SAN DIEGO POLICE DEPARTMENT
PROCEDURE

DATE:	DECEMBER 18, 2020
NUMBER:	1.45 - ADMINISTRATION
SUBJECT:	USE OF CITY/DEPARTMENT COMPUTER SYSTEMS
RELATED POLICY:	1.45
ORIGINATING DIVISION:	INFORMATION SERVICES
NEW PROCEDURE:	☐
PROCEDURAL CHANGE:	■ MINOR CHANGES
SUPERSEDES:	DP 2.14 – 02/15/2017

NEW

I. PURPOSE

This Department procedure establishes guidelines on the use of Police Department computers and systems by Department members. This procedure is based upon City Administrative Regulations 90.62, 90.63, 90.64, 90.66, Information Security Standards and Guidelines, Data Loss Prevention System Standards and Guidelines and Department Policy 1.45.

II. SCOPE

This procedure applies to all members of the Department.

III. DEFINITIONS

A. Computer Systems – all City, County, state, and national computer systems that can be accessed through established City/County telecommunications networks. These include, but are not limited to:

1. Automated Regional Justice Information System (ARJIS) – regional system that includes, but is not limited to, crime, adult arrest, juvenile contact, pawn slip, field interview, misdemeanor citation, traffic accident, and traffic citation information.

2. The California Law Enforcement Telecommunications System (CLETS) – state-wide system accessed via San Diego County's SUN message switch.

3. The County Computer System – County-wide system that includes, but is not limited to, local criminal history information, County jail booking information, City Attorney, District Attorney, courts, and probation information.

4. National Crime Information Center (NCIC) – nationwide system that includes information similar to CLETS.

NEW

5. Any internal San Diego Police Department or City hosted application used for storage and retrieval of information collected by Department personnel.

B. Law Enforcement Purposes – the prevention, detection and control of crime; the identification, location and apprehension of criminals; and all other related functions that are the responsibility of the Department.

C. Local Area Network (LAN) – a network of communication lines and devices that provide central access to computer systems and applications.

D. Personal Identifying Information – sensitive personal identifying information, as defined in A.R. 90.64, including an individual's social security number, date of birth, driver's license number, credit card number, bank account number, health insurance number, home/personal address, telephone number, password, and passport number.

IV. GENERAL PROCEDURES

A. All uses of Department computer equipment, telephone and voice mail systems, electronic systems, and electronic data, including e-mail and the Internet, are limited to work-related purposes only. Use of e-mail and the Internet is provided as a means of efficient and effective communications, as a tool to obtain specific data pertinent to Department business, and for other purposes that benefit the Department. (See City Administrative Regulation 90.62, Electronic Mail and Internet Use, for further information.)

B. When using the City's e-mail system or the Internet to communicate with others external to the City organization, the user shall recognize that he/she is representing the City of San Diego and the San Diego Police Department. Therefore, communication must be in a business-like manner and users must ensure that the communication is not in conflict with City policies.

C. Use of e-mail or the Internet in any way to facilitate the conduct of a private commercial purpose is strictly forbidden.

D. All records containing information about suspects, victims, or witness that are contained in Department systems will be used only for purposes directly related to Department business, must be used for law enforcement purposes only, and must strictly follow Department and California State Department of Justice (DOJ) policy related information release. (See Department Procedure 1.26, Access and Release of Criminal Records, for further information.)

E. Members must not use facsimile (fax) machines, electronic mail, or any other electronic communications systems owned by the Department for the distribution of unsolicited material.

F. Users must not attach personally-owned computer hardware, software, or computer peripherals to any Department-owned computer system or network without the approval of the Chief of Police and the Department's Information Services Program Manager.

G. Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users, except by authorized Information Services Division/Data Systems staff when required to resolve technical problems.

H. Transmitting confidential, sensitive, or privileged City/Department information to unauthorized persons or organizations via e-mail or the Internet is prohibited.

I. Department members are not to change the configuration of any Department laptop or desktop computer. These are configured and maintained by Information Services Division/Data Systems staff.

J. Electronic Mail Systems

1. Every member will be assigned a Department e-mail account. External mail systems (e.g., Hot Mail, Yahoo mail) are not authorized for use on Department systems unless the access is work related.

2. Department-related business matters should be conducted on the Department's e-mail system. Under no circumstances should matters relating to criminal history, crime cases, personnel, or other sensitive Department-related matters be sent to and from personal e-mail systems.

3. Members must not use an electronic mail account assigned to another individual to either send or receive messages.

4. Transmission of any material in violation of Federal or State laws or regulations and City and/or Department policy and procedures is prohibited.

NEW

5. Members shall not e-mail personal identifying information via the Internet. In the event that personal identifying information must be sent for business purposes to outside recipients, the information must be sent via encrypted email or an approved cloud service platform.

