

**SAM – INFORMATION SECURITY  
(Office of Information Security)**

**CRITERIA FOR REPORTING INCIDENTS**

**5350.2**

(Revised 10/09)

Incidents reported to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) include, but are not limited to, the following:

1. **State Data (includes electronic, paper, or any other medium).**
  - a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal. (See SAM Section 5320.5).
  - b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
  - c. Deliberate or accidental distribution or release of personal information by an agency, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
  - d. Intentional noncompliance by the custodian of information with his/her responsibilities. (See SAM Section 5320.3).
2. **Inappropriate Use & Unauthorized Access** - This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.
3. **Equipment** - Theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.
4. **Computer Crime** - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.
5. **Any other incidents that violate agency policy.**