Campus Security Incident Response Team (CSIRT)				
	Document No	ITS-2511	Rev	B
	Owner	IT Security and Compliance		
	Approved by	Sheryl Okuno, Director IT Security and Compliance		
	Issued	7-21-10	Revised	5/3/2017
				Page 1 of 17

Table of Contents

1. Purpose 3
2. Related California State University Policies and Standards 3
3. Entities Affected by These Guidelines 3
4. Definitions 4
5. Standards 5
   - 5.1 Mission 5
   - 5.2 Roles and Responsibilities 6
     - 5.2.1 Director 6
     - 5.2.2 Coordinator 7
     - 5.2.3 Breached Department Representative 7
     - 5.2.4 Executive Officers and Vice Presidents 8
     - 5.2.5 Ad Hoc Members 9
     - 5.2.6 Internal Ad Hoc Members 9
     - 5.2.7 External Ad Hoc Members 9
     - 5.2.8 Technical Team 9
   - 5.3 Activities 9
   - 5.4 Incidents 10
     - 5.4.1 Incident Prioritization 10
     - 5.4.2 Incident Notification 11
     - 5.4.3 Incident Reporting 12
     - 5.4.4 Incident Response 12
   - 5.5 Information Disclosure 13
     - 5.5.1 Classification of Information 13
     - 5.5.2 Types of Groups 14
     - 5.5.3 Advance Notification to the Media 14
     - 5.5.4 University Community Announcements 14
     - 5.5.5 Breach Notification 15

6. Contacts 16
7. Applicable Federal and State Laws and Regulations 16

1. Purpose

The purpose of this document is to establish the California State LA Computer Security Incident Response Team (CSIRT) to ensure effective response to information security incidents and assist in the protection of University protected data from loss and disruption of operations

Rapid response and collective actions are required to:

- Counteract security violations and activities that lead to information security breaches and incidents;
- Return to a normalized and secure state as quickly as possible and
- Minimize the adverse impact to the University.

The Campus Security Incident Response Team is a cross-domain operational group that is responsible for receiving, reviewing and assisting breached departments in responding to information incidents in the most expeditious and efficient manner.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8010.0	**Policy**	**Establishing an Information Security Program**
8075.0	**Policy**	**Information Security Incident Management**
8075.S000	*Standard*	*Information Security Incident Management*

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Entities Affected by These Guidelines

The CSIRT operates under the approval and support of the University president and associate vice president for Information Technology Services. This document applies to all users (students, faculty, staff, administrators, Auxiliary units and others) involved in the reporting and/or handling of information security incidents.

4. Definitions

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

b) Breach of the Security of the System: Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by Cal State LA. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

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

d) 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.

e) Identifying Information: Any name or number that may be used alone or in conjunction with any other information to identify a specific person. Identifying information generally includes name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or unique electronic identification number.

f) Incident Information: Information concerning an incident (e.g., department in which the incident occurred, number of individuals whose protected data may have been compromised, the priority level of the incident, etc.).

g) Intruder Information: Identifying information about someone who intrudes on the privacy or property of another without permission.

h) 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 information to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential data must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

i) 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 may not be released except under certain prescribed conditions.

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

k) 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 number or California Identification Card number.
- Account number, 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.

l) Private Site Information: Technical information about particular systems or sites.

m) 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.

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

o) Security Incident: An event that results in any of the following:
- Unauthorized access or modification to Cal State LA information assets.
- An intentional denial of authorized access to Cal State LA information assets.
- Inappropriate use of Cal State LA's information systems or network resources.
- Inappropriate disclosure of Cal State LA data.

p) User: Users are one or more of the following:
- Anyone or any system that accesses Cal State LA 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.

q) Vulnerability Information: Technical information about vulnerabilities or attacks, including fixes and workarounds.

5. Standards

5.1 Mission

The mission of the 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. The CSIRT will:

- Coordinate and oversee the response of departments in which the incident occurred.

- Ensure that the response is in accordance with the requirements of state and federal laws, CSU policy, and University guidelines and standards.
- Minimize the potential negative impact to the University as a result of such incidents.
- Restore services to a normalized and secure state of operation.
- Provide clear and timely communication to all affected parties.

5.2 Roles and Responsibilities

A computer security incident response team (CSIRT) 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 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 CSIRT consists of a director, a coordinator, a department representative, the executive officers, ad hoc team members and a technical team.

5.2.1 Director

The director position is filled by the director of IT Security and Compliance and reports to the associate vice president for Information Technology Services.

