OFFICIAL ORDER
MICHIGAN STATE POLICE

Chapter:	**Phones, Computers, and Information Technology**
Subject:	**17-07 – Information Technology Security**
Effective:	December 28, 2022
Supersedes:	Official Order 17-07, dated April 19, 2022
Distribution:	Department Members

PURPOSE: This Order outlines the acceptable use of information technology resources. Members using information technology equipment to communicate data to, through, or on any device connected to any Michigan State Police (MSP) data network shall adhere to the following security policy.

17-07-1 INFORMATION TECHNOLOGY SECURITY STANDARDS

The primary objective of information technology security is controlling the confidentiality, integrity, and availability of computerized information. Only properly authorized individuals shall possess the ability to review, create, delete, or modify information. Controlling this access imposes four requirements:

A. Personnel, proprietary, or other sensitive data is accessible only by authorized users.

B. Stored information and managing programs adhere to strict controls.

C. Systems, data, and services are accessible by those who require access.

D. All aspects of operation conform to applicable laws, regulations, licenses, contracts, and established ethical principles.

17-07-2 SECURITY MISSION STATEMENT

The information technology security mission of the department is to support the organization by facilitating access for authorized users and protecting information from unauthorized access, disclosure, modification, or destruction.

17-07-3 SECURITY STANDARDS AND POLICIES

A. Privacy and Monitoring

The department and the State of Michigan reserve the right to monitor and log all network and system activity with or without notice. Members have no expectation of privacy in the use of these resources.

B. Acceptable Use of Information Technology Resources

(1) Members shall adhere to the State of Michigan’s Acceptable Use of Information Technology.

(2) Members shall not use State of Michigan technology to access inappropriate material unless the access is work-related. Inappropriate material includes, but is not limited to:

a. Adult/sexually explicit

b. Chat/instant messaging

c. Gambling

d. Games

e. Glamour and intimate apparel

f. Personals and dating

g. Remote proxies

h. Web-based email

i. Internet/peer-to-peer file sharing

j. Music and movie downloads

k. Personal e-commerce activities such as online banking, online bill paying, online purchases, and bidding on online auctions.

C. Applicable Information Resources

(1) Information technology media used for temporary or permanent storage of department information, regardless of its type.

(2) Information technology media used to transmit department information.

(3) Information technology devices containing information pertaining to the function of the department.

(4) Information technology devices used to communicate to or through networks or stand-alone devices which store or have access to department information.

D. Physical Access Control Requirements

(1) Access to any computing device by persons not employed or authorized by the department is strictly prohibited.

(2) Printers capable of printing sensitive or secure information shall be placed in an area where access can be monitored and where it is out of view of the general public.

(3) Data communications equipment and servers used in the transmission and storage of department data shall be placed in a secure location.

(4) No unsecured worksite or office shall have a live data connection to the network.

(5) All information systems shall be configured to display the following network login banner before granting access:

****************************** NOTICE TO USERS ***************************
This system is the property of the State of Michigan and is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site and law enforcement personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site and State of Michigan personnel.

Unauthorized or improper use of this system may result in civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.
****

E. Workstation Controls

(1) At a minimum, all workstations shall require the use of a unique username (user ID) and password to gain access.

(2) Members shall manually lock their systems when leaving their work area and have the screen saver enabled and configured to lock the system after 15 minutes of inactivity.

F. User ID/Password Assignment and Use

(1) Each user shall be issued a unique user ID and password for system/network access. This ID will be used to authorize access and to log user activity.

(2) Laptops must utilize full disk encryption and antivirus protection.

(3) The Department of Technology, Management, and Budget (DTMB) shall generate and assign the initial password for each user ID. The end user of the password shall change the password upon initial system login.

(4) Password composition shall be a minimum of eight characters in length. Passwords shall not be a dictionary word, a proper name, or the user ID. The password shall include a special character and at least one number and upper/lower case letters.

(5) Members shall change their passwords every 90 days. The new password must not be the same as the previous ten passwords.

(6) Members shall keep their passwords private. If written down, passwords must be stored in a secure location where others cannot gain access to them.

(7) Systems shall be configured to automatically enforce the department’s password policy, shall not display the password when entered and shall not transmit the password unencrypted.

G. Viruses, Piracy, and Unauthorized Software

(1) Media sent to another site or received by a worksite shall be checked against the virus detection software.

