Business Practice for Security Incident Response

PURPOSE:

Describe the business process for responding to information security incidents at CSU Channel Islands.

BACKGROUND:

CSU Channel Islands must develop and maintain an information security incident response program that includes processes for investigating, responding to, reporting, and recovering from incidents involving loss, damage, misuse of information assets containing protected data, or improper dissemination of critical or protected data, regardless of the medium in which the breached information is held or transmitted (e.g., physical or electronic). The campus program must:

- Define and/or categorize incidents.
- Designate specific personnel to respond to and investigate information security incidents in a timely manner.
- Include procedures for documenting the information security incident, determining notification requirements, implementing remediation strategies, and reporting to management.
- Include processes to facilitate the application of lessons learned from incidents.
- Support the development and implementation of appropriate corrective actions directed at preventing or mitigating the risk of similar occurrences.

The campus information security incident response plan must be reviewed and documented annually and comply with the CSU Information Security Incident Management Standards. This document describes the information security incident management process and the roles and responsibilities of those involved as required by ICSUAM Policy 8075.0, https://calstate.policystat.com/policy/11773867/latest#autoid-2wevq

CSU Channel Islands utilizes California State University's Information Security Advisory Committee (ISAC) Services. ISAC enables CSU Channel Islands to develop a highly effective and professional information security program in concert with CSU system-wide information security. This policy delineates the roles and responsibilities of campus personnel for security incident response.

Business Practice for Security Incident Response

BUSINESS PRACTICE: Accountability:

AVP for Information Technology Services (CIO)

Applicability:

All users of campus information and campus information systems, including but not limited to students, faculty, staff, alumni, and members of auxiliary organizations. **Definitions:**

Unless otherwise defined by this section, the terms used in this Business Practice are defined in Attachment 1 — CSUCI Incident Response Guideline.

(1) **Information Security Incident**

a. Any known or highly suspected circumstance that results in an actual or possible unauthorized release of information deemed confidential or sensitive by the University or subject to regulation or legislation beyond the University's sphere of control.

(2) Incident Response Team (IRT)

a. These resources will act as the IRT at CSU Channel Islands. These resources should be appointed and in place well before any incident occurs at CSU Channel Islands.

i. AVP for Information Technology Services (CIO) (or designee)
ii. Campus Information Security Officer
iii. Campus Law Enforcement representative
iv. Campus EOC (Emergency Operations Center) Director
v. ITS Help Desk
vi. ITS Network Team
vii. ITS Server Team

Text: ***General***

Unless otherwise specified or defined by this Business Practice, Information Security Incidents at CSU Channel Islands are handled as prescribed in Attachment 1 — CSUCI Incident Response Guideline.

AVP for Information Technology Services

Business Practice for Security Incident Response

Incident Severity Levels

Security incidents at CSU Channel Islands will be categorized into three (3) levels – High, Medium, and Low:

(1) High Severity Incident (Level 1)
   a. An incident is categorized as High/Level 1 if it meets the following criteria:
      i. The incident could have long-term effects on the Campus Community.
      ii. The incident affects critical systems or has a Campus-wide effect.
      iii. The incident could damage the reputation of the University.
      iv. The incident is a violation of State and/or Federal law.
   b. Examples of incidents that would be considered as High/Level 1 Severity include:
      i. Security compromise of Campus enterprise systems or applications
      ii. Cyber-stalking
      iii. Patriot Act violations iv. Loss or theft of Level 1 (Confidential) information
      v. International, Federal, State, or Local law violations, including:
         1. HIPPA
         2. FERPA
         3. Child Pornography

(2) Medium Severity Incident (Level 2)
   a. An incident is categorized as Medium/Level 2 if it meets the following criteria:
      i. The incident indicates a threat of future attack (network reconnaissance)
      ii. The incident has a strong possibility of affecting a large portion of the campus network
      iii. If there's an imminent danger, the incident may modify the public's perception of CSU Channel Islands due to information security reasons other than disclosure of personal and sensitive information or disruption of service.
   b. Examples of incidents that would be considered as Medium/Level 2 Severity include:

i. Loss or theft of Level 2 (Sensitive) information (as prescribed in the University Policy on Data Classification Standards - https://policy.csuci.edu/it/01/it-001-003.htm
ii. Web site defacement
iii. Personal business operations using Campus resources
iv. Unauthorized excessive resource utilization
v. Compromised Faculty/Staff accounts
AVP for Information Technology Services

c. There may be cases where a Medium/Level 2 Severity Incident must be escalated to a higher-level incident based upon the findings of that incident.

(3) Low Severity Incident (Level 3)

a. An incident is categorized as Low/Level 3 if it meets the following criteria:
   i. The incident poses no imminent threat to the California State University, Channel Islands' information systems, or CSU Channel Islands' confidential and sensitive data (as prescribed in the University Policy on Data Classification Standards - https://policy.csuci.edu/it/01/it-001-003.htm
b. Examples of incidents that would be considered as Low/Level 3 Severity include:
   i. Malware/virus-infected system connected to the Campus network
   ii. Copyright infringement notification (RIAS, MPAA, DMCA)
   iii. Illegal sharing of copyrighted materials, including music, movies, and software
   iv. Compromised student accounts
   v. Unauthorized servers including:
      1. Game Servers
      2. Chat Servers
      3. File Servers
      4. DHCP Servers
c. There may be cases where a Low/Level 3 Severity Incident must be escalated to a higher-level incident based on the findings of that incident.

