IT Security Standard: Incident Response Program (DRAFT)

Effective Date:
November 1, 2011

Compliance Date:
November 1, 2011

Revision History:
- Reviewed with LAN Coordinators (in progress)
- Reviewed with Security Management Team
- Written by Mary Shaffer - August 2011
- Source documents: Incident response standards, plans and protocols from other universities

Review Frequency:
This standard will be reviewed annually to ensure its applicability to the current university environment. Upon resolution of critical or high-risk incidents, it may be reviewed to determine if changes are needed.

Responsible Office:
Information Services, Office of the CIO, in cooperation with the Information Security

Responsible Officer:
Vice Provost/Chief Information Officer, in cooperation with the Information Security Officer

Brief Description:
To ensure that security incidents and policy violations are promptly reported, investigated, documented and resolved in a manner that promptly restores operations while ensuring that evidence is maintained.

Related Policy:
- Cal Poly’s Information Security Program (ISP)
- Cal Poly’s Information Technology Resources Responsible Use Policy (RUP)
- 8075.0 Information Security Incident Management

Introduction:
This standard outlines the workflow, roles and responsibilities, and escalation provisions with respect to identifying and handling information technology (IT) policy violations and information security incidents at Cal Poly. An accurate, complete and consistent response is essential to ensure the protection of university information assets while complying with applicable policies and laws. Timely and relevant communication with appropriate parties is necessary to ensure the quality of the response, support legal action if necessary, and maintain public confidence. Complete, accurate documentation and subsequent debriefing are important to prevent recurrence of similar incidents.
Scope:
All information security incidents are to be handled according to this standard and in a manner consistent with applicable laws and regulations. This standard applies to any information security incident or policy violation involving IT resources at Cal Poly, whether initiated from on- or off-campus. It applies to all university IT resources, whether centrally administered or locally administered; to all users, auxiliary organizations, third parties, visitors, or else anyone with access to Cal Poly information assets; and to personally-owned computers with access to university networks. While mainly intended to address violations of Cal Poly’s Information Security Program and Responsible Use Policy, this standard applies to any information security related incident involving the university.

Incident Response Program:

Workflow
The incident response process consists of the following steps which are described further in this section:

- Identification
- Assessment and Classification
- Notification and Containment
- Eradication
- Documentation
- Improvement
- Communication

Identification
Potential incidents are identified using information from various sources, including but not limited to:

- Contact from affected or impacted parties
- Contact from network, system and/or application administrators
- Contact from external third parties
- User alerts and/or Service Desk requests
- Monitoring of university networks, systems and/or applications for anomalies, intrusions, and/or unusual behavior that could reasonably raise suspicious of potential compromise

Examples of incidents covered by this standard include but are not limited to:

- Breach or improper disclosure of university information
- Compromise of information integrity, e.g., damage or unauthorized modification of data
- Compromise of information availability, e.g., denial of service attack
- Theft of or damage to physical information assets
- Denial of service attack that impacts university business or services or external parties
- Misuse or abuse of university services, information or assets
- Infection of systems by unauthorized or malicious software
- Unauthorized access attempts that impact university business or services or external parties
• Unauthorized changes to university information assets
• Trigger of intrusion detection alarms beyond “normal” levels

Once identified, incidents are reported to abuse@calpoly.edu or other appropriate reporting methods, which triggers the incident response plan.

Assessment and Classification
Once a potential problem has been identified, the Incident Response Team will analyze the situation and attempt to confirm whether it is the result of a security incident. If yes, then the team will determine the severity of the incident and classify the incident as Critical, High, Medium or Low. Incident severity and classification is based on whether an incident poses a threat to university or external resources, stakeholders, and/or services. The determination may include, but is not limited to, the following factors:

• Does the incident involve unauthorized disclosure of high-risk or confidential information?
• Does the incident involve serious legal issues?
• Does the incident cause serious disruption to critical services?
• Does the incident involve active threats?
• How widespread is the incident?

Incidents classified as critical or of high severity are referred to the Information Security Management Team. All other incidents are handled by the Incident Response Team in accordance with established practices. Further assessment may effect a reassignment to a different level of severity by the team.