The CSIRT director performs high-level direction of the team's overall activities. This position:

- Confirms that an incident has occurred and utilizes form ITS-2813 to assign an incident tracking number.
- Immediately notifies the associate vice president for Information Technology Services of the incident.
- Assigns the CSIRT coordinator.
- Serves as a substitute for the coordinator, when the coordinator is unable to perform the assigned duties.
- Utilizes form ITS-2815 *CSIRT Director Checklist* to assign and manage the director's incident tasks and responsibilities.
- Distributes form ITS-2820, *CSIRT Incident Evaluation Form* (adding the incident tracking number to each form), to each member of the team following the resolution of an incident.
- Reviews the completed ITS-2820 *CSIRT Incident Evaluation Forms* to determine the effectiveness of the team, to improve CSIRT processes and to ensure that the team is meeting the needs of the constituency.
- Proposes changes to current policies, guidelines, standards or procedures.
- Acts as the first level of appeal for community members who wish to appeal the actions of the CSIRT. The associate vice president for Information Technology Services serves as the final appeal.
- Collects statistics concerning incidents that occur in, or involve, the University community and annually submits ITS-2822 *Information Security Incident Statistics Report* to the associate vice president for Information Technology Services.

- Ensures that those individuals who report information security incidents are appropriately acknowledged and notified of an incidents resolution.
- In conjunction with the coordinator, acts as liaison between the CSIRT, the University and other CSU-CSIRT teams.
- In conjunction with the coordinator, issues alerts, advisories, guidelines or technical procedures to the University about certain actions to take to reduce vulnerabilities that were exploited during the incident.
- Notifies the CSU Information Security Officer of the incident and resolution, and submits any required written report.

5.2.2 Coordinator

A member of the IT Security and Compliance department shall serve as the coordinator. This position reports to the CSIRT director. When the CSIRT coordinator is unable to perform the assigned duties of that position, the director shall substitute for the coordinator.

The CSIRT coordinator manages the team's overall response and recovery activities for all security incidents. This position:

- Determines the category and priority of each incident.
- Receives an incident tracking number from the CSIRT director and provides the number to the breached department.
- Determines the members needed for the team, completes ITS 2814 *CSIRT Membership List*, and submits a copy to the CSIRT director for approval to proceed with team assembly.
- Utilizes form ITS-2816 *CSIRT Coordinator Checklist* to assign tasks to the CSIRT.
- Ensures that the incident is addressed in the most expeditious and efficient manner.
- Maintains ITS-2818 *Information Security Incident Action Log* throughout the incident response to document each action taken and the action execution timeframe.
- In conjunction with the CSIRT director, acts as a liaison between the CSIRT and the University and other CSU-CSIRT teams.
- In conjunction with the CSIRT director, issues alerts, advisories, guidelines or technical procedures to the University about certain actions to take to reduce vulnerabilities that were exploited during the incident.
- If breach notification is required:
    - Provides the breached department representative the template for breach notifications
    - Ensures notification is timely, clear and concise
    - Ensures the notification and has been appropriately reviewed by the Office of Communications and Public Affairs prior to being sent.

5.2.3 Breached Department Representative

The department in which the incident occurred shall appoint a department representative. This individual will:

- Serve as the contact between the department and the CSIRT.

- Designate other department participants (e.g., Information Technology Consultants, individual directly involved in or by the incident, vendors of compromised systems, etc.).
- Utilizing form ITS-2817 *Information Security Incident – Department Representative Checklist*, coordinate actions to be taken by the department in response to the incident.
- Ensure that the department has completed all actions required in response to the incident in the most expeditious manner.
- Determine if costs for breach will be tracked. If so, ITS-2821 *Information Security Incident Cost Estimate* form will be used to capture cost data.
- Complete and submit ITS-2819 *Information Security Incident Status Reports* to the CSIRT director.
- If breach notification or advance notification to the media is required:
  - Request the template for breach notifications from the coordinator
  - Prepare the notification
  - Ensure the notification is timely, clear and concise
  - Ensure the notification has been appropriately reviewed by the Office of Communications and Public Affairs prior to being sent.

Important Notification Note:

1. If criminal activity is suspected or confirmed, University Police must be consulted to determine if breach notification or advance media notification can occur or if it must be delayed because it will compromise their investigation.
2. If more than 500 California residents are to be notified of a security breach as a result of a single breach of the security system, the breached department representative shall electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the State Attorney General.

- Prepare for responding to inquiries in a consistent and timely manner if a large number of inquiries are anticipated.

5.2.4 Executive Officers and Vice Presidents

The associate vice president for Information Technology Services is responsible for immediately notifying the vice president for Administration and CFO, or the President in the absence of the vice president, of an incident. The President is responsible for immediately notifying the CSU Chancellor of the incident.

The executive officers are responsible for executive endorsement and top-down communications of the information security program. Management support is shown in the approval of budget requests above

the level delegated to the CSIRT director and in the commitment of their staff to participate actively in the CSIRT process, when needed. The executive officers also allow for the appropriate University officials to remain informed about information security incidents.

