St. Joseph, Missouri Police Department

DIRECTIVE TYPE: GENERAL ORDER		INDEX NUMBER: GO1202
SUBJECT: AGENCY/SYSTEM SECURITY		
ISSUE DATE: April 23, 2012	REVISIONS: 8/8/12, 6/7/18	AMENDS/RESCINDS: N/A
REVISIONS CONTINUED:		DISTRIBUTION: A (All)

I. Purpose

The purpose of this policy is to establish security access guidelines for the use of the St. Joseph Police Department Law Enforcement Center and the Police Department's computer system(s).

II. Policy

It is the policy of the St. Joseph Police Department to use security measures to protect the confidentiality, integrity and availability of information handled by computers and communications systems. Physical security, logical security and change management work to ensure the reliability of the information technology assets and computer resources.

III. Procedure

A. Computer System Access

1. **Adding a user to the St. Joseph Police Department system(s):**
   Access to all Police Department systems must be restricted to users with a legitimate business need. In order for a user to gain access privileges, his or her supervisor must send necessary information to the Public Safety Network Administrator (PSNA). The email must include:
   - **a.** The employee's name;
   - **b.** The employee's date of birth;
   - **c.** The employee's social security number;
   - **d.** Whether the employee is a new hire or assigned to a new position and needs new privileges;
   - **e.** The employee's division and job title

   Supervisors must promptly report all significant changes in end user duties or employment status to the PSNA.
2. **Deleting a user from the St. Joseph Police Department system(s):**

Access must be terminated regardless of the reason for the end of the business relationship. Supervisors must notify the PSNA and the Chief's Administrative Assistant, along with the IT Department at City Hall, when a user leaves the St. Joseph Police Department and specify:

a. The user's name;
b. The user's department;
c. The user's last day;
d. Whether the user has system access

If possible, notification should be made prior to the user's separation from the Police Department. In cases where the separation between the user and the Police Department are hostile, the PSNA must be notified immediately by telephone so that access can be promptly and completely revoked. Supervisors will be notified by the PSNA when their request has been completed.

B. User Virus Protection Responsibilities

1. Electronic mail attachments

Although the email server checks all email attachments for viruses before delivery, users must exercise caution when opening unknown email attachments. Users must not open or execute email attachments unless they originate from a trusted party.

Users should also be advised that some viruses propagate, or copy and send themselves, through an infected system's email address book. This means that an attachment from a trusted party or friend potentially could contain a virus. Users are urged to be alert and not to open or execute attachments that seem suspicious. If a user becomes aware of a virus, they should immediately contact the Public Safety Network Administrator and the Information Technology Department at City Hall.

2. External disks, peripheral devices and software

Because viruses that can harbor malicious programs can also be spread via computer disks and innocuous-seeming software, users must not use personal disks or peripheral devices with the St. Joseph Police Department computers or install software that has not been approved by the PSNA/IT Department.

C. Physical Security

Access to the St. Joseph Police Department, beyond the public lobby, must be physically restricted.

1. No "piggybacking" through controlled doors

Authorized individuals must not permit unknown or unauthorized persons to circumvent door security controls by allowing them to follow the authorized individual through an entrance to a restricted area.

2. Escorts required for all visitors

Visitors to the St. Joseph Police Department Law Enforcement Center must be escorted at all times by an authorized employee. The escort is required as soon as the visitor enters a controlled area and until that visitor goes outside the controlled area. Visitors requiring an escort include but are not limited to: customers, third party representatives, former employees, employee family

members or friends, equipment repair contractors, package delivery personnel, vending machine personnel and any other non-employee.

Unescorted visitors in a restricted area must be politely but firmly questioned about their purpose in the building. They must be escorted back to the lobby or to their contact person.

3. **Visitor log**

   The St. Joseph Police Department shall maintain visitor access records to the physically secure areas of the department. The department member will check the visitor's ID, unless already familiar with the visitor. The log shall include:

   a. Name of the visitor (ID checked)
   b. Date of access
   c. Time of entry and departure
   d. Purpose of visit
   e. Name of person visited

   The log shall be maintained for a minimum of one year.

