

HONOLULU POLICE DEPARTMENT
POLICY
AUXILIARY AND TECHNICAL SERVICES

April 24, 2019

Policy Number 8.02

SECURITY BREACH OF PERSONAL INFORMATION

POLICY

It is the policy of the Honolulu Police Department (HPD) to comply with all statutory requirements in the event of a security breach of personal information.

PROCEDURE

I. **APPLICABILITY**

- A. This procedure shall be initiated if a security breach occurs involving personal information (e.g., a laptop or thumb drive containing police reports with personal information is lost or stolen or a database containing personal information is hacked).
- B. In the event of a security breach of personal information, the HPD is required, as a government agency that collects personal information for specific government purposes, to provide notice to the affected persons that there has been a security breach following discovery or notification of the breach.

II. **DEFINITIONS**

- A. **Encryption or encrypted:** the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.
- B. **Personal information:** an individual's first name or first initial and last name in combination with any one or more of the following when either the name or the following are not encrypted:
 - 1. Social security number;

2. Driver's license number or Hawaii State Identification Card number; or
3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- C. Records: any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.
- D. Security breach: an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur and that creates a risk of harm to a person.

Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the HPD for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the HPD and is not subject to further unauthorized disclosure.

III. PROCEDURE

- A. Personnel shall immediately notify their commander upon the discovery or notification that a security breach has occurred.
- B. Upon discovery or notification of the security breach, disclosure notification shall immediately be made to the affected person.

1. Required notice shall be delayed if notification may impede a criminal investigation or jeopardize national security.
 2. If such a delay is required, it shall be documented in writing to include the name of the law enforcement officer making the request and the division engaged in the investigation.
 3. Notice shall be immediately provided once it is determined that the notice will no longer impede the investigation or jeopardize national security.
- C. The notice shall be clear (see Attachment 1 for a sample notice) and shall include the following information:
1. The incident in general terms;
 2. The type of personal information that was subject to unauthorized access and acquisition;
 3. The general steps taken to protect the personal information from further unauthorized access;
 4. A telephone number that the person may call for further information and assistance, if one exists; and
 5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
- D. Notice to affected persons may be provided by one of the following methods:
1. A written notice to the last available address on record via certified mail;
 2. An electronic mail notice if the HPD is in possession of a valid electronic mail address and if the person has agreed to receive communications electronically from the HPD;

3. Telephonic notice, provided that the contact is made directly with the affected person; and
4. Substitute notice under specific conditions.
 - a. Substitute notice shall only be allowed if:
 - (1) The cost of providing notice would exceed \$100,000;
 - (2) The affected class of subject persons to be notified exceeds 200,000 persons;
 - (3) The HPD does not have sufficient contact information for or consent from the affected person. In this case, it may be used for only that affected person; or
 - (4) The HPD is unable to identify a particular affected person. In this case, it may be used for only that unidentifiable person.
 - b. Substitute notice shall consist of ALL of the following:
 - (1) An electronic mail notice when the HPD has an electronic mail address for the subject person;
 - (2) Conspicuous posting of the notice on the HPD Internet Web site; and
 - (3) Notification to major statewide media.
- E. The commander of the element that is responsible for the breach or the focal point of the breach shall oversee the drafting and issuance of the notice.

F. The commander of the element that is responsible for the breach or the focal point of the breach shall prepare a written report to the Legislature within 20 days after discovery of the security breach. The written report shall contain the following information:

1. Detailed information relating to the nature of the breach;
2. The number of individuals affected by the breach;
3. A copy of the notice of security breach that was issued;
4. The number of individuals to whom the notice was sent;
5. Whether the notice was delayed due to law enforcement considerations; and
6. Any procedures that have been implemented to prevent the breach from reoccurring.

If notification to the Legislature may impede a criminal investigation or jeopardize national security, the report to the Legislature may be delayed until 20 days after it has been determined that notice will no longer impede the investigation or jeopardize national security.

G. The report shall be submitted via the element's chain of command for approval and transmitted to the Legislature through the Legislative Liaison Office.

April 24, 2019

Policy Number 8.02
Page 6

- H. The report to the Legislature shall be in letter form and addressed to the Speaker of the House of Representatives and the President of the Senate (see Attachment 2).



SUSAN BALLARD
Chief of Police

Attachments

Post on bulletin
board for one week

April 24, 2019

Mr. John Doe
1234 Alapai Street, Apartment 567
Honolulu, Hawaii 96813

Dear Mr. Doe:

On April 8, 2019, it was discovered that a security breach occurred possibly exposing your personal information. On April 7, 2019, a computer storage device containing your personal information from a police report was stolen.

The personal information subject to the theft was your full name and social security number. The Honolulu Police Department is actively investigating the theft of the storage device. We encourage you to remain vigilant by reviewing your account statements and monitoring free credit reports. You can find more information on identity theft by visiting our Web site at [www.honolulupd.org](http://www.honolulu.honolulupd.org).

We apologize for any inconvenience this may have caused you. Should you have any further questions, please call the Honolulu Police Department between the hours of 7:45 a.m. and 4:30 p.m., Monday through Friday, at 123-4567.

Sincerely,

SUSAN BALLARD
Chief of Police

By
JANE ROE, Major
District 1

April 24, 2019

The Honorable Scott Saiki
Speaker
House of Representatives
Hawaii State Capitol, Room 431
415 South Beretania Street
Honolulu, Hawaii 96813

Dear Speaker Saiki:

In accordance with Section 487N-4, Hawaii Revised Statutes, this letter shall serve as our report to the Legislature concerning a security breach at the Honolulu Police Department.

On April 8, 2019, it was discovered that a security breach occurred possibly exposing private information. On April 7, 2019, a computer storage device containing official Honolulu Police Department reports was stolen. A criminal theft investigation under report number 13-123456 has commenced.

A total of 45 individuals were affected by the breach. Attached are copies of the notice of security breach that were issued. The notices were sent without undue delay.

Procedures are currently in place to guard against security breaches; however, in-service training will be conducted to prevent a breach from reoccurring. Also, an administrative investigation into this incident is currently underway to address any violations of our policies and Standards of Conduct.

Should there be any questions, Major Jane Roe of our District 1 may be contacted at 123-4567.

Sincerely,

Susan Ballard
Chief of Police

Attachments

April 24, 2019

The Honorable Ronald D. Kouchi
President
State Senate
Hawaii State Capitol, Room 409
415 South Beretania Street
Honolulu, Hawaii 96813

Dear President Kouchi:

In accordance with Section 487N-4, Hawaii Revised Statutes, this letter shall serve as our report to the Legislature concerning a security breach at the Honolulu Police Department.

On April 8, 2019, it was discovered that a security breach occurred possibly exposing private information. On April 7, 2019, a computer storage device containing official Honolulu Police Department reports was stolen. A criminal theft investigation under report number 13-123456 has commenced.

A total of 45 individuals were affected by the breach. Attached are copies of the notice of security breach that were issued. The notices were sent without undue delay.

Procedures are currently in place to guard against security breaches; however, in-service training will be conducted to prevent a breach from reoccurring. Also an administrative investigation into this incident is currently underway to address any violations of our policies and Standards of Conduct.

Should there be any questions, Major Jane Roe of our District 1 may be contacted at 123-4567.

Sincerely,

Susan Ballard
Chief of Police

Attachments