State of Michigan
Technical Standard

1340.00.130.02 Acceptable Use of Information Technology

Issued: 04/03/2013
Revised: 03/24/2023
Reviewed: 08/09/2022
Next Review Date (1 yr): 03/24/2024

Authoritative Policy: 1340.00 Information Technology Information Security Policy (https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/Admin-Guide/1300/POLICY-1340-Information-Technology-Information-Security.pdf)
Associated Procedures: n/a
Distribution: Statewide

Purpose

This statewide standard identifies acceptable use of information technology resources (IT Resources) to conduct state of Michigan (SOM) business and provides notice of expected User behavior. Unacceptable IT Resource use exposes the SOM to unwarranted risks, such as data breach, disruption of SOM network or application services, and other legal and liability issues. Unacceptable use may also consume IT Resource capacity and hinder SOM employees' ability to conduct business.

Contact/Owner

Department of Technology, Management and Budget (DTMB)
Cybersecurity and Infrastructure Protection (CIP)

Scope

This standard applies to all users granted access rights to SOM IT Resources (Users).

Standard

Acceptable Use of IT Resources

IT Resources, including devices, networks, data, software, email, and system accounts, are provided to conduct official SOM business. Authorized Users must act within the scope of their employment, contractual, or other relationship with the SOM and must agree to use IT Resources efficiently, responsibly, professionally, ethically, and lawfully, using approved applications, tools, and mechanisms. Users, regardless of their relationship with the SOM, as a condition of receiving access to SOM IT Resources, agree to abide by this standard, all applicable SOM policies and procedures, and all federal, state, and local laws.

Users are obligated to review these guidelines on a regular basis. Compliance is enforced based on the requirements in the currently published standard.

UNACCEPTABLE USE OF IT RESOURCES

1. ILLEGAL USE

IT Resources may only be used for lawful purposes. Prohibited activity includes use that is illegal under local, state, or federal law; violates SOM or other applicable regulations, policies, or standards; compromises public safety or the privacy of legally protected personal information; is malicious; or is fraudulent.

Users must abide by all intellectual property laws. Downloading, duplicating, or distributing copyrighted materials without specific written permission of the copyright owner is not allowed. Users shall respect all licensing agreements.

2. ABUSE

IT Resource use interfering with work obligations or SOM business is prohibited. IT Resources shall not be used for purposes unrelated to the SOM's mission and objectives, unless specifically authorized by this standard and agency work rules or directives. Examples of inappropriate use include(s):

- Commercial or personal product advertisements, solicitations, promotions, or for-profit purposes; political fundraising or lobbying; promoting a social, religious, or political cause; or gambling, gaming, or online shopping.
- To access, send, receive, or store any obscene, pornographic, offensive, or excessively violent content.
- To send messages containing unwelcome advances, profanity, or discriminatory or harassing remarks.
- To send hate mail or chain mail.
- To download entertainment software, music, movies, television shows, video-sharing content, or other similar files.

Users shall not download or install any software (including shareware and freeware) unless authorized by DTMB. No SOM-owned or -licensed software may be installed, copied, or used on non-SOM equipment unless expressly approved by DTMB.

Users shall not divulge or release any confidential information to the public that is not available to members of the general public. This does not prohibit disclosing a violation or suspected violation as authorized in Civil Service Commission Rule 2-10, unless otherwise prohibited.

Incidental personal use of IT Resources during lunch or break times may be authorized in agency work rules or directives but shall not interfere or conflict with a User's work obligations or SOM business and must comply with all applicable SOM policies.

3. SOCIAL NETWORKING

SOM Social Media Use:

DTMB's 1340.00.130.03 Social Media Standard (https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013003-Social-Media-Standard.pdf) establishes a statewide standard for the creation,

use, and management of official SOM social media and social networking accounts for Executive Branch Departments, Agencies, and Sub-units. Employees and contractors must follow the Social Media Standard when establishing social media accounts or profiles for the State of Michigan. When representing, giving opinions, or speaking on behalf of the SOM as part of an employee's or contractors legitimate job duties, the employee should be designated as an authorized spokesperson. Compliance with restrictions in section 5. Security of this standard are applicable to all social media usage.

