Electronic Security Incident Reporting Procedure	Procedure No.	ITS-2018-P	Rev	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	1-29-15	Revised:	
				Page 1 of 10

Table of Contents

1. General Scope and Responsibilities

The purpose of this document is to provide information to guide users in reporting electronic security incidents. Security incidents will happen and the ability to quickly identify and act in a coordinated manner are required to:

- Counteract security violations;
- Remediate activities that lead to security breaches; and
- Prevent the potential spreading of malware throughout the campus.

By following the procedure outlined in this document, it will be possible to return to a normalized and secure state as quickly as possible while minimizing the adverse impact to the University.

2. Entities Affected by This Standard

This document applies to all University employees, Auxiliary Services and third-party service providers.

3. Definitions

a) Breach: Infraction or violation of a law, regulation, guideline, policy or standard.

b) Campus Security Incident Response Team (CSIRT): The name given to the team that handles information security incidents of any type of media.

c) Confidential Information: See Level 1 Confidential Data and Level 2 Internal Use Data.

d) CSIRT Director (also called CSULA-CSIRT Director): The campus CSIRT director is the director of IT Security and Compliance.

e) Family Educational Rights and Privacy Act of 1974 (FERPA): A federal legislation in the United States that protects the privacy of students' personally identifiable information and applies to all educational institutions that receive federal funds.

f) Health Insurance Information: An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history, including any appeals records.

g) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

h) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information many not be released except under certain prescribed conditions.

i) Level 3 Public Data: This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. Publicly available data may still be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

   A student may exercise the option to consider directory information, which is normally considered public information, as confidential per the Family Educational Rights and Privacy Act (FERPA). Directory information includes the student's name, address, telephone listing, email address, photograph, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, grade level, enrollment status, degrees, honors and awards received, and the most recent educational agency or institution attended by the student. For bargaining unit student employees, directory information also includes: the name of the department employing the student, the student employee's telephone listing within the department, the student employee's email address within the department and the student employee's job classification.

j) Malware: Software of malicious intent/impact such as viruses, worms and Spyware.

k) Medical Information: Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional.

l) Personal Information: California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:

   - Social Security number
   - Driver's license or California Identification card number
   - Account number, or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
   - Medical information
   - Health insurance information

m) Proprietary Information: Information that an individual or entity possesses, owns or for which there are exclusive rights. Examples include: faculty research, copyrighted or patented materials, white papers, research papers, business continuity and other business operating plans, email messages, vitae, letters, confidential business documents, organization charts or rosters, detailed building drawings and network architecture diagrams. Proprietary information, if lost or stolen, could compromise, disclose or interrupt operations, or embarrass the individual or the University.

n) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential data and Level 2 Internal Use Data.

o) Security Breach: Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained on it.

p) Security Incident: An event that results in any of the following:

- Unauthorized access or modification to CSULA information assets.
- An intentional denial of authorized access to CSULA information assets.
- Inappropriate use of CSULA's information systems or network resources.
- The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations.

q) Social Engineering: The art of using trickery or deception to manipulate individuals into divulging confidential or personal information.

r) User: Users are one or more of the following:

- Anyone or any system that accesses Cal State L.A. information assets.
- Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community.
- Individuals who are given access to sensitive data and have a position of special trust and as such are responsible for protecting the security and integrity of those data.

4. Requirements

Report all electronic security incidents promptly and to the appropriate parties as cited in Section 5 below. Any delay in reporting the incident could result in broadening or accelerating the problem to other campus users and possibly reaching off-campus sites.

Never personally attempt to remediate the symptoms, actions or damage from an incident as this could unintentionally escalate the effects of the initial incident.

Never remediate or reimage a computer before the CSULA-CSIRT team has evaluated the situation to determine the residual impact on the network and the presence of Levels 1 and 2 confidential data.

4.1 Electronic Security Incident Symptoms

Symptoms that may indicate an electronic security incident is occurring or has occurred include, but are not limited to:

- Logins into dormant accounts (one of the best SINGLE indicators).
- Physical theft and intrusion (e.g., theft of laptop computer, tablet or electronic storage media with critical information).
- Applications and/or windows opening without user prompting.
- Generation of spontaneous emails.
- Strange characters appearing in documents.
- System reboots or shuts down for no apparent reason.
- Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources).
- Defaced web pages.
- Virus attacks which adversely affect one or more computers, servers or workstations.

