PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure that proactive security measures are taken to prevent and detect malicious software installation and that awareness is raised for recognizing and immediately reporting suspected occurrences of malicious software.

REVISION HISTORY

Reviewed: 01/01/2024.
Next Review: 01/01/2025.

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS that all computing devices, whether connected to the network or stand-alone, must use malicious software protection controls and configurations approved by the Department of Technology, Management and Budget (DTMB). All MDHHS computing devices must have automatic updates turned on to update at least once daily where applicable. These include all workstations, servers and portable computing devices.

Malicious software protection controls:

- Must not be disabled or bypassed without written authorization
- Must not be altered in a manner that will reduce the effectiveness of the controls

- Must not be altered to reduce the frequency of automatic updates

PROCEDURE

Department of Technology, Management and Budget

DTMB is responsible for the passive monitoring of IT security services, monitoring of firewalls, hardware security scanning and virus protection. DTMB is also responsible for monitoring infrastructure breaches and reporting those to MDHHS as warranted.

Only trained DTMB personnel will make changes or modifications to the configuration or function of the malicious software protection controls.

A plan should be developed and implemented to scan all computing devices on a periodic basis to ensure no unauthorized software is resident on any information system.

Workforce Member

Workforce members must:

- Use reasonable precautions to prevent importing data onto computers through physical (such as floppy disks, tapes, memory cards, jump drives, etc.) or electronic means (such as email, FTP, downloading from the web) that contain malicious software.
- Ensure that all portable computing devices or personal computers in their custody are running the malicious software protection controls specified by the Unit ISM.
- Immediately report to a supervisor, DTMB and MDHHS security officer any suspected downloads of malicious software.

Department of Technology, Management and Budget/MDHHS Security Staff

Malicious software protection training must be provided to all users in the unit.

REFERENCES

45 CFR 164.308(a)(5)

DTMB 1340.00.01 Acceptable Use of Information Technology

CONTACT

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