Classification Levels
Critical: Any unexpected or unauthorized change, disclosure or interruption to information assets that could be damaging to the campus community or university reputation. Examples: A major attack against the university’s IT infrastructure; an incident with major impact on operational activities; significant loss of confidential data and/or mission-critical systems or applications.

High: Campus-wide and potentially public impact. A successful breach has occurred and/or a threat has manifested itself. There is significant risk of negative financial or public relations impact. A large number of systems or accounts are affected. A very successful attack that is difficult to control or counteract because no countermeasures, resolution procedures or bypass exist. Level 1 data may be involved.

Medium: The threat and impact is limited in scope, e.g., department-wide not campus-wide. Early indications of a possible attack or intrusion detected with minimal risk of negative financial or public relations impact. A small number of systems or accounts are affected. A nominally successful attack that is easy to control or counteract, although countermeasures may be weak. Level 2 data may be involved.

Low: An incident with no effect on system operations. Intelligence received concerning threats to which systems may be vulnerable. Penetration or denial of service attacks attempted with no impact. No critical infrastructure is affected. Solutions or countermeasures are readily available. Procedures are available and well-defined to resolve the problem. No protected information is involved.
Notification and Containment

Once an incident has been positively identified, the Incident Response Team will work with appropriate personnel to isolate the affected equipment in order to prevent secondary threats, attacks on other internal systems, and potential legal liability, including blocking network access.

A compromised system or account that is actively causing widespread problems or affecting non-Cal Poly networks or computers will be blocked from the network immediately following established practices. Other immediate actions may include removal from service and/or forensic analysis if appropriate using established protocols. The Incident Response Team may recommend additional containment measures in addition to those outlined in related procedures for this standard.

Depending on the nature of the incident, the Incident Response Team may be required to work with law enforcement. If served with a warrant or subpoena for information related to security incidents, the Incident Response Team will consult with University Legal Counsel to ensure compliance with federal and state regulations and applicable CSU policies and practices.

Some incidents require notification of affected parties or individuals under contractual commitments or in accordance with applicable laws and regulations. Notification may not be required in incidents in which the university can reasonably conclude that disclosure or misuse of the compromised information is unlikely, and appropriate measures are taken to safeguard the interests of affected parties.

Using established practices, Cal Poly will comply with federal and state requirements to notify any individual whose unencrypted personal information has been or is reasonably believed to have been disclosed by the university to an unauthorized person.

Copies of security breach notifications sent to affected individuals will be posted on the Information Security website. Beyond that, information shared with the media or general public regarding a security incident must be coordinated through Cal Poly’s Public Affairs Office.

Eradication

On receiving notice of an incident, the party responsible for the affected information asset is responsible for resolving the issue. This includes but is not limited to changing passwords, reformatting media, updating or reinstalling software, running scans and taking appropriate remediation action, and/or taking other steps as needed to remove the threat and prevent similar compromises in the future.

Individuals are expected to follow any specific protocols or recommendations cited in the notice and to document any actions they take to resolve the problem. This includes following established protocols for proper evidence collection, handling and storage; problem identification, remediation and mitigation; incident reporting and documentation, etc. (See Related Procedures and Resources.)

Once a system is secured, the responsible party must notify abuse@calpoly.edu so the Incident Response Team can take appropriate measures to document and resolve the incident.
**Documentation**

The Incident Response Team will create and maintain a confidential written record for each incident in Cal Poly’s secure electronic trouble ticket system until the incident is finally resolved. At minimum, the record must include the incident date and time, incident type and severity and impact, who or what reported the incident, detailed description of what occurred, supporting evidence if available, source and target of the attack, affected campus resources, response actions taken and by whom, evidence collected, suspected cause(s), total hours spent and other costs (if applicable). Records will be used to report the number and type of incidents as needed and to identify incident response trends over time.

Individuals involved in any investigation or corrective measures are responsible for documenting their actions, communications and findings related to the incident. This information must be submitted to abuse@calpoly.edu so it can be incorporated into the confidential ticket.

