BAY CITY DEPARTMENT OF PUBLIC SAFETY
BAY CITY, MICHIGAN

SECTION 1 - ADMINISTRATIVE — August 9, 2019
GENERAL ORDER — INDEX NO. 1.3

INFORMATION TECHNOLOGY

I. PURPOSE

The purpose of this policy is to assure that:

1. The use of city-provided IT resources is related to, or for the benefit of, the Bay City Department of Public Safety.

2. City-provided IT resources are used productively.

3. Disruptions to departmental activities, because of inappropriate use of city-provided IT resources, are avoided.

4. All employees are informed about confidentiality, privacy, and acceptable use of city-provided IT resources as defined in this policy.

II. USE OF CITY-PROVIDED INFORMATION TECHNOLOGY RESOURCES

The purpose of city-provided information technology (IT) resources (e.g., E-mail, electronic voice and video communication, facsimile, the Internet, cellular telephones, Records Management System, Lexis/Nexis and future technologies) is to support the Bay City Department of Public Safety in achieving its mission and goals. These resources are intended to assist in the efficient and effective day to day operations of the department, including collaboration and sharing/exchange of information within and between other police and fire agencies, other branches of government, social service agencies, etc. Some of these resources also provide public access to public information.

Effective use of city-provided IT resources is important to the Bay City Department of Public Safety. To help improve the effectiveness of your use of these resources, incidental and occasional personal use is permitted*, as long as such use does not:

- Interfere with existing rules or policies pertaining to the agency,
- Involve the disclosure of confidential information,

* Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does so to assist in such judgment by providing the enclosed guidelines. If you are unclear about the acceptable "personal" use of city-provided resources or wish to use the resource for what may be considered as a good cause, seek authorization from your respective supervisor.

- Involve the dissemination of public safety information/reports for non-law enforcement or fire operations purposes,
- Disrupt or distract the conduct of department business (e.g., due to volume or frequency),
- Involve solicitation,
- Involve a for-profit personal business activity,
- Have the potential to harm the department, or
- Involve illegal activities.

Note: Any resources used for personal use that incurs a cost must be reimbursed to the city

III. PRIVACY ISSUES AND LEGAL IMPLICATIONS

A city agency has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate city operational or management purposes. Do not transmit personal information about yourself or someone else using city-supplied IT resources without proper authorization. The confidentiality of such material cannot be guaranteed. E-mail and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a “record” and therefore are reproducible and subject to judicial use.

IV. UNACCEPTABLE USE OF I.T. RESOURCES

Any use of city-provided IT resources for inappropriate purposes, or in support of such activities, is prohibited (unless authorized through job responsibilities). The following list is currently considered unacceptable use of city-provided IT resources.

1. Illegal Use: Any use of city-provided IT resources for illegal purposes, or in support of such activities. Illegal activities shall be defined as any violation of local, state or federal laws.

2. Commercial Use: Any use for commercial purposes, product advertisements or “for profit” personal activity.

3. Sexually Explicit: Any sexually explicit use, whether visual or textual. You shall not view, transmit, retrieve, save, or print any electronic files which may be deemed as sexually explicit (Unless necessary for investigative purposes).

INFORMATION TECHNOLOGY

4. Religious or Political Lobbying: Any use for religious or political lobbying, such as using E-mail to circulate solicitations or advertisements.

5. Copyright Infringement: Duplicating, transmitting, or using software not in compliance with software license agreements. Unauthorized use of copyrighted materials or another person's original writings.

6. Unnecessary Use of IT Resources: Wasting IT resources by intentionally:

   - Placing a program in an endless loop;
   - Printing unnecessary amounts of paper;
   - Disrupting the use or performance of city-provided IT resources or any other computer system or network (for example, unauthorized world wide web pages, recurrent mass communications); or
   - Storing any information or software on city-provided IT resources which are not authorized by the agency.

7. Security Violations:

   - Accessing accounts within or outside the city's computers and communications facilities for which you are not authorized or do not have a business need.
   - Copying, disclosing, transferring, examining, renaming or changing information or programs belonging to another user unless you are given express permission to do so by the user responsible for the information or programs.
   - Violating the privacy of individual users by reading E-mail or private communications unless you are specifically authorized to maintain and support the system.
   - Representing yourself as someone else, fictional or real (unless doing so in the course of your duty).

8. Viruses: Knowingly or inadvertently spreading computer viruses. "Computer viruses" are programs that can destroy valuable programs and data. To reduce the risk of spreading computer viruses, do not import files from unknown or disreputable sources. If you obtain software or files from remote sources, follow proper procedures to check for viruses before use. You should adhere to any state agency-specific policy in this area.

9. Junk Mail: Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.

10. Confidential Information: Transmitting confidential information without using proper security. (Note: Use caution when sending classified information. Always display "CONFIDENTIAL' on the screen when sending classified information. Confirm that encryption has been enabled. Inform the recipient of the information's classification, their responsibility to keep private, and their responsibility to dispose of it in a secure manner at the end of its retention period.)

11. Unauthorized Sharing of Information: Providing access to or supplying information gained through privileged access to the Records Management System for anything other than a function of your job duties.

