320.03
COMPUTER DATA SECURITY SYSTEMS
02-28-17

PURPOSE

The purpose of this order is to provide guidelines for the security of electronic information and computer equipment (hardware and software).

POLICY

It shall be the policy of the Sacramento Police Department to provide for the security and integrity of computerized systems and documents accessed by employees or authorized persons acting as agents of the Department.

PROCEDURE

A. DEFINITIONS
   1. COMPUTER SYSTEM - All computer hardware (attached or not attached to the Department Network), software, removable media and resources owned, leased, rented, or licensed by the Sacramento Police Department that are provided to Department employees for official use.
   2. HARDWARE - Shall include, but is not limited to, computers, computer terminals, network equipment, computer peripheral equipment, or any other tangible related devices generally understood to comprise hardware.
   3. SOFTWARE - Shall include, but is not limited to, a collection of computer programs, procedures, and documentation that perform tasks on a computer system. This does not include files created by individual users using software.
   4. REMOVABLE MEDIA - Storage media which can be removed from its reader device, conferring portability on the data it carries. Removable media shall include, but is not limited to hard drives, flash drives, CDs, CD-Rs, DVD-Rs, memory sticks, and floppy discs.
   5. ELECTRONIC FILES - Any temporary or permanent electronic document, information, or data residing or located, in whole or in part, on the Department computer system, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, or messages.
   6. NETWORK - The interconnected system of computers within the Department that allows various computing systems to communicate with each other.

B. PUBLIC SAFETY INFORMATION TECHNOLOGY (PSIT)
   1. PSIT shall
      a. Ensure electronic information and computer systems are used for official business purposes only and in compliance with Department policies and procedures and any pertinent Federal, State, and local laws.
      b. Ensure proper disposition and security of Departmental electronic information, records, and documents.
      c. Be solely responsible for the movement and installation of all Department computer equipment.
      d. Approve all computer-related purchases that are submitted to the Fiscal Division for procurement.
   2. PSIT shall be responsible for
      a. Entry, update, and/or deletion of employee network access and attributes when employees are assigned or move from their assigned areas.
      b. Initial and/or temporary updating of access code passwords.
      c. Assisting the Internal Affairs Division (IAD) regarding computer system violations.
   3. PSIT shall observe and report on the physical security of computer equipment. They shall do research and make recommendations on computer security changes, uses, or new applications.

C. RECORDS SECURITY
   1. Each office/division shall establish procedures for the storage of confidential electronic media materials. NOTE: All procedures shall be approved by the PSIT Manager prior to implementation.
   2. Internal Affairs Division (IAD) reports and disciplinary actions shall be stored on a dedicated secured server accessible only by IAD and, when permissible, PSIT.

a. Personnel preparing confidential personnel material shall submit removable media with the hard copy and original notes to the originator of the material when preparation is complete.
b. Backup copies of confidential non-personnel material shall be secured in the appropriate division supervisors' office in a manner to maintain data integrity and security.

3. The only information authorized to be stored on Department computer systems shall be
   a. Department approved software.
   b. Authorized software created by City/Department employees.
   c. Electronic files commonly used by Department personnel.
   d. Non-confidential documents/databases.
   NOTE: Exceptions shall be approved by the appropriate Division Commander.
4. When using removable media employees shall
   a. Only use removable media that has been approved by PSIT for departmental work.
   b. Ensure that all departmental materials stored on removable media is password protected.
5. Employees and volunteers shall
   a. Complete an Employee Computer Security Acknowledgement form (SPD 214) before receiving access to data.
   b. Protect their assigned password and restrict it to their own official use.
   c. Periodically change their assigned password to protect its confidentiality when prompted to do so.
6. Employees and volunteers shall not
   a. Use another employee's password or attempt to access other employees' accounts that are password protected unless otherwise authorized.
   b. Access criminal history files for pre-employment, licensing, or certification purposes, except as provided for by law.
   c. Access any computer databases or manual records for other than law enforcement purposes.
   d. Access computer databases on themselves or others for training or any other purposes.
   e. Access, print, or reproduce a confidential record on any employee for other than law enforcement purposes without supervisory authorization.
   f. Store personal files or files of a non-business nature on Department-issued computers or removable media.
7. All electronic files stored on Department computers systems are subject to search.
8. Employees or volunteers misusing any computer system or manual records information are subject to criminal prosecution as well as Departmental disciplinary action.

