

INFORMATION SECURITY INCIDENT RESPONSE PLAN

(No.32 May 2015)

For information on what constitutes a reportable incident, please refer to the [Information Security Office Incident](#) webpage on the CAL FIRE Intranet or the [CAL FIRE 0900 Information Technology Handbook Section 0938](#).

1. The person who discovers the incident will **immediately contact** the **CAL FIRE Information Security Officer (ISO) at (916) 206-5900 cell or (916) 327-3993 office** and his/her local Information Technology Services (ITS) Coordinator in addition to any other mandated reporting protocols.

Depending on the severity of the incident others requiring contact may include:

- CAL FIRE Director, Chief Deputy Director, State Fire Marshal
- Deputy Director, Region Chief
- Chief Legal Counsel
(916) 653-4153 Office
- Deputy Director for Communications
(916) 653-5587 Office
(916) 704-4287 Cell
- **Chief Information Officer (CIO)**
(916) 445-5053 Office
(916) 799-9917 Cell
- **ITS Customer Services Manager**
(916) 324-3391 Office
(916) 799-9927 Cell
- Deputy Chief Law Enforcement
(916) 653-0067 Office
(916) 205-1066 Cell
- Unit Chief/Program Chief, Manager, Supervisor, Incident Commander
- Emergency Command Center
- Other internal staff and/or cooperators through departmentally established chain of command processes.
- External sources as determined by the CAL FIRE Director, Chief Deputy Director, ISO, and/or CIO including, but not limited to:
 - The California Highway Patrol
 - The California Information Security Office
 - The California Technology Agency
 - The California Natural Resources Agency
 - The California Department of Justice
 - The Department of Homeland Security
 - The Office of Emergency Services
 - The Office of the Governor

2. If the person discovering the incident is a member of ITS, proceed to step 5.
3. If the person discovering the incident is not a member of ITS, contact the ISO and the local ITS Coordinator and/or ITS Customer Services Manager.
4. The ISO will make appropriate contacts in accordance with State of California policy for incident reporting. The ISO, at minimum, will log the following information:
 - Name of the caller
 - Time of the call
 - Contact information
 - Nature of the incident.
 - Equipment or persons involved
 - Location of equipment or persons involved
 - How the incident was detected?
 - When the event was first noticed?
5. The ITS staff member who receives the call (or discovers the incident) will contact the ISO and ITS Customer Services Manager while ensuring other appropriate personnel and/or designated managers are contacted. The ITS staff member will log the information received in a similar format as the ISO in the previous step adding the following:
 - Is the equipment affected business critical?
 - What is the severity of the potential impact?
 - Name of system being targeted, along with operating system, and Internet protocol (IP) address
 - Any information about the origin of the attack
6. Depending on the severity of the incident, contacted members (comprising an incident response team) will meet and/or discuss the situation to determine a response strategy including, but not limited to:
 - Is the incident real or perceived?
 - Is the incident still in progress?
 - What data or property is threatened and how critical is it?
 - What is the impact on the business should the attack succeed (e.g., minimal, serious, or critical)?
 - What system(s) are targeted (e.g. located physically and on the network)?
 - Is the incident inside the trusted network?
 - Is the response urgent?
 - Can the incident be quickly contained?
 - Will the response alert the attacker?
 - What type of incident is this (e.g., virus, worm, intrusion, abuse, damage)?

7. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
 - Category 1 – A threat to public safety or life
 - Category 2 – A threat to sensitive data
 - Category 3 – A threat to computer systems
 - Category 4 – A disruption of services
8. Team members will establish and follow internal procedures dependent on the type of incident. Furthermore, dependent on the circumstances surround the event the Department's Technology Recovery Plan and/or Continuity of Operations & Continuity of Government (COOP/COG) may be activated.
9. Team members will use applicable forensic techniques, including, but not limited to, reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only the ISO, CIO, ITS, or Law Enforcement should be performing interviews or examining evidence depending on the situation.
10. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems and upon management approval, the changes will be implemented.
11. ITS will restore the affected system(s) to the uninfected state by doing any or more of the following:
 - Re-install the affected system(s) from scratch and restore data from backups if necessary (preserving evidence before doing this)
 - Make users change passwords if passwords may have been sniffed
 - Be sure the system has been hardened by turning off or uninstalling unused services
 - Be sure the system is fully patched
 - Be sure real time virus protection and intrusion detection is running
 - Be sure the system is logging the correct events and to the proper level
12. The following, at minimum, shall be documented:
 - How the incident was discovered?
 - The category of the incident
 - How the incident occurred (e.g., through email, firewall, etc.)?
 - Where the attack came from (e.g., IP addresses and other related information)?
 - What the response plan was?
 - What was done?
 - Whether the response was effective?
13. For evidence preservation where needed, ITS will make copies of logs, emails, and other communication. Evidence must be kept in accordance with direction from the Legal Office.
14. The ISO will notify proper external agencies in accordance with State of California incident reporting requirements.

15. The ISO with assistance from ITS will assess damage and cost utilizing the California Information Security Office tools. The damage to the organization is both the damage cost and the cost of the containment efforts.

16. Team members will review response and update policies to plan and take preventative steps including, but not limited to:
 - Considering whether an additional policy could have prevented the intrusion
 - Considering whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future
 - Was the incident response appropriate and how could it be improved?
 - Was every appropriate party informed in a timely manner?
 - Were the incident-response procedures detailed and did they cover the entire situation and how can they be improved?
 - Have changes been made to prevent a re-infection?
 - Have all systems been patched, locked down, passwords changed, anti-virus updated, email policies set, etc.?
 - Have changes been made to prevent a new and similar infection?
 - Should any security policies be updated?
 - What lessons have been learned from this experience?

[\(Handbook Table of Contents\)](#)