The associate vice president for Information Technology Services serves as the final appeal of the actions of the CSIRT, if the initial appeal regarding the actions of the CSIRT submitted to the director of IT Security and Compliance is unsatisfactory.

5.2.5 Ad Hoc Members

Ad hoc members are temporary team members and are convened, as needed, depending upon the nature of the incident. These members are the subject-matter experts for particular systems, applications and business issues involved in the incident. Temporary team members are assigned to an incident by their managers at the request of the CSIRT coordinator and serve on the CSIRT until released by the CSIRT coordinator or for the duration of the incident, whichever comes first.

5.2.6 Internal Ad Hoc Members

Internal ad hoc members may include, among others, the University auditor; University counsel; executive director of Communications and Public Affairs; assistant vice president, Human Resources Management; registrar; director of Risk Management/Environmental Health and Safety; and a representative from the reporting entity.

5.2.7 External Ad Hoc Members

External ad hoc members may include, among others, representatives from the CSU Chancellor's Office; Common Management Systems (CMS); University Police (local to incident); FBI, Secret Service, or other forensic specialists; the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA) or Entertainment Software Association (ESA); and the Digital Millennium Copyright Act (DMCA) Enforcement Office.

5.2.8 Technical Team

The technical team consists of security analysts, senior network analysts, operations specialists and desktop specialists from Information Technology Services (ITS). The technical team remains informed regarding changing legislative requirements for information security; hardware and software requirements for intrusion detection and intrusion prevention; user awareness training; and forensic tools. In addition, members of the technical team participate in all ITS projects to ensure information security compliance and security best practices are incorporated during the planning and implementation phases.

5.3 Activities

Although the main role of the CSIRT is to respond to incidents, members of the CSIRT may coordinate the following services to the extent possible and depending on the availability of resources:

- Propose to the CSIRT director and coordinator alerts, advisories, guidelines, or technical procedures for the University about certain actions to take to reduce vulnerabilities that were exploited during the incident.
- Evaluate the risk of compromised systems being online, or accessed, against the risk of shutting them down.
- Provide a repository of vendor-provided and other security-related patches for various operating systems.
- Provide a repository of security tools and related documentation.

5.4 Incidents

Suspected incidents can be discovered in various ways, such as normal monitoring or via a report from inside or outside the organization. Information Technology Services should have industry-standard tools in place to monitor system and network activity. Information Technology Consultants (ITCs) assigned to departments operating decentralized systems should also have industry-standard tools in place to monitor system activity. Personnel should be in place to maintain and observe those tools. Persons, both internal and external to the University, are authorized to report a suspected incident.

5.4.1 Incident Prioritization

Prioritizing the handling of individual incidents is a critical decision point in the incident response process and the level of CSIRT provided support may vary depending on the incident's priority level and the CSIRT's available resources. Resources will be assigned according to the following priorities, listed in decreasing order.

Priority Level	General Description
1 **Critical**	Includes any one or more of the following: ○ Unauthorized disclosure of information has a catastrophic adverse effect on the University. ○ Unauthorized modification or destruction of information has a catastrophic adverse effect on the University. ○ Disruption of access to or use of information systems has a catastrophic adverse effect on the University. ○ The incident poses a threat to human life or results in major damages, costs, fines, or legal actions against the University.
2 **High**	Includes any one or more of the following: ○ Unauthorized disclosure of information has a serious adverse effect on the University.

Priority Level	General Description
	○ Unauthorized modification or destruction of information has a serious adverse effect on the University. ○ Disruption of access to or use of information systems has a serious adverse effect on the University. ○ The incident results in considerable damages, costs, fines against the University.
3 **Moderate**	Includes any one or more of the following: ○ Unauthorized disclosure of information has a serious effect on the University. ○ Unauthorized modification or destruction of information has a serious effect on the University. ○ Disruption of access to or use of information systems has a serious effect on the University. ○ Requires extensive corrective actions or repairs. ○ The incident results in limited damages or costs against the University
4 **Low**	Includes any one or more of the following: ○ Unauthorized disclosure of information has a limited adverse effect on the University. ○ Unauthorized modification or destruction of information has a limited adverse effect on the University. ○ Disruption of access to or use of information systems has a limited adverse effect on the University. ○ Requires minor corrective actions or repairs. ○ The incident results in little damage to the University.