**Improvement**

Individuals and units involved the incident response process may have recommendations to improve system/network configuration, security practices, business processes or the incident response process. Recommendations will be collected and documented by the Incident Response Team.

At the conclusion of major incidents, the Incident Response Team will hold a debriefing to review lessons learned and to recommend changes to this standard and related procedures if appropriate.

**Communication**

Communication with affected parties involved in the incident occurs at each stage in the incident response cycle. Specific communication responsibilities are identified in the Roles and Responsibilities section of this standard.

**Escalation**

While isolated incidents may be resolved with minimal involvement outside the initial response team, some incidents may require escalation to notify appropriate entities, to obtain investigative information or assistance, and/or to ensure an appropriate public response by the university. Four escalation levels are outlined in this standard:

- Initial
- Unit Level
- University Level
- External

Initial and unit level escalation may be undertaken by the Incident Response Team as the case indicates; university level and external escalation are at the discretion and delegation of the Information Security Management Team.
**Escalation - Initial**

Initial escalation may be necessary when an incident has the potential to affect network services or other conditions on a limited but not isolated scale. Entities involved in the initial escalation may include, but are not limited to:

- ITS Service Desk
- Affected ITS group(s), e.g., Network Administration, Collaboration Support, Central Systems, etc.
- Affected group(s) outside ITS, e.g., ResNET, ANTS, etc.
- LAN Coordinator, System Administrator, and/or Application Manager
- User

**Escalation - Unit Level**

Unit level escalation may be necessary when an incident has the potential to affect network services, high risk and/or confidential data, university business services or other conditions university-wide. Unit level escalation may also be necessary in the event of a refusal or official non-compliance with recommended eradication methods.

Entities involved in unit level escalation may include, but are not limited to:

- Information Authority/Owner
- Campus Compliance Officer
- Information Security Management Team
- Information Security Coordinator
- Other management within the affected units

**Escalation - University Level**

University level escalation is at the discretion or delegation of the Information Security Management Team. Entities involved in unit level escalation may include, but are not limited to:

- University Legal Counsel
  - before contacting law enforcement
  - if a breach of contract has occurred
  - if a warrant or other valid legal request has been received
  - to authorize a litigation hold or other investigation
- Public Affairs
  - if a security breach notification is required
  - if a case is likely to affect public confidence
  - before responding to media-initiated contact
- University Police
  - if physical safety is threatened
  - if university property has been stolen
  - if investigation reveals evidence of a crime
  - if external law enforcement needs to be contacted
• if investigators need information or record retention that requires a warrant to obtain
  - Executive Management
    • if a case is likely to affect public safety, enterprise services, and/or public confidence
    • if a security breach notification is required
  - CSU Chancellor’s Office
    • if a security breach notification is required
    • if a breach of Level 1 or Level 2 data has occurred

Escalation - External
External escalation is at the discretion or delegation of the Information Security Management Team. External entities which may be involved and examples of when those entities may be contacted include but are not limited to:

- Internet Service Providers
  • to report abuses and provide evidences (e.g., logs) for incidents originating off-campus
  • to obtain transaction records or other evidence
- Telecommunication Carriers
  • to obtain call records or other evidence
- Third party providers or contractors
  • to report, verify and coordinate incident response activities
  • to obtain transaction records or other evidence
- Local, state of federal law enforcement agencies
  • to report criminal activity
  • to obtain search warrants or other assistance
  • to obtain other assistance

Definitions:
The following definitions apply to terms used in this standard.

