8075.S000 Information Security Incident Management

Implements:	CSU Policy #8075.0
Policy Reference:	8075.00 Information Security Incident Management

Introduction

Incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff who are capable of investigating and developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

1.0 Campus Incident Management Plans

Each campus must develop incident management plans and procedures that include, at a minimum, the following:

1.1 ***Identification of a Computer Security Incident Response Team (CSIRT)***. Each campus shall identify the positions responsible for responding to an incident.

1.2 ***Protocol for escalation and internal reporting***. Campus procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that:

a) Appropriate campus officials are informed about appropriate security incidents.

b) The CSIRT is assembled.

c) The incident is addressed in the most expeditious and efficient manner.

d) Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is reported immediately to the CSU Chief Information Security Offer.

1.3 ***Procedures for investigating an incident***. Each campus must document and develop appropriate procedures and processes for investigating information security events and incidents. These procedures must include minimal investigative requirements required to determine if protected information was stored on or accessible by a potentially compromised system. Campuses must document the mitigation process after identifying vulnerabilities on previously deployed systems.

1.4 ***Post incident analysis.*** Campuses shall review each incident to identify and apply lessons learned.

2.0 Investigating

Each campus must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. For the purposes of this standard, incidents include, but are not limited to, the following:

2.1 Data (includes electronic, paper, or any other medium):

a) Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any Level 1 or Level 2 data.

b) Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29, HIPAA regulations or other legal or contractual obligation.

c) Deliberate or accidental distribution or release of personal information by a campus, its employee(s), or its contractor(s) in a manner not in accordance with law or CSU/campus policy.

d) Data handling compliance failures that constitute information security risk potential.

2.2 ***Inappropriate Use and Unauthorized Access*** – This includes tampering, interference, damage, or unauthorized access to campus information assets. This also includes, but is not limited to: successful virus attacks, web site defacements, server compromises, and denial of service attacks.

2.3 ***Equipment*** – Theft, damage, destruction, or loss of campus IT equipment, including laptops, tablets, integrated phones, personal digital assistants (PDAs), or any electronic devices containing or storing confidential, sensitive, or personal data.

2.4 ***Computer Crime*** – Use of a campus information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

2.5 Any other incidents that violate campus information security policy or conditions that provide substantial information security risk.

3.0 Evidence Collection and Handling

3.1 Each campus must develop and maintain procedures and processes for evidence handling. At a minimum, the campus plan must describe the campus' access to forensic resources (either internal or through external arrangements) and its criteria for contacting law enforcement.

3.2 If a campus chooses to maintain its own forensic capability, the campus must maintain procedures and processes for ensuring that evidence and/or information collected under circumstances such as a litigation hold, or Public Information Act request is collected, documented and stored in a manner consistent with legal requirements as appropriate.

4.0 Incident Reporting

4.1 Each campus must identify a point of contact (POC) for information security incident reporting. A campus POC can be an individual (e.g., ISO) or an organization [e.g., IT Help Desk or Computer Security Incident Response Team (CSIRT)].

4.2 A formal, centralized method (i.e., email or phone number) for reporting information security incidents to campus POCs must be provided to users. Each campus must identify and communicate means for users and third parties to report suspected incidents. This information must be part of routine security awareness activities. Any user who observes or suspects that an information security incident is occurring with a campus' information assets must promptly report the incident to the campus' POC. Third parties who observe or suspect that an information security incident is occurring with a campus's information asset must promptly report the incident to their campus business contact. A user must not prevent or obstruct another user from reporting an information security incident in the above manner.

4.3 Each campus' POC must implement feedback processes to ensure that those reporting information security incidents are appropriately acknowledged.

5.0 Internal Notifications

5.1 Each campus must inform the CSU CISO of any security incident resulting in exposure of protected information. The notification process must include the following steps:

a) Initial notification informing the CSU CISO that the campus is investigating a potential breach. This notification must be made immediately. If notice is made via voice, the campus must provide an email message confirming that the notice has been made and providing the required elements of § 5.1(b).

b) The initial notification must include the nature of the potential breach, an estimate of the severity – i.e. number of records and types of information at risk of exposure.

c) On completion of the incident risk assessment, the campus ISO must immediately notify the CSU CISO and the campus whether or not the campus has determined that there is a low probability that protected information has exposed.

d) If protected data has been exposed:

   a. The CSU CISO will then:

      i. Notify CSU Risk Management

      ii. Notify the CSU HIPAA Privacy Officer if appropriate (HIPAA related incidents

      iii. Notify the CSU OGC

      iv. Notify the CSU CIO

      v. Notify the CSU CFO if appropriate (PII or HIPAA related incidents)

   b. The ISO shall

      i. Notify the campus President and CIO as appropriate.

      ii. Notify the campus OGC liaison.

   c. The campus President shall contact the Chancellor.

6.0 External Notifications

6.1 In the case that external notifications are to be made to impacted party(ies), the notification process must include the following steps:

a) A DRAFT copy of the notification must be sent to the CSU CISO for review.

   a. The CSU CISO will then:

      i. Review DRAFT and provide input

      ii. Send the DRAFT to CSU OGC for review and input

      iii. Send updated DRAFT to campus ISO / POC

6.2 In the case that the exposed data contains HIPAA or PII and the impacted group is 500 records or greater, the following steps must occur

a) The ISO will send a DRAFT copy of the notice intended for the appropriate organization (AG, HHS, DOE, Media, etc.) to the CSU CISO.

   a. The CSU CISO will then:

      i. Review DRAFT and provide input

      ii. Send the DRAFT to CSU OGC for review and input

      iii. Send the updated DRAFT to campus ISO / POC for external organization

REVISION CONTROL

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	3/7/2011	Macklin	Incorporates campus and ISAC comments. TBD Clarification on evidence/forensics	14.X
1.0	3/22/2011	Washington	Formerly known as standard “14”. Reformatted and re-arranged text. Add a statement regarding post-event reviews.	All
1.1	1/23/14	Macklin	Updated notification, HIPAA updates	§1, 2, 5
1.2	2/20/14	Perry	Updated notifications	5.1.d, 6

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
3/21/12	ISAC	Recommended
6/5/13	ITAC	Review
7/16/13	Perry (CISO)	~~Approved for posting~~
2/20/14	CISO	Reviewed Approved for posting