12. Unauthorized Printing of Reports from Outside Agencies: Printing police reports or other information accessed through the Records Management System which originated from departments, other than the Bay City Department of Public Safety, without permission from a supervisor.

V. WARNINGS/CORRECTIVE ACTIONS

Complaints or instances of unacceptable use brought to the attention of a supervisor shall be reviewed and investigated. Violators will be subject to corrective action and discipline, and may also be prosecuted under applicable state and federal statutes.

VI. RESPONSIBILITIES

1. Access only files, data and protected accounts that are your own, that are publicly available, or to which you have been given authorized access.

2. Use IT resources efficiently and productively. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, disk space, printer paper, or other IT resource.

3. Be responsible for the use of your accounts. Under no condition should you give your passwords to another person. Guard yourself against unauthorized access to your accounts by periodically changing your passwords.

4. Immediately report to a supervisor if you:

   - Receive or obtain information to which you are not entitled,
     (*Note: Also notify the owner or sender of such information)*
   - Become aware of breaches of security, or
   - Know of any inappropriate use of city-provided IT resources.

5. Seek the advice of your respective supervisor for any city-provided IT resource if you are in doubt concerning your authorization to access that resource.

6. Adhere to copyright law regarding use of software, information, and attributions of authorship. Upon the request of the agency, delete (from any computer) and return all city-provided software used for off-site work.

7. Conduct yourself as a representative of both the Department of Public Safety and the City of Bay City as a whole.

VII. OVERVIEW OF TECHNOLOGIES

The following are examples of technologies that this policy governs. As new technologies gain popularity and use, they, too, will be governed by this policy. This overview will increase understanding of the uniqueness of these technologies as they relate to creating electronic ‘records’. Each of these technologies creates an electronic record. This is what separates these from other forms of communications such as a telephone conversation. An electronic record is reproducible and therefore deserves special recognition.

A. EMAIL

Email is a major means of communication in city government, and it offers an efficient method of conducting city business. Email, as defined in this document, consists not only of the city-provided Email system, but also the act of sending and receiving Email through the Internet.

There are a number of characteristics that distinguish Email from the other means of communication, such as paper records, telephones, and information stored on electronic media such as diskettes. Awareness of these characteristics should guide your use of Email.

1. Backups. As part of standard computing and telecommunications practices to prevent loss of data, Email systems and the systems involved in the transmission and storage of Email messages usually are "backed up" on a routine basis. This process results in copying data such as the content of an Email message, onto storage media that may be retained for periods of time and in locations unknown to the sender or recipient of the message. The frequency and retention of backup copies vary from organization to organization. While it may be difficult and time consuming, it should be assumed backup copies of Email messages exist and can be retrieved, even though the sender or recipient has discarded his/her copy of a message.

2. Special Status. While password protecting your Email account is beyond usual measures taken to protect access to paper records and telephones, it does not confer a special status on Email records with respect to applicability of laws, policies, and practices.

3. Monitoring. In the course of their work, managers, network and computer operations personnel or system administrators may monitor the network or Email system. It should be assumed that the content of Email messages may be seen by these authorized individuals during the performance of their duties.

4. Forgeries. No system of communication is completely secure, including Email. Just as with paper communications, an Email message can be forged, and it can be distributed beyond the address list originally defined by its author.

5. Legal Implications. Email and other electronic files may be accessible through the discovery process in the event of litigation.

B. FACSIMILE (FAX)

The same rules governing acceptable use of other city-provided IT resources also apply to the use of fax technology. The faxed message may be "backed up" onto other storage media. As with other technologies, the content of faxed messages may be seen by authorized individuals during the performance of their duties.

Use of fax technology does not always require a password for access. Recipients should not assume that the sender is always as reported. A fax should always be perceived as non-private communication method. Remember, anyone at the other end may read your fax.

C. INTERNET

The Internet provides the ability to communicate, collaborate with others and access information throughout the world. However, there is little in the way of hierarchy or control of the information available. Increased access to computers and people all over the world also brings the availability of controversial material that may not be considered of value to an individual or the city.

Even if you are able to encrypt your data, anything you transmit over the internet is subject to interception, reading, and copying by other people. This includes Email, personal information and passwords that are transmitted when you log into the account or log into another computer.

D. VOICEMAIL

Voicemail is a means of communication that is in and of itself unique. It is similar to a telephone conversation, but it creates a "record". This should always be remembered by anyone using this technology. By the very definition of a record, the sender must remember that the message can also be saved, replayed, and shared with others that the sender did not intend. It also can be used in litigation. The same rules of password protection and confidentiality that concern other technologies also apply here.

E. CELLULAR TELEPHONES

1. Initiating outgoing communications while driving is prohibited unless necessary in the performance of duties.

2. Receiving incoming calls, messages, etc., while operating a motor vehicle shall be permitted only if the operator determines it is safe and that operation can safely be terminated within 60 seconds unless it is necessary in the performance of duties to be longer.

3. Lengthy or non-emergency communications may be completed after pulling to the side of the road, coming to a stop, and putting the vehicle in park.

4. Incidental and occasional use of personal cellular telephones during working hours is permitted, as long as such use does not:

   - Interfere with existing department rules or policies
   - Disrupt or distract the conduct of department business (e.g., due to volume or frequency)
   - Involve solicitation
   - Involve a for-profit personal business activity
   - Have the potential to harm the department
   - Involve illegal activities

5. Where there is a dispute over the circumstances or situations for use, the personal cellular telephone is prohibited.

F. MDT (MOBILE DATA TERMINALS)

All use of the Laptop Computer system for LEIN/NCIC inquiries shall be governed by the current policies of the LEIN Council, which adopted NCIC policy regarding training of LEIN/NCIC users. Personnel will abide by FBI and Criminal Justice Information Services policies and user agreements.

The Bay City Department of Public Safety provides MDT’s for the conduct of law enforcement business and record keeping. The use of MDT’s for personal purposes and the use of personally purchased software, information storage discs, or PCMCIA cards is prohibited unless advance approval is granted by the Public Safety Director or their designee. Users are prohibited from introducing, modifying or altering authorized software or related components.

All MDT transactions are stored electronically and are retrievable from the system. The Bay City Department of Public Safety reserves the right to conduct random audits for violations of this policy and all applicable laws. Employees in violation shall be subject to disciplinary action.

1. Security/Access

a. MDTs must remain within the control of an authorized user or be kept in a locked vehicle or within the Law Enforcement Center in a secure area.

b. Access to MDTs will be restricted to those with the credentials to sign-on to the MDT and who have been trained in its use.

2. Training

a. All law enforcement personnel will receive training in the operation/use of the MDT during the administration phase of the FTO program and anytime the MDT is updated to a different or newer model.

3. General Issues

a. Care is to be taken to eliminate foreign objects from damaging the MDT equipment. The MDT and docking station are not to be used as food or beverage trays.

b. MDT messages are to be of professional nature. MDT users must not transmit any material that may discredit or bring disrespect upon the department

c. Information transmitted or received through the MDT's shall be considered confidential. Unless specifically authorized by standard operation procedures, personnel will not disseminate information to any unauthorized persons.

d. MDT's that are damaged or inoperative shall be reported to your immediate supervisor in a timely manner.

4. Specific User Issues

a. Officers using the MDT shall do so signed on under their own user ID and Password.

1. Passwords must be at least eight (8) characters in length and contain three out of the following four categories:
   a. Uppercase letter
   b. Lowercase letter
   c. Number
   d. Symbol

2. Passwords must be changed when the MDT prompts the user to do so.

b. Officers shall log off the MDT system at the conclusion of their shift.

c. Officers will regularly check to ensure that the MDT is charging.

5. Safety Issues

a. All pertinent information shall be voice broadcast unless doing so will compromise officer safety.

b. All incidents requiring an emergency response shall be dispatched verbally.

c. MDT's shall not be used by the driver of the vehicle in motion unless necessary in the performance of duties.

1. RECORDS MANAGEMENT SYSTEM

1. The Department of Public Safety utilizes a Records Management System (RMS) to complete police reports and manage various police records. The department has used and will use various vendors to provide the necessary software. These systems all involve several different law enforcement agencies which allows all users on the network to have access to information and police reports from each of the agencies using the system. With this access is the responsibility to respect the information belonging to other departments. If anyone wishes to utilize information on the system that originated from another agency, it must only be used for legitimate law enforcement business. Additionally, users may print reports or information originating from police agencies other than the Bay City Department of Public Safety only after a permission is granted from a supervisor.

2. All users should be aware that **everything** done on a RMS is recorded and can be accessed by the system administrators at any time and for any reason. This is all tracked based on the individual signed onto the system. Users are responsible for keeping their password private for

this reason. The system also saves every "version" of anything completed within it. For example, if someone completes a report and then makes corrections at a later time, both the original version and corrected version can be accessed by system administrators.

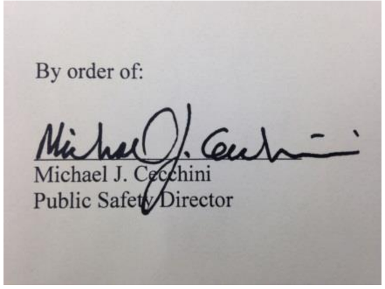
3. The RMS that the department utilizes will have all data stored at a site separate from the department. This data will also be backed-up at a separate physical location from the main data storage center.

VIII. LEXIS / NEXIS

Lexis / Nexis software is an investigative tool utilized by public safety personnel to assist them with investigations. This software provides both public records and confidential Criminal Justice Information (CJI). Any access to CJI shall comply with General Order 1.27 – Criminal Justice Information System Security. Lexis / Nexis is not to be used for personal reasons and may only be used in the performance of official duties.

IX. EMERGING TECHNOLOGIES

This policy does not address the specific details of technologies that are yet to be invented or implemented within city government. This policy should be sufficient to allow you to determine the acceptable use of any new or emerging technology. If you have any questions regarding appropriate use of a particular technology not specifically covered in this policy, please contact your respective supervisor.



By order of:

Michael J. Cecchini

Michael J. Cecchini
Public Safety Director