Employee Personal Social Media Use:

SOM public officers and employees must comply with the Standards of Conduct for Public Officers and Employees Act (MCL 15.341 et seq.) (http://legislature.mi.gov/doc.aspx?mcl-15-342). Personal social media activity referencing the SOM, SOM employment, SOM activities, or the use of SOM logos or images increases the likelihood that personal usage will be viewed as representing the SOM. The use of a SOM email address for any online activity also associates such activity with the SOM and supports an interpretation of representing or speaking on behalf of the SOM. Personal social media activity on one's own time and device(s) may still create concerns if identified or identifiable as a SOM employee. For compliance with this standard, employees must be diligent in preventing the interpretation they are representing or speaking on behalf of the SOM in their personal online activity.

4. Online License Agreements

Some Internet sites may impose Terms of Service agreements that are unacceptable to the SOM, such as indemnification clauses or agreements to be sued in other states. When accessing these sites without specific prior SOM authorization, the User accepts such terms solely in a personal capacity and is personally and solely responsible for any legal claims arising from an agreement "signed" by clicking to agree on the terms of service.

5. Security

Users must follow all applicable security policies and standards and are responsible for the reasonable (1) physical security and protection of their IT Resources and devices and (2) protection and use of granted access. Users shall not reveal to or allow use of their accounts or passwords by others, including family members. Users shall not leave workstations, devices, or IT Resources unattended without engaging password protections.

Users must maintain the security of SOM data. Providing unauthorized persons any information that is sensitive or protected by law; unauthorized posting of SOM information to external newsgroups, bulletin boards, or other public forums; sharing personal information about another person unless part of legitimate job duties; and storing SOM information in public storage services without DTMB approval are prohibited.

Users also shall not:

- Interfere with the normal operation of any IT Resource.
- Act to disrupt systems or cause unnecessary network congestion or application delays.

- Try to compromise or cause intentional damage or loss to SOM systems or data.
- Modify or circumvent security safeguards or access controls.
- Use tools or utilities to reroute traffic on, scan, probe, or attack a network.
- Intercept or try to intercept any data transmissions without authorization.
- Use unauthorized peer-to-peer (P2P) networking, file sharing, instant messaging or Internet Relay Chat (IRC) applications or services.
- Forward SOM email messages to personal email accounts that would create unacceptable privacy, security, or compliance risks.
- Use non-DTMB approved email servers or services to conduct SOM business.
- Use any app, software, or other technology on an electronic device that prevents it from maintaining or preserving a public record as required by law.
- Use any unauthorized remote-control software, tools, or services on any internal or external SOM devices or systems not set up by DTMB.
- Store SOM data in public storage services, unless approved by DTMB.
- Post SOM information to external newsgroups, bulletin boards, or other public forums, unless authorized.
- Send unsolicited email messages, including junk mail or other advertising material, to individuals who did not specifically request such material.
- Install or attach any unauthorized equipment to an IT Resource without approval of DTMB and the resource owner, (e.g., wireless access points, modems, disk drives, external hard drives, networking devices, personal mobile devices or computers, etc.). Unauthorized equipment will be confiscated.
- Intentionally modify, damage, or remove IT Resources owned by the SOM without authorization from DTMB and the IT Resource owner.
- Intentionally modify, disable, test, or circumvent any IT Resource security controls without authorization.
- Intentionally cause a security incident resulting in a loss of data confidentiality or integrity or a disruption or denial of availability.
- Circumvent user authentication or compromise the security of a host, network, or account.
- Seek or enable unauthorized access to any computer system, application or service.
- Intentionally seek information on, obtain copies of, or modify files, data, or passwords of other Users.

- Impersonate or fraudulently represent other Users on the network.
- Attempt to access any computer account or part of the SOM's network to which they are not authorized.
- Participate in activities that promote computer crime or misuse, including posting on internal or external sites; disclosing passwords, credit card, or account numbers; and revealing system vulnerabilities.

6. ACCOUNTABILITY

All SOM business functions must be conducted on equipment approved for the type of work being completed. The use of private email for conducting state business within the executive branch of state government is prohibited. State email accounts must not be used for non-state activity.