Account
Combination of user name and password that provides an individual with access to a system or network

Application
A software program designed to perform a specific function for one or more users

Approved Reporting Methods
While the preferred method for reporting is abuse@calpoly.edu, to ensure confidentiality, other more secure methods may be used, including contacting the Office of the CIO, Information Security Office, or Service Desk by phone or in person, or submitting a confidential trouble ticket

Auxiliary
Non-State supported and self-support organizations affiliated with Cal Poly
**Availability**
The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it

**Confidentiality**
The need to ensure that information is disclosed only to those who are authorized to view it

**Data**
Individual facts, statistics or items of information represented in either electronic or non-electronic forms

**Enterprise Production Service**
Application or system that provides simultaneous services to a large number of users, typically over a network

**External or Third Parties**
Include, but are not limited to, contractors, service providers, carriers, vendors, and those with special contractual agreements or proposals of understanding with Cal Poly; as well as entities not affiliated with Cal Poly such as Internet Service Providers, government agencies, businesses, and organizations

**Incident**
Any event, successful or unsuccessful, that threatens or has the potential to negatively impact the confidentiality, integrity or availability of university information assets; an event that results in the unauthorized access, use, disclosure, modification, or destruction of information assets; intentional denial of authorized access; interference with system operations; or inappropriate use of IT resources; any violation of information security or IT related policies or standards may be considered an incident

**Information Asset**
Information systems, data, and network resources to include automated files and databases

**Information Security**
Protecting the confidentiality, integrity and availability of information assets from unauthorized access, use, disclosure, disruption, modification or destruction

**Information System**
A combination of hardware, network and other information technology resources that are used to support applications and/or to process, transmit and store data

**Integrity**
The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete

**Malicious Software**
Software designed to damage or disrupts information assets
**Network**
A series of points or nodes interconnected by communication paths that can transmit data, voice, or video signals; includes network devices such as routers, switches, wireless access points, firewalls; the transmission method such as fiber optic cable; and any associated transmission capability (bandwidth)

**Network, System or Application Administrator (LAN Coordinator)**
The individual responsible for administering, managing, operating or supporting an application, network, information system or other university information asset

**Personally Identifiable Information**
Any information that identifies or describes an individual, including but not limited to first name or initial and last name in combination with one or more data elements, such as Social Security number, driver’s license, birth date, account numbers, physical description, address, phone number, financial matters, medical or employment history (California Information Practices Act)

**Security Breach**
The unauthorized acquisition or disclosure of data that compromises the confidentiality, integrity or availability of personally identifiable information maintained by Cal Poly in an unencrypted form; may require notification to affected users in accordance with applicable laws

**Threat**
A person or agent that can cause harm to an organization or its resources, including other individuals or malicious software acting on behalf of the original attacker

**User**
Anyone or any system with access to Cal Poly information assets

**Roles and Responsibilities:**

**Incident Response Team**
- Membership will vary depending on the nature of the incident but at minimum will include members of the IT Policy/Abuse Team and the Information Security Office as needed
- Coordinates incident response activities, involving others as needed
- Receives complaints sent to abuse@calpoly.edu
- Creates, updates, maintains and resolves confidential tickets to document each incident
- Requests additional information if necessary
- Determines the nature, scope and severity of the incident
- Blocks and restores network access or authorizes others to do so as appropriate
- Identifies the potential source of the problem and the responsible university entity or user
- Notifies the responsible entity or user and consults with them on actions to be taken
- Monitors progress of the investigation
- Escalates incidents as appropriate
- Facilitates communications
- Creates summary reports for management
- Conducts lessons learned to determine if any changes are required
• Provides training to campus staff involved in incident response

**Information Security Management Team**

• Coordinates Incident Response Team assignment and ensures it has the necessary resources
• Coordinates investigation, assessment, tracking, resolution and reporting of security incidents classified as Critical or High, including evidence collection and preservation
• Determines if a reportable security breach occurred and enacts security breach protocol
• Determines if a university production service should be taken offline until incident resolution after consultation with appropriate campus entities if possible
• Determines if an incident may result in media inquiries or legal action and escalates to Public Affairs, University Legal Counsel and/or University Police if appropriate
• Keeps executive management informed as appropriate
• Reviews and analyzes summary reports to identify trends and lessons learned

**Campus Compliance Officers (FERPA, HIPPA, PCI, ADA, etc.)**

• Participates in the Incident Response Team for incidents involving a compliance issue
• Investigates, documents and reports violations in accordance with established practices
• Coordinates required notifications in accordance with established practices
• Makes recommendations to prevent similar incidents and/or improve the response process
• Advises management on applicable policies and procedures, including potential sanctions
• Participates in lessons learned as requested

