SECURITY BREACH REPORT
(SIMM 65C)

Agency:	Developmental Services

Agency Organization Code:	4300

(As identified in the Uniform Codes Manual)

Incident Number:	

(Provided by the State Information Security Office)

A. Notification

1. Date of notification to the California Highway Patrol (CHP) ENTAC:	

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:	

SECURITY BREACH REPORT
(SIMM 65C)

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
- ☐ Social Security Number
- ☐ Driver's License/State ID Number
- ☐ Other (Specify)
- ☐ Health or Medical Information
- ☐ Financial Account Number

b) Is a privacy disclosure notice required? ☐ Yes ☐ No

c) If a Privacy Disclosure Notice is required, attach a sample of the notification. ☐ Not available

d) Consumer(s) TCM eligible? ☐ Yes ☐ No

e) Consumer(s) on HCBS waiver? ☐ Yes ☐ No

f) Number of individuals affected:	
g) 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:	

SECURITY BREACH REPORT
(SIMM 65C)

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.

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.).
      - **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.