OFFICIAL ORDER
MICHIGAN STATE POLICE

SUBJECT: Telephone, Web, Social Media Use, and Information Technology Security Policy

TO: Members of the Department

This Order establishes department policy and member responsibilities for the following:

Section 21.4	REVISION RESPONSIBILITY	19

21.1 LANDLINE AND CELLULAR DEVICE USAGE, BILLING, AND REPORTING

Proper and courteous telephone use by members is essential to establishing and maintaining the public image of the department. This section provides policy and procedure for the proper use, billing, and reporting of landline and cellular devices.

21.1.1. LANDLINE TELEPHONE USE

A. Handling Calls

(1) Telephone calls shall always be answered promptly and courteously.

(2) The member answering the telephone call shall identify themselves and their work unit unless prohibited from doing so by their work site's policy.

(3) If a member has arranged for a coworker to answer their telephone when they are away from their desk, they shall keep the coworker informed of their whereabouts and probable return time.

B. Placing Calls

(1) Calls made on the state network should be dialed as instructed in the "Dialing Procedures" chapter of the State of Michigan Telephone Directory.

(2) Business-Related Long-Distance Calls

a. Calls to out-of-state areas shall be placed direct-dial, long-distance.

b. International Calls

Members making an international call shall receive prior authorization from their district or division commander. The Headquarters switchboard operators will place international calls for authorized members and will report these calls to the Communications Section.

c. To minimize costs, long-distance calls shall be as brief as possible, organized in advance, and limited to business matters.

d. The Headquarters switchboard operators shall not transfer callers to long-distance telephone numbers.

(3) Personal Long-Distance Calls

a. The state telephone system, FAX machines, modem lines, and state-issued telephone calling cards shall be used only for official state business and shall not be used for personal long-distance calls.

b. Personal calls shall be charged to one's residence telephone, personal credit card, or made from a pay phone.

c. Long-distance calls from union members to their representation organizations are considered personal calls if they are made for other than official state business. Such calls shall not be made on state lines or charged to the department.

C. Telephone Call Forwarding

(1) Published Business Number

Work site commanders shall arrange for calls to the published work site business number to be forwarded to the consolidated or regional communication center during hours when the work site office is not staffed.

(2) During business hours, work site commanders should make every effort to ensure calls are answered by a member to avoid the possibility of citizens reaching a recorded message during emergency calls. In the event it is not possible for a member to answer the call, such as during times of high call volume, the call may terminate at a recorded greeting following the procedures outlined in Section 21.1.3 of this Order.

(3) Non-Published Department Numbers

a. Telephone lines serving non-published department numbers may terminate at a voice mail or answering machine system.

b. The recorded greeting shall, at a minimum, follow procedures outlined in Section 21.1.3 of this Order.

21.1.2. CHANGES TO LANDLINE TELEPHONE SERVICE

A. The Communications Section shall coordinate telephone moves, additions, and changes.

B. Requests for additions or deletions to telephone service on Department of Technology, Management, and Budget (DTMB) supported telephone systems shall be submitted by the work site telephone site coordinator on a DTMBe-906 form for AVAYA users or a Remedy ticket for CISCO users. Requests for additions only must first be requested on the Landline and Data Services Request form (ADM-089) and forwarded to the agency site coordinator in the Communications Section.

Requests for additions or deletions to telephone systems not supported by DTMB should be submitted by the work site telephone site coordinator to the agency site coordinator in the Communications Section. Work site commanders should contact local service providers for emergency repairs and follow-up with notification to the agency site coordinator in the Communications Section.

C. Requests for new phone service or phone systems require approval from the Communications Section.

21.1.3. VOICEMAIL GREETINGS

Members shall update voicemail greetings to inform callers whether they are in or out of the office and when a return call may be expected.

A. Individual Voicemail Greeting, At-Post Personnel:

"Thank you for calling Sgt./Tpr. _____ of the Michigan State Police. I am currently unavailable to take your call. Please leave your name, telephone number, and the reason for your call and I will contact you at my earliest opportunity. If you need immediate assistance, please press 0. Thank you and have a safe day."

NOTE: When 0 is pressed during business hours, callers will be routed to the desk sergeant. After-hours, callers will be routed to the Regional Communication Center (RCC).

B. Post Voicemail:

"You have reached the Michigan State Police – _____ Post. If this is an emergency, please hang up and dial 9-1-1. All lines are currently being answered by post personnel. To leave a message to be returned by post personnel, press 1, to reach the Michigan State Police Regional Communication Center please press 2; to leave a message or crime tip for the detective bureau, tips can be anonymous, please press 3; to receive road and weather condition information, please press 4; If you are calling for a copy of a traffic crash report handled by the Michigan State Police, please press 5; to repeat these options, please press 6. Thank you and have a safe day."

