

AGENCY INFORMATION SECURITY INCIDENT REPORT

Agency: _____

Agency Organization Code: _____
(As identified in the [Uniform Codes Manual](#))

Incident Number: _____
(Provided by the Office of Information Security)

A. Notification

1. Date of notification to the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC): _____

B. Incident Information

1. Details of Incident:

a) Date incident occurred: _____ Unknown

b) Date incident detected: _____ Unknown

c) Incident location: _____

d) General description:

Please describe:

e) Media/Device type, if applicable: _____

Was the portable storage device encrypted? Yes No

If NO, explain: _____

f) Describe the costs associated with resolving this incident:

:

g) Total estimated cost of incident: _____

2. Incidents involving personally identifiable information

a) Was personally identifiable information involved? Yes No (If No, go to Part C)

Type of personally identifiable information (Check all that apply)

Name Health or Medical Information

Social Security Number Financial Account Number

Driver's License/State ID Number

AGENCY INFORMATION SECURITY INCIDENT REPORT

Other (Specify) _____

b) Is a privacy disclosure notice required? Yes No

c) If a Privacy Disclosure Notice is required, attach a sample of the notification.

d) Number of individuals affected: 5

e) Date notification(s) made: _____

Incidents involving personally identifiable information

C. Corrective Actions Planned/Taken to Prevent Future Occurrences:

Please describe:

1. Estimated cost of corrective actions: _____

2. Date corrective actions will be fully implemented: _____

D. Signatures:

Printed Name of Information Security Officer	Signature of Information Security Officer	(Date)
--	---	--------

HIPAA Coordinator

Printed Name of Privacy Officer	Signature of Privacy Officer	(Date)
---------------------------------	------------------------------	--------

(Required if privacy incident occurred whether or not notices were sent)

Printed Name of Secretary/Director or Designee	Signature of Secretary/Director or Designee	(Date)
--	---	--------

Mail this completed Incident Report to the following address:

California Technology Agency
Attention: Office of Information Security
1325 J Street, Suite 1650
Sacramento, CA 95814

AGENCY INFORMATION SECURITY INCIDENT REPORT INSTRUCTIONS

Following the requirements outlined in State Administrative Manual (SAM) Section 5350 and guidance outlined in Statewide Information Management Manual (SIMM) Section 65B, complete this form and send the signed copy to the Office of Information Security within ten (10) business days from the day of notification to the California Highway Patrol Emergency Notification and Tactical Alert Center (ENTAC). ***Do not send these instructions with the signed report.***

The following instructions will assist in completing the form. All questions must be completed, even in a case where the response is a future action.

Agency – Provide your agency, department, board, bureau or commission's full name.

Agency Organization Code – Provide your agency's organization code (format nnnn) as identified in the [Uniform Codes Manual](#).

Incident Notification Number – The Office of Information Security will provide this number to the agency when the Office is notified of the incident.

A. Notification

Date of notification to the CHP ENTAC – Provide the date the CHP ENTAC at **(916) 843-4199** was notified of the incident. Other notifications to CHP or the Office of Information Security by email, telephone or any other method is **NOT** a substitute for the required ENTAC notification.

B. Incident Information

1. **Details of incident** – Provide the date the incident occurred and the date the incident was detected, if known. In the general description field, provide an overview of the incident, with enough details so that the incident can be easily understood. *Do not include any personally identifiable information* (such as social security numbers, home addresses, etc.). Your report should include the following information as applicable:
 - a) **Date incident occurred.**
 - b) **Date incident discovered.**
 - c) **Incident location** – Provide the location where the incident occurred. For example, if a laptop was stolen from an employee's home, suggested content might be, "Employee's Home, Roseville, CA" or, if the incident occurred at the agency's headquarters office, suggested content might be, "Agency's Headquarters, 123 Any Street, Sacramento, CA"
 - d) **General description** – include the following in the description:
 - When the incident occurred and how it was discovered.
 - The effect of the incident on the business and infrastructure of your agency.
 - The number of people (inside your agency and outside your agency) affected by this incident.
 - The effects if any of this incident to people, businesses or services outside of your agency.
 - The details of any law enforcement investigation of this incident such as which agency investigated it, when, and the report number.
 - Any personal, confidential, or sensitive information involved.
 - e) **Media/Device type, if applicable** – Provide the type of media or device involved in the incident such as paper (fax, mail, etc.) or electronic (CD, floppy drive, laptop, PDA, email, etc.).

AGENCY INFORMATION SECURITY INCIDENT REPORT INSTRUCTIONS

- **Was the portable storage device encrypted?** – Check appropriate box. If **NO**, describe why the storage device was not encrypted.
 - f) **Describe the costs associated with resolving this incident** – Provide a cost estimate of resolving the incident. Cost should include everything necessary to resolve the incident including hardware, software, staff time, contracting services, and any other pertinent costs that were triggered due to the incident. It should also include costs associated with a disclosure notification (such as preparation, postage, call center activation, etc.).
 - g) **Total estimated cost of incident** – Provide the total cost associated with handling the incident as it relates to information technology including the cost to replace any stolen equipment and/or software. For example, if a state vehicle was stolen with a state-issued laptop in it; do not include the cost of the state vehicle.
2. **Incidents involving personally identifiable information**
- a) **Was personally identifiable information involved?** – Check appropriate boxes.
 - b) **Is a privacy disclosure notice required?** – Check appropriate box.
 - c) **Sample** – If yes, attach a sample copy of the notification sent to the affected individuals. *DO NOT provide a sample that includes personally identifiable information.*
 - d) **Number of individuals affected** – Identify the number of individual's whose personally identifiable information was breached.
 - e) **Date notification(s) made** – Provide the date that the Notifications were made to the affected individuals.
- C. **Corrective Actions Planned/Taken to Prevent Future Occurrences** – Provide a detailed description of the corrective actions taken by the agency to prevent future occurrences of a similar incident occurring again.
- 1. **Estimated cost of corrective actions** – Provide cost estimations to implement the corrective actions. For example, hardware and/or software may need to be upgraded, installed or purchased; new policies may need to be developed, additional training may need to be given. Include all related costs such as staff time, contracting services, and hardware or software purchases.
 - 2. **Date corrective actions will be fully implemented** – Provide a date when the corrective actions were, or will be, fully implemented.
- D. **Signatures** – The agency's Information Security Officer and Secretary/Director or Designee must sign this report for all incidents. The agency Privacy Officer is required to sign the report only in those instances where personally identifiable information is involved. If personally identifiable information is involved and no disclosure notice is required, the Privacy Officer's signature is still required.

Mail the completed Incident Report, without these instructions, to the address provided above.