

INFORMATION SECURITY INCIDENT REPORT

Department: _____

Incident Number: _____
(For Information Security Office only)

A. Notification

1. Date of notification to the Chief Information Security Officer or Departmental Information Security Representative (ISAC member): _____

B. Incident Information

1. Details of Incident:

- a) Date incident occurred: _____ Unknown
- b) Date incident detected: _____ Unknown
- c) Incident location: _____
- d) General description:

- 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)

- | | |
|---|--|
| <input type="checkbox"/> Name | <input type="checkbox"/> Health or Medical Information |
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Financial Account Number |
| <input type="checkbox"/> Driver's License/State ID Number | |
| <input type="checkbox"/> Other (Specify) | |

- b) Is a Privacy Disclosure notice required? Yes No

INFORMATION SECURITY INCIDENT REPORT

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

d) Number of individuals affected: _____

e) Date notification(s) made: _____

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

1. Estimated cost of corrective actions: _____

2. Date corrective actions will be fully implemented: _____

D. Names:

Departmental ISR (ISAC Member*)

(Date)

* See <http://security.co.contra-costa.ca.us/ISAC/email.htm>
for ISAC members by department

Department Head (or Designee)

(Date)

Route completed Incident Report to the following address or e-mail to
informationsecurity@cao.cccounty.us.

County Information Security Office
30 Douglas Drive
Martinez, CA 94553

INFORMATION SECURITY INCIDENT REPORT INSTRUCTIONS

Following these instructions to complete this form and send the a copy to the Information Security Office within ten (10) business days from the incident. Do not send these instructions with the report.

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

Department – Provide your Department full name.

Incident Notification Number – Completed by the Information Security Office.

A. Notification

Date of notification to the Chief Information Security Officer or Departmental Information Security Representative (ISAC member)

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, Concord, CA" or, if the incident occurred at the Department's headquarters office, suggested content might be, "Department's Headquarters, 123 Any Street, Martinez, 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 Department.
 - The number of people (inside your Department and outside your Department) affected by this incident.
 - The effects if any of this incident to people, businesses or services outside of your Department.
 - The details of any law enforcement investigation of this incident such as which Department 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.).
 - **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

INFORMATION SECURITY INCIDENT REPORT INSTRUCTIONS

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 County vehicle is stolen with a County-issued laptop in it; do not include the cost of the County 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 Department 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. **Names** – The Department's Information Security Representative and Department Head will report all incidents.

Route the completed Incident Report, without these instructions, as indicated on the form.