- Accounting/system/network logs discrepancies that are suspicious (e.g., gaps/erasures in the accounting log in which no entries whatsoever appear; user obtains root access without going through the normal sequence necessary to obtain this access).
- Use of attack scanners, remote request for information about systems and/or users, or social engineering attempts.
- New user accounts not created by system administrators.
- New files or unfamiliar file names.
- Modifications to file lengths or dates (especially in system executable files).
- Attempts to write to system files or changes in system files.
- Modification or deletion of data.
- Changes in file permissions.
- Denial of Service (e.g., inability of one or more users to login to an account; inability for customers to obtain information or services via system).
- Abnormally slow or poor system performance.
- Unauthorized operation of a program or sniffer device to capture network traffic (e.g., presence of cracking utilities).
- Unusual time of usage (Remember, more computer security incidents occur during non-working hours than any other time.).
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program; use of commands/functions not normally associated with user's job).

4.2 Breach Notification

Cal State L.A. is required by California Civil Code 1798.29 and 1798.82 to immediately notify upon discovery any California resident whose unencrypted and computerized personal information (Levels 1 and 2 data) was, or is reasonably believed to have been, acquired by an unauthorized person because of a breach of the security of the systems or data that contains such information. In the case of a breach or possible breach of data, Cal State L.A. has chosen to notify any individual, whether they are a resident of California or not.

5. Procedures

All incidents, whether major or minor, must be reported immediately to the ITS Help Desk or the director of IT Security and Compliance. If an electronic security incident is suspected or may be imminent, the following actions are required:

5.1 Information Technology Consultants (ITCs)

- Respond to calls from users as a priority one event.
- Have the user cease use of the computer immediately since continued use may inadvertently damage potential evidence in the event that the electronic security incident becomes part of a criminal case.
- Immediately contact the ITS Help Desk at 323-343-6170 or the director of IT Security and Compliance at 323-343-2600 to verbally report the incident. Avoid evaluating whether the incident is minor or major and making determinations that some incidents do not need to be reported. **All incidents must be reported**.
- For incidents occurring after normal working hours, also send an immediate email to itsecurity@calstatela.edu.

- The initial report should include as much of the following information as is available at the time:
  - The date and time of detection.
  - Room or area and department in which the incident occurred.
  - Who discovered the incident.
  - Brief description of the incident and type of data involved (e.g., student information, SSNs, etc.).
  - Names of shared resources, network drives or servers connected to the computer at the time of infection.
  - List of additional networks to which the computer has access.
- Follow any initial guidance provided by the ITS Help Desk or the director of IT Security and Compliance, such as disconnecting the affected information technology device from the network or taking other actions that will otherwise limit damage to other IT resources.
- Notify the user's department administrator of the incident.
- Complete form *ITS-2812 Information Security Initial Incident Report* immediately, even if all information regarding the incident has not been gathered, and send by one of the following methods:
  - FAX 323-343-2602
  - Email itsecurity@calstatela.edu (preferred method)
  - Address CSULA-CSIRT
IT Security and Compliance
Information Technology Services, LIB PW 1070
California State University, Los Angeles
5151 State University Drive
Los Angeles, CA 90032
- Do not reimage the computer until the CSULA-CSIRT completes an investigation and has given approval to reimage. It is mandatory to determine whether the computer contains Level 1 or Level 2 data prior to reimaging.

5.2 Users

- Cease use of the computer immediately since continued use may inadvertently damage potential evidence in the event that the electronic security incident becomes part of a criminal case.
- Contact your assigned ITC or, if you do not have an ITC, immediately contact the ITS Help Desk at 323-343-6170 or the director of IT Security and Compliance at 323-343-2600 to verbally report the incident.
- Follow any initial guidance provided by the ITC, ITS Help Desk or the director of IT Security and Compliance, such as disconnecting the affected information technology device from the network or taking other actions that will otherwise limit damage to other IT resources.
- Always create and retain a current backup of data files on the workstation in the event the workstation must be cleaned and reimaged. Do not attempt to create or update the backup after the incident occurs as the backup may become unusable.

5.3 Breached Department Representative

Once the CSULA-CSIRT team completes their investigation and determines that a reportable breach has occurred, the CSULA-CSIRT director will request the department administrator to designate a "breached department representative" for the incident. The breached department representative serves as the contact between the department and the ITS CSULA-CSIRT coordinator. The breached department representative should:

- Notify appropriate individuals of the incident within the department (e.g., supervisor, Information Technology Consultant, system administrator, etc.).
- Manage the breach notification process, if necessary.
- Follow the steps outlined in form *ITS -2817 Department Representative's CSULA-CSIRT Checklist.*
- Provide ongoing updates to the CSULA-CSIRT director and prepare the final report on the incident status by using form *ITS -2819 Information Security Incident Status Report.*

5.4 ITS Help Desk

The ITS Help Desk is the initial point-of-contact for collecting appropriate information about suspected or actual electronic security incidents. The ITS Help Desk will notify the CSULA-CSIRT director of the incident, or if the incident is passed directly to an ITS technical expert, will copy the CSULA-CSIRT director on the request.