(2) Members or contractors shall not copy any software licensed by the department without authorization from the Information Security Officer (ISO), Michigan Cyber Security officer (MCS), and the software licenser.

(3) Software that violates copyright provisions, violates a license agreement, or conflicts with existing network or application software shall not be used at a worksite.

(4) Only software that has been approved by the ISO and the DTMB shall be installed on MSP information technology systems.

H. Access Control

(1) Access Control of Servers and Data Communications Equipment

a. Servers and data communications equipment shall be kept in a locked, secure environment with access granted only on a need basis.

b. Server and data communications equipment consoles shall be protected by a password for keyboard access.

c. Remote administration of server and data communications equipment shall be via secure channels using a minimum of 128-bit encryption using a FIPS 140-2 certified encryption module.

(2) Server and Data Communications Equipment Protection

a. Servers and data communications equipment shall be kept in strict compliance with the manufacturer's power and cooling requirements.

b. File servers shall have isolated power that is fault protected and uninterruptible power supplies which filter AC power and which allow graceful and automatic shutdown of servers when loss of power is imminent.

(3) Backup Controls

All data shall be backed up frequently. Site coordinators shall ensure proper backup based on guidelines issued by the DTMB and the ISO.

(4) Remote Access

Any single connected state government workstation shall not have its own dial-in capability. All dial-in access shall be through centralized authentication servers approved by the MCS.

(5) Authority and Privileges

a. End users shall have full access to the data files they create. Files should be stored by default in the user's own directory within OneDrive.

b. Servers shall have a shared common directory where end users may save non-secure information.

c. Electronic mail (email) shall be treated the same as a written memo where security and confidentiality are concerned. All email is available under the Freedom of Information Act (FOIA). Email that has been deleted may still be part of the server backup.

d. Designated site coordinators, the ISO, and DTMB personnel may have extended authority beyond what is normally available to an end user.

e. All extensions to the department's wide area network or modifications to existing extensions must be approved by the ISO and MCS.

f. Use of wireless data communications to provide connectivity to department information technology resources must be approved by the ISO and MCS.

(6) Granting Privileges

Only authorized DTMB personnel and the ISO may upgrade the security access rights of end users to the network or devices.

(7) Procedures for Changing Security Access to the network or devices

Higher security privileges are granted on a need basis. Requests for increased security privileges shall come from the end user’s immediate supervisor to the ISO.

I. Storage of Sensitive Information on Mobile Devices or Portable Media

(1) Storage of sensitive information on mobile devices or portable media is permitted only if all of the following requirements have been satisfied:

a. Use is restricted to individuals whose job duties require it.

b. Sensitive data is encrypted. Encryption must comply with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy.

(2) Any instance of sensitive information (encrypted or unencrypted) being lost or stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, must be reported immediately to the worksite commander, the ISO, and the DTMB at 1-877-264-2546.

(3) Mobile devices are defined as any mobile device (state or privately owned) capable of storing data, such as laptop and tablet PCs, Blackberry’s, cell phones, personal digital assistants (PDAs), iPods, and MP3 players.

(4) Portable media is defined as any portable media (state or privately owned) capable of storing data, such as external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs DVDs, and floppy disks.

(5) Sensitive information is defined as items that are governed or restricted in some manner by a federal or state statute, rule, policy, or requirement. At a minimum, sensitive information includes social security numbers, credit card numbers, personal health records, and criminal justice information.

J. Standard/Policy for Using Wireless

(1) “Wireless Network” is defined as a telecommunications network whose communication between devices is implemented without the use of wires. Wireless telecommunication networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier.

(2) “Wireless” is defined as any type of electrical or electronic operation which is accomplished without the use of a "hard wired" connection. Wireless communication is the transfer of information over a distance without the use of electrical conductors or wires.

(3) Wireless technology is generally used for mobile information technology equipment. It encompasses cellular telephones, PDAs, global positioning units, garage door openers, wireless computer mice and keyboards, satellite television, etc.

a. Currently, department imaged laptops and department issued cellular devices are allowed to connect wirelessly to the department's network.

b. The user shall use an approved Two Factor Authentication solution such as SecurID token and Virtual Private Network (VPN) client software that employs a minimum of 128-bit encryption whenever they wirelessly connect to the department network.

c. Wireless connections to any other network (coffee shops, bookstores, etc.) without the use of the State of Michigan VPN or Netmotion client are not allowed, since said networks are not protected or controlled by State of Michigan personnel. (This includes any wireless technology built into or added to the laptop.)

d. Users must connect to the State of Michigan Network to get patches and virus updates every two weeks.

