

# WEST PALM BEACH POLICE DEPARTMENT

---

## II-14 COMMUNICATIONS AND DATA SYSTEMS PROTOCOL

**EFFECTIVE: 01/01/2005**

CALEA Standards: 81.2.9, 82.1.7

CFA Standards: 34.12

---

**I. POLICY:** Various communications and data systems may be utilized or provided to our members. These communications and data systems will be used appropriately at all times by all employees. Management will reserve the right to inspect any and all communications and data systems for the appropriate and proper entries.

**II. COMMUNICATIONS AND DATA SYSTEMS:** Include, but are not limited to:

- A. Telephone, cell phone and facsimile (fax) devices;
- B. Radio and paging systems;
- C. Electronic mail;
- D. Mobile computer units, networked desktop computers and any software installed thereon;
- E. NCIC, FCIC, PALMS, or any other criminal justice electronic data storage, retrieval, or inquiry system;
- F. Bulletin boards and places where documents, paper mail and messages are posted or stored;
- G. Voice and video recorders and players;
- H. Data Exchanges;
- I. Internet, and
- J. Other means of communication used to convey any type of message.

**III. MEMBER RESPONSIBILITY:**

A. These systems will be used for their intended purpose.

- 1. Members may use the Department owned equipment for their personal use as long as it does not interfere with their productivity and is in accordance with Department Policy.

**EXAMPLES:** A member who uses a Department computer during non-work hours to do a homework assignment for school not associated with employment.

A member who uses the Internet to review weather conditions in an area they are planning to visit.

B. Except when incidental to an investigation or as part of an official inquiry, response or report, communications systems must never be used to:

- 1. Threaten or intimidate another person;
- 2. Send or receive images that contain pornography or to send images or words of a prurient or sexually suggestive nature, even if the recipient has consented to or requested such material; or
- 3. Send or receive jokes or comments that could disparage a person or group because of race, ethnic background, national origin, religion, gender, sexual orientation, age, verbal accent, sources of income, physical appearance or agility, mental or physical disability, or occupation.

C. No member will knowingly compromise the integrity of any City, Department, or external communications or data systems by the introduction of destructive ("virus") programs, removal or alteration of system or program

files, or any other means.

D. Classified, confidential, sensitive, proprietary, or private information or data as defined in statute, ordinance, or any system user agreement entered into by the Department must not be disseminated to unauthorized persons or organizations.

E. The member does not have a reasonable expectation of privacy when using a computer or communication system that is employer-authorized or is provided for the mutual benefit of the member and the employer.

F. Management may monitor member telephone conversations, read member messages, and inspect mail or documents sent to or by the member through the agency or agency owned or authorized equipment using any physical or electronic means or media.

F. The Chief of Police is the final authority in determining if any communication or data device or system has been improperly used. Any member found in noncompliance with SOP is subject to discipline.

**IV. RIGHTS OF EMPLOYER:**

A. Each Bureau Commander is accountable for the assignment and use of communication systems provided to members within his or her bureau.

B. Management may decipher encrypted text and may remove or inspect software installed by the employee on employer-provided computers.

C. Management may also access, without notice, data or text caches, pager memory banks, electronic mail, voice-mail boxes or accounts, and other employer-provided electronic storage systems.

D. Management will abide by all current legal standards and applicable collective bargaining agreements regarding the monitoring and use of communication and data systems.

E. The management of the communications infrastructure (radio towers, primary radio transmitters and repeaters, computer network cable and components, software anti-virus and firewall systems, software licensing, etc.) is the responsibility of the City MIS Department and the MIS/Public Safety Division and will be governed by MIS and City Administrative policies and procedures related to these components.

**V. SECURITY OF DATA SYSTEMS**

A. Software which enables user access to restricted systems, such as FCIC/NCIC, CAD, RMS, or any interface to the City or Department network, will be restricted to users who are authorized via a software password, hardware password, or both.

1. Members will not disclose assigned confidential passwords except:

a. to authorized maintenance personnel when necessary to upgrade, diagnose or repair software or hardware problems or

b. upon direction of a supervisor when necessary to meet supervisory review needs.

B. Virus protection software and firewall systems will be installed and maintained on Department networks, servers, desktop computers, and mobile computer units by the MIS/Public Safety Division or designee as directed by their internal policies and procedures.

C. The introduction of outside disks or software could result in virus infection of the host system. All disks or software should be inspected for virus infection prior to introduction into the Department systems or stand-alone computers or laptops. All programs should be properly licensed before being used in Department systems.

**VI. REFERENCE:**

- SOP # II-15 Use of Cellular Telephones.
- SOP # II-16 Mobile Computer System
- City Administrative Policy 1-28 Computer Hardware / Software, Networks and Communications
- AELE Sample Policy "Communications Systems".
- FCIC User Agreement.
- NCIC User Agreement.

---

**Delsa R. Bush, Chief of Police**

Original issue: 08/11/89  
Revised: 01/01/2005  
I.D. # 1491

History: SOP # changed to II-14 on 01/01/2005; SOP # changed to 33.17 on 12/15/98, changed to 33.03 on 12/01/1999  
Old SOP # 6.620.028 VII. (2)  
Revision Dates: 06/01/1999, 12/15/1998, 12/15/1999, 05/19/2002, 01/01/2005

Job Title Task Files: