BERKELEY POLICE DEPARTMENT

DATE ISSUED: August 15, 2013 **GENERAL ORDER E-12**

SUBJECT: ELECTRONIC COMMUNICATIONS

PURPOSE

1 - This Order sets forth policy with regard to access to, use of, and disclosure of electronic communications **-** messages sent or received by Department employees with the use of the City of Berkeley's email system and Berkeley Police Crime Forum (Crime Forum).

POLICY

2 - All email and Crime Forum computer files are the property of the City of Berkeley, regardless of their physical location or form in which they are maintained.

3 - All employees shall comply with the requirements set forth in this Order in their use of the City's email, Crime Forum systems, and Web/Cloud access.

(a) An employee's use of the City's email, Crime Forum systems, and Web/Cloud storage implies their knowledge of, and agreement to comply with, the policies and procedures set forth in this Order.

PROCEDURES

Electronic Communications **–** Limited To Official Purposes

4 - Employees shall use electronic communications systems in an appropriate and professional manner for official business.

(a) In addition to activities and communications that further the interests of this Department and the City of Berkeley, "official business" may include work-related social events**,** such as lunches, retirement parties, birthdays, and notices of bereavement.

5 - Employees shall check their email account **and Crime Forum Account** for new messages at least two times each duty shift.

(a) It is recommended that email **and the Crime Forum** be checked close to the beginning and end of each shift worked in order to maximize the employee's exposure to new mail messages and crime information.

6 - When requested by the sender of a message, or as otherwise necessary or appropriate, employees shall respond to received email in a timely fashion.

7 - Misaddressed email shall be sent back to the original sender with a notation the message was misaddressed.

8 - Employees may forward or re-distribute copies of email messages only when doing so fulfills a legitimate work-related purpose.

9 - Use of the email or Crime Forum systems to send messages of a threatening, harassing, obscene or profane manner is prohibited.

(a) Electronic communications containing offensive or inappropriate content, or is otherwise in violation of this Order, shall be forwarded to the recipient's supervisor for appropriate administrative action.

(b) An employee who observes another person use the City's email system inappropriately shall immediately notify their supervisor, or if unavailable, the next person in their Chain of Command.

10 - Employees shall exercise discretion when sending Department-wide email messages, and restrict such broad dissemination to matters having Department-wide importance.

(a) Fundraising events not specifically sanctioned or endorsed by the Department should not be the subject of Department-wide email messages.

(b) Employees shall not send a City-wide mass email message without the prior authorization of the Chief of Police or City Manager.

11 - Employees shall manage the volume of email messages in their City email account to ensure their mailbox does not become "full" and unable to receive new messages.

(a) Employees should not rely on the City email server as an archive for their email files.

Account Security

12 - Employees should protect the security of their email and Crime Forum accounts by regularly changing their private network login password.

(a) Employees shall not share their private network login password or Crime Forum password with any other individual.

13 - "Electronic snooping" or misuse of another employee's email account or Crime Forum account is prohibited.

(a) "Electronic snooping" is the unauthorized use, or attempted use**,** of, another employee's network access password, or the unauthorized entry**,** or attempted entry**,** to the computer files and communications of another without that person's expressed consent.

Department Access to Electronic Mail

14 - The Department shall have the right to access and disclose all messages sent over and contained in the City's email and Crime Forum systems.

15 - The Department shall have the right to delete or retain any email file of an employee who is no longer employed by the City of Berkeley.

Electronic Communication Systems, Initiation/Cancellation of Access

16 - The Professional Standards Division Captain, or his/her designee, shall ensure the Department of Information Technology is notified when an employee is hired, or subsequent to the employee's service termination, in order to add or cancel that person's email system access.

17 - Non-employees may be authorized by the Chief of Police to use the email **or** Crime Forum systems on a case**-**by**-**case basis**,** and only upon the condition that the non-employee shall use the system according to the rules and procedures established in this Order and has been given access to the system in accordance with Department of Information Technology protocols.

Crime Forum Administration

18 - The Investigations Division Crime Analysis Detail will conduct the day to day moderation of content of the Berkeley Police Crime Forum. Crime Analysis Detail Personnel will be assigned to the Forum as "Moderator".

19 - The Professional Standards Bureau will conduct routine audits of the Crime Forum to ensure compliance with this order. The Professional Standards Bureau will be assigned to the Forum as "Administrator".

20 - The City of Berkeley Department of Information Technology will maintain the Berkeley Police Crime Forum.

21 - Crime Forum content will only be retained for a period of 5 years. Information posted to the Crime Forum will be automatically deleted if the information is unused for a period of 5 years.

22 - The Crime Forum shall not be used as a repository for digital evidence. Digital evidence must be stored in accordance with General Order P-65.

Web and Cloud Access

23- In the past fifteen years, the number of crimes involving computer use and the Internet has rapidly expanded, which has in turn brought about an increase in companies and products to assist law enforcement make use of digital forensics to determine the perpetrators, methods, timing and victims of computer crime. The vast majority of those companies and products are web-based, employing "cloud" computing for storage or Software as a Service (SaaS).

24- When information and applications are stored remotely, they can be accessed from any permitted device with an Internet connection, including laptops, tablets, and smart phones. Thus, the Department must address security and privacy issues for each device accessing cloud computing spaces and services.

25- The Criminal Justice Information Services (CJIS) Security Policy sets the minimum standards for security requirements to ensure confidentiality, integrity and availability of criminal justice information maintained by the Federal Bureau of Investigation Criminal Justice Information Services Division. In order to access CJIS data, the Berkeley Police Department has a formal agreement in place with FBI CJIS affirming compliance with the policy. In accordance with CJIS Security Policy addressing web and Cloud access, the following protocols shall be followed:

(a) Employees have access to and may perform investigative activities on their systems, data and content.

(b) Employees are prohibited from uploading for storage, posting, linking to, emailing or otherwise transmission of any content that:

- **i. violates local, state, federal or international laws or regulations**
- **ii. install programs or configure systems to allow the monitoring, or "sniffing," of data traveling over a shared network**

(c) The Department must maintain a list of authorized users and accounts that are permitted to remotely access web and Cloud systems.

- **i. The list will be maintained by the City of Berkeley IT ATA CLETS coordinator.**
- **ii. Employees shall notify the CLETS administrator of usage by submitting information as to date, time, site accessed and purpose.**

iii. Log of access shall be maintained for a period of one year.

PUBLIC RECORDS, DISCLOSURE OF EMAIL

26 - Employees should be aware that all records, whether on paper or computerized, are subject to the mandatory public disclosure requirements of the Public Records Act, subject to the exceptions provided under the Act.

Reference**s**: Administrative Regulation 4.2, General Order R-23, General Order P-65