6. Any improper use of e-mail, including, but not limited to the following, is unlawful and strictly prohibited:

   a. Theft and/or forgery (or attempted forgery) of e-mail messages or electronic documents;

   b. Reading, deleting, copying, or modifying of e-mail of other users;

   c. Any attempts at sending unsolicited junk mail, for-profit messages, chain letters, or any mass mailing of a non-work related nature.

7. Electronic mail messages or attachments, containing any derogatory or suggestive materials based on a person's race, color, sex, religion, national origin, age, marital status, ancestry, medical condition, pregnancy, disability, or sexual orientation may be considered harassment under Department Procedure 5.03, Equal Employment Opportunity. Members must not create or forward externally-provided electronic mail messages, which contain these materials, except as necessary in the performance of duty.

NEW

8. The Department employs automatic electronic mail content scanning tools to identify selected keywords, file types, and other information to ensure that users restrict their communications to Department business matters.

9. All messages sent by electronic mail are the property of the Department. The Department reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. The Department may also disclose electronic mail messages for official purposes without prior notice to the members who may have sent or received such messages.

10. Automatic forwarding of e-mail to addresses outside of the City's network is not allowed.

11. City issued or personally owned mobile devices used by members to access Department e-mail must abide by security standards as defined in AR 90.66.

K. Internet Connections

1. Users may access the Internet for City business purposes only; the Internet may not be used for personal purposes as stipulated by City Administrative Regulation 90.62, Electronic Mail and Internet Use.

2. Department members must not access games, chat rooms, pornography, auctions, and similar sites, except for Department business purposes, and only then with commanding officer approval.

3. All users of the Internet should be aware that the Department will create a detailed audit log reflecting activity, which may be used for disciplinary purposes.

4. The City/Department requires full compliance with software vendors' license agreements and copyright holders' notices.

   a. The Department strictly forbids making unauthorized copies of software.

   b. Reproduction of copyrighted material is allowed only to the extent legally considered "fair use" or with the permission of the author/owner.

   c. Users must not up-load or install software that has been licensed from a third party, or software that has been developed by the Department, to any computer outside the Department, via the Internet.

5. Except for business purposes, members must not intentionally perform downloads from the Internet, as these may cause viruses to be transmitted to the Department's system.

L. All messages sent over Department computer and communications systems, or stored on these systems, are the property of the Department. Members should have no expectation of privacy associated with the information stored in or sent through these systems. (See Section V., D. – Restrictions of Privacy Rights, for further information.)

V. MEMBER OR USER COMPUTER USE

A. System Access and Security

1. Access to Department systems requires each individual to complete a Department background check to gain the appropriate level of security and information access.

2. All members granted access to the Department LAN must fulfill appropriate DOJ bi-annual testing requirements.

3. All members requiring access to Department computer systems must complete an SDPD Computer Security Access Form, available from Information Services on the Department LAN F:\Templates\Administrative\SDPD Computer Access. A commanding officer must sign the form to approve access levels and Backgrounds must sign the form to indicate the member has successfully completed a Department background check before it is submitted to Information Services.

4. Individuals who are Reserve officers, volunteers, contractors, or consultants and who have completed a Department background investigation may be granted a user-ID, or otherwise given privileges to use Department computers or communications systems.

    a. Individuals must also complete a user-ID request form (SDPD Computer Security Access Form). For RSVP members, the form must be signed by the Backgrounds lieutenant. For all other volunteers and contractors the form must be signed by a Department commanding officer, and submitted to Information Services. No other individuals may be granted these privileges.

    b. All temporary employees, consultants, or contractors must have their status noted on the form with a "termination date," which should not be longer than one year. If appropriate, the form may be renewed after the termination date.

    c. All Department information system privileges will be promptly terminated at the time an individual ceases to provide services to the Department.

5. In order to access criminal history information by telephone, Department personnel will be required to provide the County Criminal History code word, their name, and their Department ID. This code is for law enforcement personnel only and is not to be distributed to anyone outside the Department. Access to criminal history information is always based on the need to know/right to know.

6. The Department's Human Resources Unit must notify Information Services when employees, Reserve officers or volunteers leave Department service.

    a. The commands responsible for volunteers and Reserve officers must notify the Department's Human Resources Unit promptly when these individuals leave the Department.

    b. All commanding officers are expected to immediately notify the Human Resources Unit and Information Services of any individual who may be considered a security risk.

7. The Department reserves the right to revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

8. Users are required to comply with computer security settings including password expiration/complexity and the password protected screen saver feature that is invoked automatically after a period of time when a computer is not used. Users must also invoke the feature, lock the system, or log off when leaving a sensitive document that should not be accessed in the computer.

B. Physical Security

1. All Department computer workstations are to be secured from public access.

2. All media such as CDs, external drives, and tapes containing sensitive data should be secured when not in use. When it is not possible to secure such media, encryption should be used.

3. Any confidential or sensitive data files stored in an area of general user access, such as the F: or G: drive, should use password protection or encryption to prevent unauthorized viewing of data.

4. All Department printers are to be secured from public access. Devices that will output sensitive information must be located in an area that can be physically monitored by appropriate personnel at all times. Users concerned about other personnel reading their printed material should print a leading banner page containing the words, "personal and confidential output for <insert name> at <insert phone number>."

5. Users should not modify any of the settings in the printer panel relating to printer configuration. All options should be sent through software. Special printer configurations should be requested and performed by Information Services personnel only. Information Services personnel may lock the printer panel on any printer with any unauthorized printer-setting changes.

6. Zebra label printers are used for labeling impounded property/evidence and are located at each area command and the Police Headquarters building. These printer cartridges contain sensitive information; therefore, anytime they are replaced, the old printer cartridges must be properly destroyed. Department members shall place these used printer cartridges in the locked "shred bins" located at each area command station or Headquarters.

C. Data Security

1. Without specific written exceptions, all programs and documentation generated by, or provided by employees, consultants, or contractors for the benefit of the Department are the property of the Department.

2. Department employees, temporary employees, contractors, and consultants who have used Department information systems must return all hardware, software, working materials, and related property belonging to the Department as part of a check-out procedure through the Police Human Resources Unit , if applicable, or the Information Services Division/Data Systems Unit.

3. Department members must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, unless authorized by the Information Services Program Manager as part of the member's work on the system. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

4. Department software systems or configuration documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Department party for any purposes other than business purposes expressly authorized by the Chief of Police.

5. Users are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Likewise, users are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

6. Members must not test or attempt to compromise internal security controls.

7. Users must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources from other users, or to gain access to other systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to the Information Services Division/Data Systems.

D. Restrictions of Privacy Rights

1. All messages sent over Department computer and communications systems, or stored on these systems, are the property of the Department. To properly maintain and manage this property, the Department reserves the right to examine all data stored in or transmitted by these systems. Since the Department's computer and communication systems must be used for business purposes only, members should have no expectation of privacy associated with the information stored in or sent through these systems.

2. No media advertisement, Internet home page, electronic bulletin board posting, voice mail broadcast message, or any other public representation about the Department may be issued unless it has first been approved by the Chief of Police.

3. Internal messages sent over Department internal electronic systems are not subject to the privacy provisions of the Electronic and Communications Privacy Act of 1986 (which prohibits wiretapping), and therefore may be read by Department management and system administrators.

4. At any time and without prior notice, the Department reserves the right to examine archived electronic mail, user file directories, hard disk drive files, and other information stored on Department information systems. This examination is performed to ensure compliance with internal policies, and assist with the management of Department information systems.

5. In general terms, the Department does engage in blanket monitoring of employee communications using Department information systems. The monitoring is done to ensure that appropriate use of information systems conforms to Department policy. Users must also be aware that the information and communication messages could be subpoenaed by a court of law.

6. The Department routinely logs web sites visited and related information exchanges over the Internet. Commanding officers may request reports of such information from the Information Services Program Manager and may use it to determine what types of Internet usage are appropriate for their members' work activities.

E. Lost or Stolen Equipment

1. Members are to notify their supervisor immediately, and complete the required reports, for lost or stolen computer, telecommunications, and information systems equipment, such as laptop computers, computer peripherals, projectors, and modems. Supervisors are required to immediately inform Information Services Division/Data Systems personnel if the equipment contains sensitive information or has the ability to communicate with the Department systems via wireless technology.

2. The member's supervisor will conduct an investigation and determine the presence or absence of employee negligence. The supervisor will ensure that the proper reports are completed, and will forward a copy of the case report to Operational Support Administration.

3. Commanding officers are responsible for reviewing investigations of stolen or lost equipment to verify the presence or absence of employee negligence. The commanding officer is to forward his/her findings to the appropriate Assistant Chief of Police. The commanding officer will provide a recommendation as to whether the member will reimburse the Department for the equipment, which will be based upon the findings of the investigation.

4. The unit/division equipment officer will ensure that the equipment replacement procedure has been followed and forward the request for new or replacement equipment to the Information Services Division/Data Systems. In units without an assigned equipment officer, the responsibility for performing this function will be assigned to appropriate staff by the commanding officer.

5. Upon notification of negligence from the member's commanding officer, Administrative Services staff will take the appropriate action for reimbursement.