**Technical Staff (Network, System and Application Administrators, LAN Coordinators)**

• Monitors networks, systems and/or applications for anomalies, intrusions, and/or unexpected events or unusual behavior that could reasonably raise suspicious of potential compromise
• Reports potential violations to abuse@calpoly.edu
• Assists in investigating incidents involving networks, systems and applications under their control
• Collects and preserves evidence and provide support as needed throughout the investigation
• Documents any breaches, especially those involving high-risk or confidential data
• Conducts forensic investigations as required or appropriate
• Works to contain, remediate, resolve and document security incidents
• Identifies root cause, including responsible individual, if possible
• Documents findings and actions taken and reports back to the Incident Response Team
• Participates in lessons learned as requested
• Makes recommendations to prevent similar incidents and/or improve the response process

**Users**

• Reports suspected violations to abuse@calpoly.edu
• Follows instructions from the Incident Response Team to preserve evidence, prevent further damage, and/or to otherwise aid the investigation as directed
• Users whose actions result in an incident may be subject to disciplinary action and may be required to review policies or undergo training

It is the responsibility of all Cal Poly faculty, staff, students and affiliates to report potential incidents, IT policy violations and breaches of university information security to abuse@calpoly.edu.

Information Authority/Owner
• Supports the Incident Response Team in reporting, investigating, assessing and resolving potential policy violations and security incidents
• Determines if an enterprise production service may be taken off-line

Information Security Coordinators
• Supports the Incident Response Team in reporting, investigating, assessing and resolving potential policy violations and security incidents
• Serves as escalation point to ensure cooperation by users and technical staff in their area

Management
• Supports the Incident Response Team in reporting, investigating, assessing and resolving potential policy violations and security incidents
• Determines if localized production services may be taken off-line
• In consultation with the Information Security Officer, notifies affected users when a security breach requiring notification originates from an individual or system under their control
• Applies sanctions and discipline in accordance with existing policy and practice in coordination with Human Resources, Academic Personnel or Office of Student Rights and Responsibilities
• Participates in lessons learned as requested
• Makes recommendations to prevent similar incidents and/or improve the response process

Employment Equity/Human Resources/Academic Personnel/Office of Student Rights and Responsibilities
• Investigates alleged policy violations and security incidents stemming from actions taken by individual staff, faculty and students to determine if disciplinary action is appropriate
• Authorizes activities affecting accounts or files of individuals under investigation or found to be responsible for a policy violation or security incident, including but not limited to,
  o Temporary suspension of accounts
  o Early termination of accounts
  o Retention and review of electronic or other files
• Advises management on applicable policies and procedures, including potential sanctions
• Participates in lessons learned as requested

University Legal Counsel
• Authorizes litigation holds and notifies affected parties regarding their responsibilities
• Interprets the law and advises on potential legal or other risks to the university
• Reviews search warrants or other legal requests for validity prior to campus response
• Serves as escalation point for advice on legal matters outside the purview of the team

University Police
• Investigates incidents involving potential criminal activity, including theft of university property
• Assists in obtaining search warrants, subpoenas, and other legal documents as requested
• Coordinates contact with outside law enforcement agencies
• Serves as escalation point for incidents involving immediate threat to physical safety

Public Affairs
• Coordinates communications and contacts between the university and the media
• Serves as escalation point if a security breach notification is required
• Serves as escalation point if an incident is likely to affect public confidence

Executive Management
• Serves as escalation point if a security breach notification is required
• Serves as escalation point if an incident is likely to affect public confidence

Related Procedures and Resources:
• Incident investigation protocols and containment strategies (evidence collection, handling and storage; problem ID, remediation and mitigation strategies) [NEW]
• Policies, Standards, Guidelines and Procedures
• Federal and State Laws
• RUP Implementation and Practices, including Security Breach Notification Process
• SPAM Reporting
• Virus Reporting and Response Procedures
• DMCA Procedures: Cal Poly’s Response to Copyright Infringement Claims
• Procedures for Removing Networked Devices [pdf]
• Litigation Holds Guidelines