Notification Protocols

(1) If a breach of level 1 data has occurred (level 1 data as prescribed in the University Policy on Data Classification Standards - https://policy.csuci.edu/it/01/it-001-003.htmthe campus The president must notify the Chancellor; the AVP for Information Technology Services (CIO) must notify the Assistant Vice Chancellor for Information Technology Services; the campus ISO must notify the Chief Information Security Officer (CISO) of the system; and Campus Law Enforcement must contact local, State and Federal law enforcement agencies as warranted by the data breach.
(2) If a breach of level 2 data has occurred (as prescribed in the University Policy on Data Classification Standards - https://policy.csuci.edu/it/01/it-001-003.htm), the campus ISO must notify the Chief Information Security Officer (CISO) of the system. The CISO will provide the Chancellor with quarterly status reports on level 2 data breaches that have occurred in the CSU.

Business Practice for Security Incident Response

Vulnerability Reporting *Responsible Disclosure:*

Students, faculty, staff, and others with access to ITS information resources on campus are encouraged to exercise active vigilance in reporting suspected information security vulnerabilities. A person who has information about any information security vulnerability is encouraged to disclose that vulnerability to:

(1) ITS Help Desk at 805-437-8552 or helpdesk@csuci.edu; or
(2) Chief Information Security Officer at infosec@csuci.edu

Pursuant to the University Policy on Data Classification Standards (https://policy.csuci.edu/it/01/it-001-003.htm), information pertaining to vulnerabilities in University information systems are classified Level 2 – Internal Use.

Incident Reporting

Any person who knows or suspects that an information security incident is in progress must immediately report that incident to:

(1) ITS Help Desk at 805-437-8552 or helpdesk@csuci.edu; or
(2) Chief Information Security Officer at infosec@csuci.edu

Furthermore, any ITS staff member who is advised of a known, suspected, or anticipated information security incident must notify their supervisor and the AVP for Information Technology Services (CIO).

Any ITS staff to which an incident is reported must -

(1) Collect the following information from the source reporting the incident:

a. Identifying information
   i. Name of the person reporting the incident
   ii. Job title (if applicable) of the person reporting the incident
   iii. Contact information (phone number, email, office location, etc.) of the person reporting the incident
b. Brief description of the incident being reported.
   i. Start date and time when the incident was discovered.
   ii. How the incident was discovered
c. All known parties to the incident, including those in and outside of the University, and their contact information,

(2) Provide a reminder to the person reporting the incident that the details of the incident are classified Level 1 — Confidential and
(3) Transmit that information via Help Desk ticket to the Chief Information Security Officer or designee as Priority 1 – 4 Hour Response.

Pursuant to the University Policy on Data Classification Standards (https://policy.csuci.edu/it/01/it-001-003.htm), information pertaining to suspected, anticipated, or actual information security incidents are classified as Level 1 – Confidential.

Information Security Incident Reporting and Vulnerability Disclosure:

Prohibition on use for disciplinary action

(1) The AVP for Information Technology Services (CIO) may not use information disclosed to ITS concerning information security incidents or vulnerabilities for disciplinary action against ITS staff members.

(2) The prohibition in paragraph (a) does not apply to:

a. Deliberate actions that cause or permit an incident to occur or details of a vulnerability to be opened or irresponsibly disclosed to an outside party,
b. Criminal actions and
c. Conduct that is careless or reckless to endanger the information security of the University or the life or property of another.

Incident Classification and IRT Activation The IRT Lead will, within 24 hours, determine:

(1) If the incident is a High (Level 1), Medium (Level 2) or Low (Level 3) level incident
(2) If the security incident warrants the activation of the IRT or can be handled without full IRT activation and
(3) The severity of that incident, in accordance with Section 3.0 of Attachment 1 – CSCUI Incident Response Guideline.

IRT will always be activated to respond to High (Level 1) and Medium (Level 2) severity incidents.

Incident Review and Reports
After the conclusion of each information security incident, the ITS Chief Information Security Officer will issue an incident report containing facts, findings, and recommendations. Incident reports are classified as Level 1 – Confidential.

Business Practice for Security Incident Response

ITS Information Security incident reports are inquisitorial in nature and intended to present narrative information along with the results of incident investigation. To the extent practical, actors named by reports are de-identified and the reports are not intended to fix responsibility for an information security incident in an adversarial manner.
ITS Information Security incident reports are retained indefinitely. The AVP for Information Technology Services (CIO) may authorize the release of incident reports to those persons outside of ITS with a need to know.

Implementation:
Initial training of required personnel:

(a) The Manager of ITS User Services shall certify that:
  (1) Each ITS Help Desk employee has reviewed the University Policy on Data Classification Standards (https://policy.csuci.edu/it/01/it-001-003.htm) and the portions of this Business Practice that pertains to incident reporting to the ITS Help Desk and
  (2) ITS Help Desk training materials and operating manuals have been revised to incorporate information security incident response and the portions of this Business Practice that pertain to incident reporting to the ITS Help Desk.

(b) The Manager of ITS Infrastructure shall certify that:
  (1) Each member of ITS Infrastructure has reviewed the University Policy on Data Classification Standards (https://policy.csuci.edu/it/01/it-001-003.htm) and the portions of this Business Practice that pertain to incident reporting to the ITS Help Desk.

(c) The Information Security Officer shall certify that:
  (1) Each member of ITS has access to review the University Policy on Data Classification Standards (https://policy.csuci.edu/it/01/it-001-003.htm) and the portions of this Business Practice that pertain to incident reporting to the ITS Help Desk.

Exhibits:

Attachment 1 - CSUCI Incident Response Guideline
Attachment 2 – Incident Process Flow Diagram

Assessment Requirements:

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
General review of business practice	Annual – July	ISO

Revision History:

BP Nbr:	BP-01-008	**Enacted Date:**	03/06/2013		
Revision Nbr:	001	**Revision Date:**	05/11/2016	**Revised By:**	Neal Fisch
	002		02/02/2017		Neal Fisch
	003		11/06/2023		Carlos Miranda