(1) When 1 is pressed, dial-by-name directory may be available; however, it is based on the capabilities of the phone system.

(2) Number programmed should be the appropriate RCC.

(3) This should be a general mail box for the Post to record their own message or be attached to the Post detective-sergeant's phone.

(4) Road Condition Script: When 3 is pressed; it will provide the Michigan Department of Transportation Roads and Travel website. The official message is:

"For road and weather information, please visit www.michigan.gov/midrive , Thank you."

(5) Traffic Crash Script: When 1 is pressed; it will provide information on the crash report website to pull the crash reports. The official message is:

"If you would like a copy of a traffic crash report taken by the Michigan State Police, please visit www.michigan.gov/crash. Information and directions for ordering a report can be found on the website. Thank you."

(6) When 0 is pressed during business hours, callers will be routed to the desk sergeant; after-hours, callers will be routed to the RCC. This option will not be specified in the script as to encourage people to listen to the entire message to make the best selection.

21.1.4. USE OF DEPARTMENT-ISSUED CELLULAR DEVICES

A. Cellular Devices are defined as: cellular phone, smartphone, connected tablet, wireless air card, wireless modem, mi-fi (or Jet Pack).

B. General Requirements

(1) Members issued department cellular phones for business use shall carry the department-issued cellular phone with them while on duty. Such members, however, are not required to carry their issued cell phone while off duty.

(2) Cellular voicemail shall be checked several times during each work day and calls shall be returned by the next working day.

(3) If a member has been issued a cellular device that is no longer being used by that member, it shall be returned to the Communications Section, along with the Wireless Device Return form, (ADM-091).

(4) Department members that have been issued a smartphone or tablet must have the Mobile Device Management (MDM) software installed on their device. MDM software shall only be removed by the Communications Section, or authorized DTMB personnel. MDM adds another layer of encryption making the device more secure, and allows department-issued devices to meet Criminal Justice Information Services (CJIS) requirements.

C. Requests and Changes

(1) Requests for new cellular devices shall be submitted on the Wireless Device Request form (ADM-088), signed by the district/division commander and bureau commander, and forwarded to the Communications Section, MSP-Phones.

(2) Refer to the ADM-088i Wireless Device Request Matrix for general guidelines, approval, and cost information.

(3) Cellular devices are assigned to a department member and shall be transferred with the member.

(4) Mobile numbers are assigned to a department member and shall be retained by the member when transferred. If required, the Communications Section, Wireless and Landline Unit, can change the mobile number to reflect the new work site assignment, if the number is assigned to a position or is retained due to restricted funding.

(5) The Communications Section, Wireless and Landline Unit, shall be notified of personnel transfers in order to track and coordinate equipment and service. Cancellation of service, repair or replacement of equipment, or any other changes shall be coordinated through the Communications Section. Upon a member's retirement from the department, their cellular devices shall be returned to the Communications Section, with a completed Wireless Device Return form, (ADM-091).

D. Handling Calls

(1) Members answering department-issued cellular telephones shall identify themselves and their work unit unless they are part of a unit that conducts undercover operations.

(2) Members issued department cell phones with enabled voicemail shall use the following greeting:

"Thank you for calling Mr./Ms./Sgt./Tpr. _____ of the Michigan State Police. I am currently unavailable to take your call. Please leave your name, telephone number, and the reason for your call and I will contact you at my earliest opportunity. Thank you and have a safe day."

E. Personal Usage

Unless the employee is participating in the department-authorized program that requires pre-payment by the employee to the department for any personal use of a department-issued cellular device, the following restrictions apply to personal use of department-issued cellular devices:

(1) Department-issued cellular device shall be used only for official state business and shall not be used for personal calls or data.

(2) Department members may use personally owned cellular telephones for personal calls in department vehicles if done so safely and in accordance with Section 21.1.7 of this Order.

F. Vehicle Installation

(1) District or division commanders and Executive Council members who are often required to conduct business while traveling in a department vehicle may equip their assigned vehicle with a hands-free cellular telephone device.

(2) Other department members who believe they also need such a device may only proceed with installation in their assigned vehicle with the approval of their bureau commander.

G. International Usage

(1) Members shall notify the Communications Section prior to international travel when taking their department-issued cellular device.