No data shall be stored in any unauthorized storage system. The only exception to this is data that is classified as Public based on the Data Classification Standard (1340.00.150.02 Data Classification Standard (sharepoint.com) with:

- Confidentiality of Low
- Integrity of Low
- Availability of Low

NO PRESUMPTION OF PRIVACY

Data is a valuable SOM asset that must be protected. As per MCL 750.491, all records created by or received in any state agency are public property belonging to the State of Michigan. Any data Users create, store, process, or send using SOM IT Resources remains the property of the SOM. The SOM cannot guarantee the confidentiality or privacy of Users, unless applicable law provides differently. Users have no expectation of privacy in their use of SOM-provided email, instant messaging, computing equipment, Intranet or Internet access, or other SOM information systems. Any effort to circumvent this standard by using anonymous proxies, software, or hardware; use software or websites to hide Internet activity; or use devices or utilities to remove or camouflage information of evidentiary value is considered a violation of this standard. This includes the use of mobile device applications that do not encrypt messages and/or do not retain them for official records purposes. There is also no expectation of privacy for users who access personal email or messages using SOM equipment of information systems.

The SOM actively monitors IT Resources to ensure compliance with policy. This includes real-time monitoring of network traffic; the transfer of data created, sent, received or stored on IT Resources; and other monitoring and auditing the SOM may deem necessary. The SOM also blocks unauthorized internal and external traffic and services that may cause risk to IT Resources. Any evidence of illegal activity or unacceptable use discovered during monitoring or reviews may be provided to SOM management or law enforcement organizations.

Electronic records may also be available for public distribution under the Freedom of Information Act (FOIA).

The SOM may require Users to surrender to SOM authorities any IT Resources (state-owned or personal) that have been used to conduct SOM business or on the SOM's network, in response to discovery orders from a court of law; information holds from the Agency or Attorney General; acceptable use or cybersecurity-incident investigations by the SOM; or FOIA Requests.

INADVERTENT OR ERRONEOUS USE

Users inadvertently directed to a website that violates laws, regulations, polices or this standard may claim erroneous use by immediately reporting to managers when unintentional misuse occurs. Self-reporting is encouraged and may be done without consequence in demonstrated cases of inadvertent use.

RESPONSIBILITIES

- Agencies shall communicate this standard to all Users, ensure that users read and understand this standard, and develop processes to certify and document User acceptance.
- Users shall read this standard, understand its expectations, and follow its provisions. Each User shall acknowledge receipt of this standard and any agency-specific addenda. Each User shall report all violations to their manager or Agency contact, who must report all violations to Michigan Cyber Security (MCS).
- Agents, contract staff, vendors, and volunteers who use IT Resources shall follow and acknowledge awareness of this standard.
- Managers or Directors shall require all Users under their management to read and acknowledge this standard and abide by its provisions.
- Agency Human Resources shall support managers as needed in assuring awareness and enforcement of this standard.
- DTMB Information Technology Staff shall report suspected violations of this standard found in system support activity to CIP and assist CIP with audits and enforcement actions.
- CIP shall receive and document reports of suspected abuse from any source and respond as necessary. CIP shall supervise periodic system and network audits for abuse and compliance with this standard. CIP shall report abuse to Agency Human Resources, internal auditors, and appropriate law enforcement officials when appropriate. CIP shall also assist in preserving digital forensic evidence.
- DTMB Procurement, Contract Administrators, and Project Managers shall ensure contracts obligate contractors to comply with all applicable IT policies, standards, and procedures and that appropriate compliance activities occur.

EFFECT

The standard sets minimum expectations for all SOM IT Resources. Agency work rules supporting this standard may provide departmental guidance on how violations are handled. SOM agencies may implement policies on IT Resources consistent with this standard and may implement more restrictive standards on IT Resources with prior coordination with MCS.

All employees must understand and accept that misuse or abuse of IT Resources may lead to agency investigation and criminal, civil, or legal actions and discipline, up to and including discharge. IT Resources may be removed from a work area for analysis.

REFERENCES

SOM 1340.00.130.03 Social Media Standard (https://www.michigan.gov/documents/dtmb/1340.00.130.03_Social_Media_Standard_604897_7.pdf).

APPROVING AUTHORITY

Michelle Lange, Director Revised: 03/24/2023