D. Department-Issued Equipment Control

The St. Joseph Police Department has enacted the following measures and actions that users must follow in order to safeguard equipment and information on the department's system and resources.

1. **Password Protected Screensavers**

   In order to prevent use of workstations by unauthorized parties, users must activate password protected screensavers whenever they are away from their workstations. Screensavers also must activate automatically after fifteen minutes of inactivity.

   The system will display a login prompt when the keyboard or mouse is activated. The user must re-enter his/her username and password in order to regain access to the system. Under no circumstances are individuals allowed to change this setting.

2. **Inactivity Timeout**

   If there has been no activity in Aegis for 30 minutes, the system will automatically blank the screen. Users must re-enter their username and password in order to re-activate the system.

E. Passwords

Members shall choose passwords that are unique and difficult to guess. They will choose new passwords when prompted to do so by the system. The following attributes to user passwords shall be observed:

1. Your password must be 8-15 characters in length;
2. Your password must not be identical to the previous ten (10) passwords;
3. Your password is case-sensitive;
4. You must use a number(s) in your password;
5. You must use a letter(s) in your password;
6. You must use a symbol(s);
7. You will have five login attempts; and
8. Your password will expire after 90 days.

F. Information Security Controls

Employees must not test, attempt to compromise or exploit vulnerabilities or deficiencies in information systems security. Users are required to notify the Public Safety Network Administrator if they discover an information security incident.

G. CJI Media Security

1. Media Types

Digital Media - Electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Physical Media - Printed documents, printed imagery, etc.

2. Dissemination

Dissemination to another agency is authorized if:

- **a.** The other agency is an authorized recipient of such information and is being serviced by the accessing agency; or
- **b.** The other agency has a non-terminal agency agreement with the St. Joseph Police Department and is performing personnel and appointment functions for criminal justice applicants.

3. Media Transport

Digital and physical media containing CJI shall be protected and controlled during transport (physically moved from one location to another) outside of controlled areas to prevent inadvertent or inappropriate disclosure and use. Only authorized personnel will transport such media and only in conjunction with their official duties.

4. Digital and Physical Media During Transport

Personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

- **a.** Use of privacy statements in electronic and paper documents.
- **b.** Limiting the collection, disclosure, sharing and use of CJI.
- **c.** Limiting CJI access to only those people or roles that require access.
- **d.** Maintaining continuous physical control of the media until dissemination to another authorized agency or disposal.
- **e.** Restricting the viewing or accessing of digital or physical CJI to authorized personnel in a physically secure location.
- **f.** Packaging hard copy printouts in such a way as to not have any CJI information viewable.
- **g.** Encrypting digital media when possible.

5. Mailing or Shipping

Personnel shall document their mailing or shipping procedures and only release to authorized individuals. Personnel WILL NOT MARK THE PACKAGE TO BE MAILED AS "CONFIDENTIAL". All packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

6. Disposal of Physical Media

Physical media shall be securely disposed of or destroyed when no longer required, **by shredding or incineration**. Disposal or destruction shall be witnessed or carried out by authorized personnel.

H. System Access Control

All users on the St. Joseph Police Department must have a unique ID and password. Sharing IDs and passwords is prohibited. Each granted user ID must be unique and permanent, connected solely with the user to whom it has been assigned. User IDs are not to be re-used, even if the original user no longer has any connections to the St. Joseph Police Department.

I. Remote Access

Remote access into the department's network is limited to personnel who have a legitimate business need; the Chief of Police and Public Safety Network Administrator approval is required. Users must submit a completed request that bears their manager or supervisor's approval to the PSNA in order to obtain remote access privileges.