(2) If member is on the Personal Use Plan, and is traveling internationally for personal reasons, they are responsible for a one-time fee and any overage charges incurred.

21.1.5. LOST OR STOLEN MOBILE DEVICE

A. The affected member shall immediately notify the MiCJIN Help Desk at (877) 264-XXXX and identify that the device has been lost or stolen and is under the ownership of the Michigan State Police. The mobile number, type, locked-state, and last known location of the device, as well as date and time of loss, shall be noted.

B. They shall also notify their immediate supervisor of the loss of the device. The mobile number, type, locked-state, and last known location of the device, as well as date and time of loss, shall be noted.

C. The immediate supervisor will notify the work site commander. The immediate supervisor will also notify the Communications Section, Wireless and Landline Unit, of the loss through an email to MSP-Phones. The mobile number, type, locked-state, and last known location of the device, as well as date and time of loss, shall be noted.

D. The Communications Section, Wireless and Landline Unit, shall suspend service on the mobile number, after a successful wipe of all content has been accomplished by the DTMB Smart Device Support Team using the State of Michigan MDM tool.

E. A Wireless Device Request form, the ADM-088, shall be completed for a replacement device and sent to MSP-Phones.

21.1.6. CELL PHONE AND SMART DEVICE ACCEPTABLE USE POLICY

A. Enrollment

(1) Members shall not use a department-issued cell phone or smart device for personal use, unless they are enrolled in the department's Cell Phone and Smartphone Personal Use Plan (ADM-090) at the time of such use.

Members who participate in the department's Personal Use Plan will be invoiced at the beginning enrollment period for the full annual amount. Rates for members with a predetermined retirement date will be prorated. Members must remit payment in full within one month of invoicing in order to be considered enrolled in the department's Personal Use Plan. Failure to pay within one month shall result in the member's immediate removal from the Personal Use Plan.

B. Personal Use of a Department-Issued Cell Phone or Smart Device

The primary purpose of a department-issued device is for conducting official department business and is subject to all state security policies, audits, and use review. By enrolling in the department's Personal Use Plan, members agree they will not use the device in an illegal or inappropriate manner. Use of a department-issued device in an illegal or inappropriate manner may result in discipline up to and including termination.

C. Illegal Use

(1) Department-issued devices may be used for lawful purposes only. Activity that is illegal under local, state, or federal law, rules, regulations, mandates, policies, or standards is prohibited.

(2) Users shall abide by all copyright, trademarks, patents, or other laws governing intellectual property. Downloading, copying, duplicating, or distributing copyrighted materials without specific written permission of the copyright owner is prohibited.

(3) Users shall respect and adhere to all licensing agreements and software license provisions. The installation of any software, including shareware and freeware, that may fall into the realm of illegal use or inappropriate use is prohibited.

D. Inappropriate Use

(1) Use of a department-issued device to access, display, process, perform, send, receive, or store any materials or content that is obscene, pornographic, lewd, lascivious, considered or categorized as adult content or offensive is prohibited.

(2) Use of a department-issued device that compromises public safety or the privacy of legally protected resident or citizen information is prohibited.

(3) Activity that is malicious or fraudulent in nature is prohibited.

(4) The use of obscenity, racial epithets, discriminatory remarks, or other language that may be offensive to another user, sending of hate mail or chain letters, harassment, and other antisocial behaviors are also prohibited.

21.1.7. USE OF MOBILE COMMUNICATION DEVICES WHILE DRIVING

A. Members shall not text message, surf the Internet, or read or respond to email while operating a department vehicle, or if utilizing a personal vehicle for state business.

(1) This prohibition regarding the use of mobile communication devices, whether state supplied or personally owned, applies to any device that makes or receives text messages, connects to the Internet, or allows for reading or responding to email.

(2) This prohibition does not apply to members who utilize in-car computers for law enforcement purposes such as accessing LEIN or other public safety databases.

(3) Members shall limit conversations on cell phones to department business while operating department vehicles or personal vehicles for state business.

B. Members are strongly encouraged to avoid driver distractions by stopping the vehicle they are operating in a safe location to attend to the distraction whether it be electronic (e.g. cell phones, portable music devices), reading directions, eating, or any other activity that reduces driver focus.

C. When a member of the department becomes involved in a vehicle crash while engaged in normal department business, during a pursuit, or emergency driving, a complete and thorough investigation shall be conducted. If negligence or noncompliance with the provisions of the Michigan Vehicle Code or the requirements of this Order is shown, appropriate disciplinary action shall follow.