5.5 Campus Security Incident Response Team (CSULA-CSIRT)

The mission of the CSULA-CSIRT is to lessen the potential impact of information driven incidents by ensuring that the response to the events is coordinated, consistent and appropriately communicated. A central incident response team shall be assembled when there is creditable evidence of an incident. One or more team members, depending on the magnitude of the incident and availability of personnel, from throughout the organization will handle the incident. The CSULA-CSIRT shall collaboratively work together as a team to identify the source and scope of the information security breach using the technical expertise of all individuals.

The CSULA-CSIRT director performs high-level direction of the team's overall activities including confirming the incident, as well as assigning a CSULA-CSIRT coordinator. The CSULA-CSIRT coordinator manages the CSIRT teams' overall response and recovery activities. Upon notification of an incident, ITS personnel will create and maintain a problem ticket and follow escalation procedures as specified in *ITS-2511 Campus Security Incident Response Team (CSIRT)*.

6. Quality Assurance Provisions

6.1 Customer Relations Management

In the event that an incident is not reported, the procedure used does not adhere to this document, or any incident corrective actions planned are not completed, the director of IT Security and Compliance is responsible for notifying the user or other appropriate individuals of the proper actions to be taken.

6.2 Configuration Management

Not applicable to this procedure.

6.3 Change Management

ITS technical staff may monitor or test any system or operational changes as a result of the response to the incident to ensure that any changes or remediations are appropriate in mitigating all identified vulnerabilities and that the affected systems are returned to an operationally ready state.

6.4 Disaster Recovery/Business Continuity Management

When collected evidence must be preserved, a clearly defined chain of custody shall be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence.

All actions to remediate the problem and notify affected individuals, if applicable, must be documented and copies of reports must be securely stored in such a manner as to be retrievable and, if stored electronically, there must be a secured backup copy.

6.5 Security Management

Incidents are to be managed in compliance with state and federal laws and regulations, CSU policy and campus standards and guidelines and in a manner that limits University risk. Information contained in information security incident reports is confidential and should be maintained and safeguarded as Level 1 Confidential Data.

The handling, retention and disposal of incident information must follow all University guidelines for managing protected data.

6.6 Accounting Management

If it is determined that costs for the breach will be tracked, cost data must be captured and retained using form *ITS-2821 Information Security Incident Cost Estimate*. Colleges and departments are responsible for any losses or costs associated with managing the security incident as required by California Civil Code Sections 1798.29, 1798.82, 1798.84 and 1798.85.

6.7 Fault Management

While users are expected to identify electronic security incidents, immediately report an incident, and take corrective action as requested by ITS or their ITCs, all CSIRT designees who are involved in the handling of such incidents are expected to be vigilant when handling such incidents, as well as in the prediction and prevention of future incidents.

Any corrective actions identified or recommended for systems to prevent future occurrences must be implemented by the appropriate department.

6.8 Efficiency/Effectiveness Management

The effectiveness of this procedure can be measured in the number of incidents not immediately reported each quarter. It is the intent of Cal State L.A. to have all incidents reported immediately. Failure to meet this expectation will require ITS to evaluate current communications and education of users regarding electronic security incident reporting.

7. Contacts

a) For questions regarding general information technology security, contact IT Security and Compliance at ITSecurity@calstatela.edu.

b) For technical assistance contact the ITS Help Desk at 3-6170.

c) For questions regarding specific department procedures, contact the department administrator.

d) For questions regarding specific technical procedures, contact the department Information Technology Consultant.

8. Applicable Federal and State Laws and Regulations

Federal	Title
NA	
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved.

9. Related Documents

CSULA	Title
ITS-1008-G	**User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1008-G_Lost-StolenComputerGuidelines.pdf This guideline outlines the steps users must take to ensure the campus complies with all laws and regulations regarding personal and confidential information when desktop or laptop computers and electronic storage devices are lost or stolen.
ITS-2511	**Campus Security Incident Response Team** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-2511_CSULA_CSIRT.pdf This document defines the steps to effectively respond to information security incidents, minimize disruption and return operations to a normal state.
ITS-2812	**Information Security Initial Incident Report** http://www.calstatela.edu/its/forms Form used by departments to report an actual or suspected security incident to IT Security and Compliance.
ITS-2817	**Information Security Breach – Department Representative Checklist** http://www.calstatela.edu/its/forms Form used by the CSIRT Department Representative to document actual steps performed and strategies used to contain, eradicate and recover from a security incident.
ITS-2819	**Information Security Incident Status Report** http://www.calstatela.edu/its/forms Form used by the CSIRT department representative to record incident updates and prepare the final status report.
ITS-2821	**Information Security Incident Cost Estimate** http://www.calstatela.edu/its/forms Form to categorically document time and material costs for handling a security incident.