

ADMINISTRATION BULLETIN

NO: 03-06

SUBJECT: INFORMATION
TECHNOLOGY INCIDENT &
COMPUTER CRIME REPORTING

DATE ISSUED: April 2003

EXPIRES: Indefinite

REFERENCE(S): State Administrative
Manual (SAM) 5350.1 and Budget
Letter (BL) 03-03

DISTRIBUTION: Supervisors and
Managers

CONTACT PERSON:

Archie Alimagno, Information Security Officer
Ethics and Operational Compliance Office
300 Capitol Mall, Ste. 1300, Sacramento, 95814

PHONE NUMBER:

(916) 492-3353

John Garamendi
Insurance Commissioner

PURPOSE:

This policy defines the process for handling Information Technology Incidents and computer crimes as well as reporting requirements in SAM § 5350.1 and BL 03-03.

Furthermore, this policy for reporting technology incidents is intended to:

1. Assess and document any potential tampering, interference, damage, or unauthorized access to computer data, computer equipment, and computer systems;
2. Minimize consequences to CDI systems when incidents occur;
3. Meet mandated reporting requirements;
4. Provide feedback to CDI management and the Information Technology Division (ITD) so improvement and/or changes in the Information Security Program and information technology programs may occur as needed;
5. Identify the Information Security Office as the clearinghouse for reporting incidents to TEALE data center, Department of Finance (DOF), the Chief Deputy Commissioner and others as required.

TECHNOLOGY INCIDENT DEFINED:

Any incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and databases, as well as incidents involving loss, damage, or misuse of information assets including (but not limited to): records, files, and data bases; and information technology facilities, equipment (including personal computer systems), and software owned or leased by state agencies.

Examples of incidents that require notification are summarized below:

- State-owned or State-managed data, without authorization, was damaged, destroyed, deleted, shared, altered, or copied, or used for non-State business. This includes computer documentation and configuration information, as well as electronic and non-electronic data and reports.
- Unauthorized parties accessed one or more State computers, computer systems, or computer networks. This includes deliberate and unauthorized uses of state-owned computer services, as well as “hacker attacks.”
- Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer software or computer programs which reside or exist internal or external to a State computer, computer system, or computer network.
- Disruption of state computer services or denial of computer services occurs in a manner that appears to have been caused by deliberate and unauthorized acts.
- A contaminant was introduced into any State computer, computer system, or computer network. This includes, but is not limited to viruses, Trojans, worms, and other types of malicious attacks.
- Internet domain names and/or user account names have been used without permission in connection with the sending of one or more electronic mail messages, and thereby caused damage to a state computer, computer system, or computer network, or misrepresented the state or state employees in electronic communications.
- Damage or destruction of state information processing facilities has occurred.
- Physical intrusions into state facilities have occurred that may have resulted in compromise of state data or computer systems.

RESPONSIBILITIES:

- The person that identifies the incident must contact the Information Security Officer (ISO) at (916) 492-3353 to coordinate the finding(s).
- The ISO shall notify the California Highway Patrol’s Emergency Notification and Tactical Alert Center (ENTAC) at (916) 657-8287 about all IT security incidents and computer-related crimes immediately upon discovery of the incidents pursuant to BL 03-03 and other appropriate law enforcement agencies as required by SAM Section 5350.1.
- The program (division/bureau/unit/office) having ownership responsibility for the information (SAM Section 5320.2) must complete an Information Technology Incident Report. If the information owner cannot fill out any area of the report, the owner shall obtain assistance from ITD staff or the IS office in order to complete the report. After the report is completed, the form should be provided to the ISO via email at alimagnoa@insurance.ca.gov.
- Once received, the Department of Insurance will investigate all known and suspected technology incidents.
- The report, signed by the Insurance Commissioner and ISO, will be submitted to the ENTAC and DOF-Technology Oversight Review Unit. CHP serves as the incident notification center after becoming aware of the incident. If you have any questions please contact the ITD or the Information Security Office for assistance.