21.1.8. BILLING AND REPORTING PROCEDURES

A. The Communications Section reviews and processes payments on all department cellular device bills and department landline telephone bills statewide. Upon written request to the Communications Section commander, call details may be shared with work site commanders to ensure compliance with Official Orders and payment policies.

B. Member Reimbursing the Department

(1) Unless enrolled in the department's Personal Use Plan, a member shall reimburse the department for personal use of a department-owned wireless devices as soon as practical after the personal use.

(2) The member shall contact the Communications Section for a copy of the appropriate billing statement so they can identify the exact amount of the necessary reimbursement.

(3) The member shall send a cover memo and reimbursement check to the Budget and Financial Services Division for credit to the appropriate section PCA and Index.

(4) If the need for a member to reimburse the department is determined by an audit, the responsible section shall notify the member's division or district commander. Administrative and legal action may be initiated as necessary.

(5) Members who violate this Official Order shall be charged for personal use on department-issued telephones or cellular telephones. Reimbursement to the department may be in addition to disciplinary actions.

21.2 WEB AND SOCIAL MEDIA POLICY

This section outlines department policy concerning the creation or use of websites and social media by department members in an effort to set clear expectations for the conduct of members using websites and social media, identify how communications on websites and social media relate to other policies as set forth in Official Orders, and to provide the grounds for member discipline based on the inappropriate use of websites and social media.

21.2.1. DEFINITIONS

A. "Internet" - a system which connects computers around the world using Transmission Control Protocol/Internet Protocol (TCP/IP) to facilitate data transmission and exchange between billions of interconnected Web pages collectively known as the World Wide Web (Web).

B. "Social Media" – those forms of electronic communication using websites, applications, and services on the Internet for social networking.

C. "Social Networking" – the use of websites, services, and applications on the Internet to facilitate user collaboration and dissemination of information including:

(1) Social networks such as MySpace, Facebook, Google, LinkedIn, and Twitter.

(2) Video, podcasts, and photo-sharing websites and applications such as YouTube, Instagram, Snapchat, Pinterest, and Snapfish.

(3) Blogs, micro-blogging, wikis, comments sections of news outlet websites, and other public forums.

(4) Any other form of social media that may be developed or emerge in the future that facilitates the collaboration and dissemination of information via the Internet.

D. "Posting" – the sharing of any information via the Internet through the use of any social media or during the course of any social networking and includes the sharing of written statements, video files, audio files, photographs, links to another posting, or any other communication regardless of format such as:

(1) Social networks such as MySpace, Facebook, Google, LinkedIn, and Twitter.

(2) Video, podcasts, and photo-sharing websites and applications such as YouTube, Instagram, Snapchat, Pinterest, and Snapfish.

(3) Blogs, micro-blogging, wikis, comments sections of news outlet websites, and other public forums.

(4) Any other form of social media that may be developed or emerge in the future that facilitates the collaboration and dissemination of information via the Internet.

21.2.2. GENERAL

A. The use of personal social media or social networking sites on duty is strictly prohibited. Members needing to utilize social media or social networking sites for duty purposes must receive departmental approval by completing an Internet Access Exemption Request (DTMB-0099) form.

B. Department members are reminded that their conduct while engaging in either professional or personal use of social media or social networking sites is subject to all other department rules and regulations as required by Official Order No. 1, including but not limited to, the Law Enforcement Code of Ethics, the department's Harassment Policy, the department's Code of Conduct, and the department's Information Technology Security Policy set forth in Section 21.3 below. As a result, members are prohibited from the following:

(1) Posting any material or information that demonstrates or infers obscene, immoral, or sexually explicit conduct or language while on duty, or which is done in association with or in the presence of any photographs or other depictions of any department uniforms, badges, patches, logos, shields, or marked vehicles or equipment.

(2) Posting any material that demonstrates a failure by a member to maintain a level of conduct in their personal and business affairs which is in keeping with the highest standards of the law enforcement profession. Members are reminded of their responsibility to conduct themselves at all times, both on and off duty, in a manner that will reflect favorably upon the department. Members shall avoid conduct unbecoming of a member which brings the department into disrepute or reflects discredit on the individual as a member of the department or that which impairs the efficiency of the department.

(3) Posting any statements, on or off duty, which show a reckless disregard for the truth.

(4) Posting images, acts, or statements that ridicule, malign, disparage, or otherwise express bias against any race, religion, or protected class of individuals identified in Official Order No. 1.

(5) Posting information gained by reason of their authority.

(6) Posting statements, speeches, appearances, endorsements, or materials that could reasonably be considered to represent the views or positions of the department without express authorization.