(4) Any exception to the above must be approved by the MSP ISO.

K. Information Technology Incident and Security Breach Reporting

(1) Any member with knowledge of a violation or potential violation of this Official Order, or any State of Michigan Standards, Policies, and Procedures related to IT Security or Privacy must immediately report this information to the Information Security Officer.

(2) Any breach or suspected breach of any MSP Information System, MSP facility, or any loss of MSP data (in any format) or any IT equipment (including, but not limited to, laptops and USB drives) must be immediately reported to the DTMB Client Service Center at 877-264-2546 or 517-241-9700, their immediate supervisor, and the Information Security Officer. DTMB Security Breach Procedure 1340.00.090.01.01 must then be followed.

a. Any breach or suspected breach of Criminal Justice Information must also be reported immediately to the CJIS Information Security Officer. Form CJIS-016 must be completed as soon as possible after reporting the incident.

(3) Following the activation of the DTMB Security Breach Procedure, the Information Security Officer will assess the incident and develop an after-action report that documents the incident, describes how the incident occurred, advises how to prevent it from occurring in the future, identifies lessons learned from the incident, and presents opportunities for improvement.

17-07-4 MANAGEMENT AND MEMBER RESPONSIBILITIES

A. The ISO shall develop and disseminate information technology security policies and standards and will function as the department-wide Information Technology Security Administrator.

B. The ISO and MCS shall monitor information technology resource usage to ensure members and systems are in compliance with existing policies through the use of various logging, capture, and analysis tools. The ISO will assist the department as necessary in investigations related to non-compliance.

C. The ISO and MCS shall audit department information systems for policy compliance and resiliency through the use of various vulnerability assessment and penetration testing tools.

D. The ISO and MCS shall audit department worksites for physical policy compliance.

E. The ISO and MCS shall oversee the incident handling and investigation of information technology systems where security has been compromised.

F. District and division commanders shall ensure that all aspects of the information technology security policies and standards are adhered to by members under their command.

G. Site coordinators shall assist the ISO and MCS in securely administering the department's information technology infrastructure.

H. Members shall assist the department in maintaining a consistent watch on all information systems by complying with applicable security policies and alerting management and/or the ISO to misuse of department information technology resources or compromises in security.

17-07-5 INFORMATION TECHNOLOGY SECURITY ADMINISTRATION

The ISO is responsible for development, administration, and auditing compliance of information technology security plans that address, but are not limited to, the following areas:

A. Develop and publish security policies, procedures, and guidelines that are in compliance with the State of Michigan's Acceptable Use of Information Technology, the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and the Criminal Justice Information Systems (CJIS) Security Policy, as well as generally accepted information technology standards.

B. Develop and maintain an organization-wide information security awareness and education program.

C. Develop and maintain minimum guidelines and procedures for access control for all wide and local area network attached computer systems, routers, gateways, and management devices, including all electronic devices that require the network for transport of information.

D. Develop and implement information security review procedures and work programs which support the organization's policies, procedures, standards, and guidelines.

E. Participate in system specification, design, development, and acquisition of information technology initiatives to ensure that security requirements are incorporated into all automated applications.

F. Evaluate, select, and implement emerging information security hardware, software, services, and techniques within the organization's computer systems as appropriate.

G. Coordinate the acquisition, development, and distribution of security information to others within the organization as appropriate and provide technical assistance to users as required or requested.

H. Accept other information security responsibilities as deemed appropriate.

17-07-6 COMPLIANCE WITH FBI CJIS SECURITY POLICY, MICHIGAN CJIS POLICY COUNCIL ACT AND CJIS ADMINISTRATIVE RULES

A. Data stored in any department information system is governed by the CJIS Policy Council Act and associated administrative rules.

B. Data obtained from systems governed by the CJIS Policy Council Act must also comply with the FBI CJIS Security Policy.

C. Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract, and/or criminal prosecution where the act constitutes a violation of law.

DIRECTOR

Annual Review Responsibility:	Information Technology Division
Accreditation Standards:	CALEA TBD