HONOLULU POLICE DEPARTMENT

POLICY
AUXILIARY AND TECHNICAL SERVICES

March 25, 2015	Policy Number 8.17

SECURITY AND HANDLING OF DEPARTMENTAL RECORDS AND FILES

11-1-2016

POLICY

The management of confidential documents protects individuals' privacy and safety while facilitating the availability of information to the public.

PROCEDURE

I. DEFINITION

Confidential document: Any departmental information recorded on paper, film, or other medium that is restricted under the provisions of the Uniform Information Practices Act (UIPA), Chapter 92F, Hawaii Revised Statutes (HRS).

A. In general, information about personnel, active investigations, or internal organizational procedures is most likely to be restricted.

B. In particular, the following kinds of documents are to be regarded as confidential:

1. Personnel orders;

2. Personnel documents reflecting an individual's medical or psychiatric history, pay, and employment qualifications and evaluations;

3. Documents of any kind in active investigations; and

4. Departmental or element directives and training materials.

This list provides only examples of confidential documents; it is not intended to be a complete list of such documents.

II. DATA AND WORD PROCESSING EQUIPMENT

Element commanders are responsible for the proper care and use of the data and word processing equipment installed in their commands.

A. No one shall operate such equipment without proper training.

B. Such equipment shall be used only for departmental business.

C. No one shall attempt to operate departmental data or word processing equipment (terminals, printers, etc.) without the explicit approval of the element commander responsible for the security of the equipment.

III. OFFICIAL POLICE RECORDS AND FILES

A. Access

Access to official police records and files is normally limited to authorized personnel assigned to the element in which the records or files are maintained. Other personnel must obtain the permission of the element commander or a designee before being granted access to the records or files.

1. Information contained in the Case Report System (CRS) or Paper Management (PM) and related files is confidential and may be used only for departmental business.

2. Additions, deletions, and any other changes to the CRS and PM and related files shall be made only by authorized personnel in the Records and Identification Division.

3. Requests for additions, deletions, or any other changes to user access in the CRS or PM shall be submitted via the HPD Security Access Request e-form. Changes to users or user access shall be completed by authorized personnel of the ITD.

8-12-2019

B. Release of Confidential Documents

Care must be taken to ensure that confidential documents are not released to unauthorized recipients. Confidential documents are not to be released to anyone outside of the department without appropriate authorization and safeguards to protect the contents.

1. When confidential documents are routinely transmitted to other government agencies for departmental purposes (e.g., personnel documents to the Department of Human Resources, investigative documents to the prosecutor, or directives to other law enforcement agencies), the confidentiality of the information is routinely ensured by the receiving agency and no special precautions are necessary.

2. When documents are provided to others outside of the normal range of governmental users, there are risks of compromise because:

   a. The recipient is not authorized to receive the document and it is used for an unauthorized purpose; or

   b. The recipient (e.g., a governmental agency) is authorized to receive the document but transmits it to another who uses it for an unauthorized purpose. In this case, the original recipient may be unaware of the need to restrict the information in the document.

3. Except for documents furnished in accordance with signed court orders and subpoenas duces tecum, an element shall not release confidential documents to anyone outside of the normal range of governmental users without the authorization of the element's bureau chief.

a. When confidential documents are released to anyone outside of the normal range of governmental users, each one shall bear a Confidential Cover Sheet, HPD-190 form. The releasing element shall fill in the information on the form before turning the document over to the recipient.

b. The releasing element shall also require the recipient to sign a Property Receipt, HPD-83 form.

c. The element shall retain the cover sheet and the property receipt for three years before destruction.

4. Penalties

Personnel who violate the confidentiality of documents protected by the UIPA are subject to administrative as well as criminal penalties.

C. Retention and Storage Via PM

Departmental documents (e.g., police reports, temporary restraining orders, geographical restrictions, and sex offender files) are either scanned into the PM or entered via the CRS, after which the information cannot be altered. Any document generated from the system is admissible in both criminal and civil court proceedings and is considered an "original document." Some older documents have been preserved on microfilm.

11-1-2016

1. All information contained in the PM is official and confidential and may only be used for authorized departmental purposes.

2. Access to information stored in the system is limited to personnel who have been authorized by the commander of the Records and Identification Division or a designee.

a. Employees shall not access the system from any computer using another employee's password.

b. If they have reason to believe that the secrecy of their assigned password has been compromised, employees shall ensure that their passwords are changed.

11-1-2016

3. Personnel shall not connect or attempt to connect any personally owned hardware or software equipment or any other device to the PM.

4. The commander of the Records and Identification Division shall determine which documents will be stored as either confidential or encrypted-security status. Personnel shall not access images classified as confidential or encrypted-security unless authorized by the commander of the Records and Identification Division.

5. Personnel who print documents from the PM shall be responsible for the security of the information contained therein.

D. Disposal and Destruction

1. Elements seeking authorization to destroy any official police records or files shall first check the retention schedule.

2. Documents may be destroyed after microfilming or document imaging and validating the imaged copy. Destruction of major, unsolved crimes and missing person reports must be authorized by the Chief of Police or designee, carried out in accordance with the law, and supervised by the commander of the Records and Identification Division or a designee.

3. Printed and written materials that are not confidential shall be disposed of in the normal manner by each element in accordance with applicable recycling laws.

4. Elements are responsible for making their own arrangements to properly dispose of their confidential materials and retaining all receipts necessary for documentation and accountability.

IV. ADDITIONAL SECURITY INFORMATION

See Policy 8.20, COMPUTER SECURITY, for information concerning the security of computerized data and files.

8-12-2019

Susan Ballard

SUSAN BALLARD
Chief of Police

Post on bulletin board for one week

Policy first issued May 14, 2001