J. Misuse of Official Information

In the absence of specific direction from the policies and procedures in this policy, information technology requirements must meet, at a minimum, the guidelines contained in the St. Joseph Police Department General Orders, Special Orders, the City of St. Joseph Personnel Manual and MO State Statute 576.050. That statute states, "a person commits the crime of misuse of official information if he or she knowingly or recklessly obtains or discloses information from the Missouri uniform law enforcement system (MULES) or the National Crime Information Center System (NCIC), or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job. Misuse of official information is a class A misdemeanor."

K. Security Awareness Training

Basic security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. (See CJIS Security Policy Area 2: Security Awareness Training)

L. Background Checks

1. **New Operators**

   The TAA (Terminal Agency Administrator) must conduct a state of residence and nationwide background screening utilizing fingerprint cards on any new operators, or employees or contractors with access to CJIS devices or information. One fingerprint card must be submitted within 30 days of an employee's date of hire. Fingerprints shall be submitted on applicant fingerprint cards, with the phrase 'criminal justice employment' as the reason for printing.

   In the period before results of the fingerprint check are returned, employees may be granted provisional access based on a check by name, date of birth, and social security number. The following classifications will be given to authorized parties having access to CJI contained in or derived from MSHP CJIS network.

a. **Physical Access Only:** These parties have been authorized for physical access to paper files, printers, terminals, PCs, network components and other data contained within a physically secure location. This party will not be provisioned with a user ID and password to any system containing CJI to include local systems or MSHP systems. (Example: Maintenance, cleaning staff, clerks or others without a documented need for logical access.)
b. **Logical Static Data Access Only:** These parties have been authorized for logical access to local networks/systems containing CJI but are not authorized for direct access to CJI inquires or data manipulation. This party will be provisioned for access to the necessary network and local system resources necessary to complete their functions but will not be provisioned with direct access to any criminal justice information sharing system. (Example: IT Staff, other employees with a need to access systems containing CJI but not performing a criminal justice function and/or lacking a documented need for direct access to law enforcement information sharing systems.
c. **Logical Limited Data Access:** These parties have been authorized for logical access to local networks, systems containing CJI as well as provisioned for limited direct access to criminal justice information sharing systems. This limited access shall be restricted to only those functions needed to perform a specific task. Any function which would be classified as not meeting the definition of a criminal justice or administration of criminal justice function shall be limited to access only to transactions aimed at the testing and diagnosis of system functions and shall not allow for direct inquiry to or data manipulation of CJI. (Example Third Party Vendor, programmer, help-desk technician other parties with a need to access systems/networks containing CJI and direct access to a criminal justice information sharing system but not performing a criminal justice function or a very limited role in a criminal justice function).
d. **Logical Direct Data Access:** These parties have been authorized for logical access to local network, systems containing CJI as well as provisioned for direct access to criminal justice information sharing systems with the access level appropriate for their assigned role. These operators must be performing a criminal justice function and should, be provisioned for the lowest possible access necessary to fulfill their role.

2. **Fingerprint Checks**

All personnel with physical or logical access to CJI must have a fingerprint based background check to include:

a. **All Personnel Employed by the Department:**
   1) All employees who have direct MULES terminal access to criminal justice information OR unsupervised access to a secure MULES terminal or printer must have a fingerprint-based background check within thirty (30) days of assignment

(Examples: Police officers, dispatchers, and administrative/support staff employed by the criminal justice agency). The "Reason Fingerprinted" field on the fingerprint card must state: **CRIMINAL JUSTICE EMPLOYMENT**.

b. All Personnel Providing Services to the Criminal Justice Agency:

1) All employees who have direct MULES terminal access to criminal justice information OR unsupervised access to a secure MULES terminal or printer AND provide services to the department must have a fingerprint-based background check within thirty (30) days of assignment (EXAMPLES: Cleaning staff, administrative staff, maintenance staff, IT staff employed by the city).

2) The "Reason Fingerprinted" field on the fingerprint card must state: **NCJA ACCESS TO TERMINAL AREA**.

c. All Personnel Working Under Contract with the Department

1) All non-employee contractors of the department who have direct MULES terminal access to criminal justice information or unsupervised access to a secure MULES terminal or printer must have a fingerprint based background check within thirty (30) days of assignment (EXAMPLES: IT staff, cleaning staff, maintenance staff, and contracted support staff).

