PURPOSE

To protect MDHHS information systems and communications from security threats, both external and internal, and ensure that information is appropriately protected in transit and at rest.

REVISION HISTORY

Issued: 6/01/2023.
Next Review: 6/01/2024.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the State of Michigan (SOM.) Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency's business.

ePHI (Electronic Protected Health Information)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

PII (Personally Identifiable Information)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (such as, name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual..

PHI (Protected Health Information)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

Sensitive and confidential agency information, whether at rest or in-transit, must be protected from accidental or intentional threats that could corrupt, modify, delete, or disclose that information. Controls must consider threats from denial of service, attacks against network boundaries, transmission mechanisms, network disconnects, collaborative computing devices, other critical system components, multi-function devices, and printers.

MDHHS must, in coordination with DTMB, prevent unauthorized system management access and control information flow via shared information sources, connections, networks, and other data sources.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the system and communications protection [SC] family of NIST controls managed by MDHHS in accordance with DTMB 1340.00.170.01, System and Communications Protection Standard. MDHHS must review this policy annually.

This policy may require compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)

- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

- Social Security Administration (SSA) Technical System Security Requirements (TSSR)

- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

Application Partitioning [SC-2]

MDHHS must ensure the information system separates user functionality (including user interface services) from information system management functionality (such as, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access).

Information Remnants [SC-4]

MDHHS must ensure the information system prevents unauthorized and unintended information transfer via shared system resources. Information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) shall not be made available for object reuse or shall residual information be made available to any current users/roles (or current processes) that obtain access to shared system resources (such as, registers, main memory, hard disks) after those resources have been released back to information systems.

Denial of Service Protection [SC-5]

MDHHS must ensure the information system protects against or limits the effects of a Distributed Denial of Service attack (DDOS) by employing boundary protection devices and increased capacity and bandwidth combined with service redundancy.

Transmission Confidentiality and Integrity [SC-8]

MDHHS must ensure the information system protects the confidentiality and integrity of transmitted information.

- This control applies to both internal and external networks and all types of information system components from which information can be transmitted (such as, servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

- Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (such as by employing protected distribution systems or by logical means (for example, employing encryption techniques).

Cryptographic or Alternate Physical Protection [SC-8(1)]

MDHHS must ensure the information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

- Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

- Alternative physical security safeguards include, for example, protected distribution systems.

Use of Cryptography [SC-13]

MDHHS must ensure the implementation and documentation of encryption algorithms in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, and DTMB 1340.00.170.03, Electronic Data Encryption Standard.

Mobile Code [SC-18]

MDHHS must ensure the implementation and documentation of the following actions:

Definition of acceptable and unacceptable mobile code and mobile code technologies.

- Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.

- Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

Establishment of usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

- Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.
- Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (such as, smart phones).

Voice Over Internet Protocol (VoIP) [SC-19]

MDHHS must establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

Session Authenticity [SC-23]

MDHHS must ensure that the information system employs controls to protect the authenticity of communications sessions at the session versus packet level (such as sessions in service-oriented architectures providing web-based services) with grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

- Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

Protection of Information at Rest [SC-28]

MDHHS must ensure that the information system employs controls to protect the confidentiality and integrity of information at rest.

- This control addresses the confidentiality and integrity of information at rest and covers user information and system information.

- Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

ROLES AND RESPONSIBILITIES

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding, and complying with policies, standards, and procedures based on access controls.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations:

NIST 800-53 rev.4:

SC-1 System and Communication Protection Policy and Procedures

SC-2 Application Partitioning
SC-4 Information Remnants
SC-5 Denial of Service Protection
SC-8 Transmission Confidentiality and Integrity
SC-8(1) Cryptographic or Alternate Physical Protection
SC-13 Use of Cryptography
SC-18 Mobile Code
SC-19 Voice Over Internet Protocol (VoIP)
SC-23 Session Authenticity
SC-28 Protection of Information at Rest

45 CFR §164.312

164.312(a)(2)(iv) Encryption and Decryption (A)

164.312(c)(1) Integrity
164.312(e)(1) Transmission Security
164.312(e)(2)(i) Integrity Controls (A)
164.312(e)(2)(ii) Encryption (A)

State Standards/Regulations:

MDHHS Policy Manuals

68D-102 Physical Safeguards for the Storage, Use or Disclosure or Sensitive or PHI

68E-300 Automatic Log Out Policy and Procedure

DTMB IT Policies, Standards and Procedures

1340.00.170.01 System and Communications Standard
1340.00.170.03, Electronic Data Encryption Standard

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.