D. <u>ACCESS TO PUBLIC SAFETY COMPUTERS AND TELECOMMUNICATION ROOMS</u>

1. The Department is mandated by the California Department of Justice (DOJ) to prevent unauthorized access to confidential police information.
2. To prevent unauthorized access, Department employees shall
   a. Maintain physical security of all computer rooms, radio room, and telecommunication closets.
   b. Secure all CLETS, DMV, NCIC and HIPPA information that is accessible through communication equipment and Department servers.
3. In compliance with FBI and DOJ regulations, all non-law enforcement employees/vendors shall not be given access to areas where confidential information is accessible/stored unless escorted by PSIT.
4. All non-law enforcement employees and vendors requiring access to these areas shall contact the PSIT Help Desk during normal working hours to schedule an appointment. PSIT shall provide access to these areas and escort employees and vendors while the work is being performed.
   NOTE: PSIT requires two (2) business days advanced notification for appointments.
5. For access after business hours, weekends, or holidays, please contact the on-duty Communications Center Supervisor. The supervisor shall immediately contact the on-call IT support specialist.

E. <u>UNAUTHORIZED USE</u>

All Computer Systems not issued by PSIT shall not be attached to the Department's network without prior authorization from PSIT.

F. DATA ACCESS THREAT RESPONSE

1. All Suspected threats to the Department's information systems shall be immediately reported to the PSIT Manager and the Office Chief (or designee).
2. The PSIT Manager shall consult with Incident Response Team to assess the threat and determine a level of response.
   a. THREAT LEVEL 1 - One instance of potentially unfriendly activity (e.g., unauthorized telnet, port scan, corrected virus detection, unexpected performance peak, etc.). Level 1 type incident occurring against systems storing confidential or sensitive data or originating from unauthorized internal systems is classified as a Level 2.
   b. THREAT LEVEL 2 - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.
   c. THREAT LEVEL 3 - Serious attempt or actual breach of security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.
3. After the PSIT manager has determined the "threat level", he/she shall:
   a. Identify which resources (both internal and external) are at risk.
   b. Identify which harmful processes are currently running on resources that have been identified as at risk.
   c. Determine whether the resources at risk (hardware, software, etc.) require physical or logical removal.
   d. Notify appropriate agency to include, but not limited to, the FBI, DOJ or other Allied Law Enforcement Agencies.
4. The PSIT Incident Response Team shall immediately remove or isolate (either physically or logically) any resources that pose a significant threat to the continuity of the business. Resources that may require physical or logical removal or isolation may include, but are not limited to, the following:
   a. Firewalls.
   b. Routers and switches.
   c. Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS).
   d. Any enterprise-wide applications (CRM systems, etc.).
   e. Remote access.
   f. Point-to-point secure data transmission methods used for data traversing on the network.
   g. Wireless networking or networks.
   h. Authentication servers (RADIUS).
   i. Web servers.
   j. Proxy servers.
   k. File servers.
   l. Email servers.
   m. DNS servers.
   n. Operating systems.
   o. Databases.
   p. Applications.

G. POTENTIAL COMPROMISE OF INFORMATION

1. When a data breach has been suspected, the PSIT manager shall facilitate an investigation of the suspected theft of account information and make proper notifications.
2. To facilitate an investigation, the PSIT Incident Response Team shall
   a. Log all actions taken.
   b. Utilize chain of custody techniques during all transfers of equipment and information related to the incident.

c. Not access or alter compromised systems (e.g., do not log on or change passwords).

d. Not turn off the compromised machine, but instead isolate compromised systems from the network (e.g., unplug the network cable, deactivate switch port, isolate to contained environment isolated VLAN). To preserve the evidence for a forensic investigation, it is extremely important to not access the system.