(7) Posting photographs or videos of official department training, activities, or work-related assignments.

(8) Posting any trademarked or copyrighted materials contrary to law.

C. This section does not apply to members who are re-posting or sharing news articles or information from the department's website or social networking sites, or to the posting or re-posting of photographs or videos of official department training, activities, or work related assignments not otherwise prohibited or deemed detrimental to the department, provided such postings do not interfere with satisfactory job performance.

D. Department members are reminded that violations of this social media policy, as with violations of any other departmental order, rule, policy, regulation or criminal law, shall result in discipline up to and including discharge.

E. Department members are reminded that the failure to report violations of this social media policy by other members which they observe, or which have been reported to them, or which they have knowledge, shall result in discipline up to and including discharge in the same manner as the failure to report other prohibited activities by another member.

F. All employees shall treat as confidential the official business of the department.

G. Members who become aware that an Internet news article or other posting contains factual errors shall notify their work site commander. Only the work site commander, in consultation with the Public Affairs Section, may post information in order to correct the record concerning misreported facts.

21.2.3. DEPARTMENTAL USE

A. Department members are reminded that they have no expectation of privacy or confidentiality with regard to any communications, posting, social networking, or use of social media on any department owned electronic devices or resources and the department reserves the right to monitor and log all network and system activity with or without notice.

B. The Public Affairs Section is responsible for setting Web and social media strategy for the department and maintains the department's official website and social media accounts.

C. Members shall not post derogatory comments or other comments that could be construed as official department views on any department website or social media site.

D. Work sites or members are not authorized to create or maintain websites or establish social media accounts on behalf of the department without the prior approval of the Public Affairs Section.

(1) All external department websites shall be developed on the www.michigan.gov platform unless prior approval has been granted by the Public Affairs Section.

(2) This section applies to department members who create websites or social media accounts outside of work that could reasonably be seen as official department sites.

(3) This section does not apply to department members using the Internet, social media, social networking, or websites for legitimate investigative purposes.

E. All department communication standards shall be applied to social media websites, as they do to print and website content. Department of Technology, Management and Budget (DTMB) policies and standards shall be applied to all department website and social media content.

21.2.4. PERSONAL USE

A. Members are free to express themselves as private citizens on social media sites to the degree that their postings do not impair working relationships, impede the performance of duties, impair discipline and harmony among co-workers, or negatively affect the public perception of the department. In order to prevent bringing the department into disrepute or negatively affecting the efficiency of the department, members shall use appropriate discretion in the use of references to the Michigan State Police so as not to discredit the department or its employees and ensure that information concerning official business is not released, either directly or indirectly, by a member.

B. Postings that contain information obtained through the employee's professional duties and responsibilities are not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department.

C. For safety and security reasons, members should not disclose their employment with the department, personal identifying information, or information that would tend to disclose the residence or location of themselves or their immediate family. For safety and security reasons, members shall not disclose another member's employment with the department, personal identifying information of another member, or information that would tend to disclose the residence or location of that member or that member's immediate family without that member's permission, unless that other member or the department has contemporaneously permitted such information to be released to and is generally accessible by the public via the Internet or social media (e.g., news stories, public announcements, press releases, etc.).

D. Department members are cautioned that communications made via the Internet, using social media or through social networking, may provide grounds for impeaching a member's credibility while under oath or in official proceedings. Postings that demonstrate a failure to exercise good judgment or a lack of personal accountability that are used to impeach a member or which discredits the department or another member in an official proceeding, or while the member is under oath, shall result in discipline.

21.3 INFORMATION TECHNOLOGY SECURITY POLICY

This section outlines the acceptable use of information technology resources. Members utilizing 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.

21.3.1. 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.

21.3.2. 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.

21.3.3. 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 work site 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. Work Station Controls

(1) At a minimum, all work stations 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 work site 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 work site.

(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 on a designated file server directory (H:\).

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 work site commander, the ISO, and the DTMB at 1-877-264-XXXX.

(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.

21.3.4. MANAGEMENT AND EMPLOYEE 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 work sites 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 staff under their command.

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

H. Employees 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.

21.3.5. 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.

21.3.6 COMPLIANCE WITH FBI CJIS SECURITY POLICY, MICHIGAN CJIS POLICY COUNCIL ACT AND CJIS ADMINISTRATIVE RULES

A. Data stored in any MSP 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.

21.4 REVISION RESPONSIBILITY

Responsibility for continuous review and revision of this Order lies with the Administrative Services Bureau, in cooperation with the Office of the Director (Human Resources Division).

DIRECTOR