographic mechanisms unless protected by alternative measures.

1.2.3. Methods of encryption, used for the communication of covered information or remote access to internal information systems over public networks shall be FIPS-validated.

1.2.4. Covered information must be protected by encryption on all mobile/removable media and while being transmitted in accordance with the *Data / Information Classification Policy*.

1.2.5. Protocols used for communications are enhanced to address any new vulnerability, and the updated versions of the protocols are adopted as soon as possible. 1

1.2.6. Strong cryptography protocols are used to safeguard covered information during transmission over less trusted / open networks.

1.2.7. Cryptographic controls are used to enhance security, taking into account compliance with legal requirements.

1.2.8. Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g. SSL).

1.2.9. Legal considerations, including requirements for electronic signatures, are addressed.

1.2.10. Security is maintained through all aspects of the transaction.

1.2.11. Data involved in electronic commerce and online transactions is checked to determine if it contains covered information.

1.2.12. Attacks of the host(s) used for electronic commerce are addressed to provide resilient service(s).

1.2.13. Storage of the transaction details shall be located outside of any publicly accessible environments are not retained and exposed on a storage medium directly accessible from the Internet.

1.3. Messaging

1.3.1. Covered information shall not be sent unencrypted through end user-messaging systems.

1.3.1.1. If covered information needs to be sent through end-user messaging systems, the information must be protected.

1.4. Third-Party and External Systems

1.4.1. Designated personnel will establish terms and conditions consistent with any trust relationship established with external organizations owning, operating, and/or maintaining an external information system. Only when terms and conditions are accepted, third parties will allow authorized individuals to:

1.4.1.1. Access the information system from external information systems;

1.4.1.2. Process, store or transmit MLBO HHS controlled information using external information systems.

1.4.2. Documented agreements for electronic commerce arrangements are entered into and maintained between vendors on the agreed terms, including details on authorization, as well as other agreements with information service and value-added network providers, as needed.

1.4.3. Security implications of any network interconnection required for the implementation of electronic commerce services are identified and addressed. Specific steps are taken to ensure the confidentiality and integrity of electronic commerce are maintained

Internal and/or External References	
Compliance - Posting Date	8/27/2024
Replaces – Policy Number	
Next Review - Due Date	