2) The "Reason Fingerprinted" field on the fingerprint card MUST state: **CONTRACTOR**.

3. Duty to Report

All arrests, convictions and disposition information discovered via criminal history record checks shall be reported to the MSHP ISU (Information Security Unit), by the department. The department will also inform the ISU of any felony arrest or charge not reported in the criminal history record systems maintained by MSHP CJIS, such as an arrest which appears in a local or other record system.

4. Miscellaneous Personnel

Miscellaneous Personnel who have received appropriate security awareness training may escort non-operator employees and visitors to areas designated as a physically secure location. All visitors to the physically secure location must provide identification and sign a visitor log. If visitors or unauthorized employees or contractors are under the direct supervision of a security awareness trained employee while they are present, a background screening is not required.

Persons not authorized for CJI access may be escorted into areas designated secure by the employing or supervising agency, provided access to terminals, by sight or otherwise, is not possible. (For example, if a whole floor is a secure area, but only one room houses the terminals, access whether escorted or unescorted to that room would be disallowed to a person to whom CJI access had been denied.)

An arrest for which the final disposition is known to be other than a conviction or suspended imposition/execution of sentence will not by itself be

used as grounds for denial of access to CJI. However, access to CJI may be denied based on an arrest record, taking into account all relevant circumstances, including the conduct underlying the arrest or prosecution, if a reasonable basis to assess that conduct is available.

Outstanding warrants must be satisfied before access to CJI is allowed, after which the employing or supervising agency shall refer to the guidelines on pending or resolved charges, as applicable. If the employing or supervising agency demonstrates to the CSO that the warrant is probably not valid or not associated with the person seeking access, access may be granted during the pendency of the warrant, at the CSO's discretion.

Employees/Contractors who have provided notification of their decision to resign, or who are the subject of disciplinary action of any kind, may present a special risk situation. The TAA/LASO should consider reviewing the access privileges of such employees.

5. **Access when Felony Record is Found:**
   Any reported felony conviction will result in a denial of access to CJI.
   Persons seeking initial access to CJI or with previously-granted access to CJI who are charged with or arrested for a felony shall have access suspended immediately by the department.
6. **Access when Misdemeanor Record is Found:**
   A misdemeanor conviction will not be grounds for denial of access CJI. Access to CJI will be determined by the CSO and the department TAC. Access by a person charged with or arrested for a misdemeanor after the time of fingerprinting will be determined by the CSO and the department TAC during the pendency of the charge or arrest.
   - **a.** If access is allowed to such an employee, that employee should in all instances be closely monitored by the department to determine what level of access is appropriate prior to resolution of the charge or arrest.
   - **b.** If such an employee is charged with or arrested for a misdemeanor act of domestic violence, or any other misdemeanor offense for which access to personal identification and location information by the accused could be problematic, and access is allowed, the employee's access shall be closely supervised.
7. **Change in Status**
   The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.)
   The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

L. Incident Handling/Response

The department shall have an established security incident response plan. A Security incident is defined as:

1. An event which includes an act of violating an explicit or implicit security policy. Security incidents may include, but are not limited to:
   - **a.** Attempts, failed or successful, to gain unauthorized access to a protected system or its data;
   - **b.** Unwanted disruption or denial of service;

c. Unauthorized use of the system for processing or storage of data;
d. Changes to system hardware, firmware, or software without the owner's knowledge or consent;
e. Misuse of official information covered in RSMO 576.050; and/or
f. Theft or loss of devices containing CJI

2. The department's response plan shall include:
a. Notification of the TAC or LASO by users reporting incidents;
b. Handling procedures to document facts and findings surrounding the event; and
c. Notifying the MSHP Security Unit within 24 hours of the incident discovery for all security incidents including misuse.

_____
Chris Connally, Chief of Police

_____
Date