5.4.2 Incident Notification

Any actual or suspected breach in any type of media (e.g., electronic, paper, microfiche, verbally, etc.) must be reported immediately to the ITS Help Desk at 323-343-6170 or the director of IT Security and Compliance at 323-343-2600. Immediately following telephone notification, form ITS-2812 *Information Security Initial Incident Report* must be sent via one of the means below:

- Facsimile: 323-343-2602
- Email Address: itsecurity@calstatela.edu
- Address: CSIRT
  IT Security and Compliance
  Information Technology Services, LIB PW 1070

California State University, Los Angeles
5151 State University Drive
Los Angeles, CA 90032

5.4.3 Incident Reporting

Reporting should not be delayed until all information regarding an incident is gathered. It is understood that in some circumstances some information may not always be readily available when first reported. ITS-2812 *Information Security Initial Incident Report* must be completed immediately upon detection of a breach by any user. Upon receipt of the report, the CSIRT director will confirm that an incident has occurred and will then assign an incident tracking number. The unique tracking number is used to track all information and actions related to the incident.

An ITS-2819 *Information Security Incident Status Report* form should be used and submitted to the CSIRT director periodically to update the status of the incident and as a final report. Information in the report is helpful for understanding the cause and extent of an incident and for post-incident analysis and a final assessment of damage. Additionally, if there is a possibility of a criminal prosecution, the information may be used as evidence.

5.4.4 Incident Response

The CSIRT will assist departments in promptly investigating incidents and coordinate actions through the breached department representative. Personnel (e.g., department head, system administrator, Information Technology Consultant, etc.) working in the department in which the incident occurred are responsible for assuming an integral role in responding to an information security incident and should have the ability and training to implement CSIRT recommendations.

The CSIRT will assist in incident triage, incident coordination, incident resolution and post-incident review as outlined below.

Incident Triage

The CSIRT will assist in:

a) Supporting system administrators with handling the technical and organizational aspects of the incident.
b) Providing assistance or advice with respect to the aspects of incident management.
c) Determining an incident's nature, scope and impact, as well as the level of damage caused by it.
d) Administering forensics tools, if required, for immediate evidence collection and preservation.

Incident Coordination

The CSIRT will assist in:

a) Determining the initial cause of the incident (i.e., the exploited vulnerability).
b) Facilitating contact with other sites that may be involved.

c) Facilitating contact with University Police and/or appropriate law enforcement agencies, if criminal activity is suspected or confirmed.
d) Delivering approved announcements to users, as necessary.

Incident Resolution

The CSIRT will assist in:
a) Removing the exploited vulnerability.
b) Securing the system from the incident's effects.
c) Evaluating whether certain actions are likely to garner results proportionate to their cost and risk, in particular, actions geared toward eventual prosecution or disciplinary action (e.g., collection of evidence after the fact, observation of incidents in progress, setting traps for intruders, etc.).
d) Responding to requests for evidence where criminal prosecution or University disciplinary action, is contemplated.

Post-Incident Review

The CSIRT director will request from each team member of the CSIRT the completion of ITS-2820 *CSIRT Incident Evaluation Form* following the resolution of an incident. The purpose of the evaluation forms is to determine the effectiveness of the teams, to improve CSIRT processes and to ensure that the team is meeting the needs of the constituency.

As a result of a post-incident analysis, the CSIRT director may issue alerts, warnings or recommendations to the University about certain actions to take to reduce vulnerabilities that were exploited during the incident. The CSIRT director may also need to propose changes to current guidelines, standards or procedures.

5.5 Information Disclosure

During and following an incident, information may need to be disclosed. There are different types of information that may be disclosed and different groups or organizations that may receive this information. The disclosure of information and the determination of the groups or organizations to which the information will be released will be determined by the CSIRT director and CSIRT coordinator.

5.5.1 Classification of Information

During incident handling, the CSIRT may need to communicate with outside parties such as other CSU campuses, law enforcement agencies, vendors and external constituents. The classification of information is a criterion for determining whether or not that information can be released. Information shall be disclosed as follows:

- Protected data will be not released in identifiable form outside the CSIRT.
- Information can be released to show a sample or to demonstrate a particular social engineering attack if a user's identity is disguised.
- Intruder information will not be released to the public unless it becomes a matter of public record (e.g., because criminal charges have been brought against the intruder).

- Private site information will not be released without the permission of the site in question.
- Vendor vulnerability information will be released freely though every effort will be made to inform the relevant vendor before the general public is informed.
- All information, except protected data, regarding a potential or actual breach may be exchanged with internal and external information security personnel on a need-to-know basis.
- Incident information will be released at the discretion of the Information Security Officer.

5.5.2 Types of Groups

The process for disclosing information will differ depending on the group receiving the information and their plans for the information. The following are examples of the different types of groups who may receive information and their reasons for receiving the information:

- Other teams about a new vulnerability that has been discovered and must be remediated elsewhere on campus.
- Other teams who are collaborating on incident analysis or response efforts.
- Sites that are the target or source of an attack.
- Management for budget purposes.
- Management for statistical reporting purposes.
- Human Resources Management or Student Conduct for potential personnel actions.
- Risk Management to assist in planning infrastructure and security improvements.
- A funding body for justification of CSIRT activities.
- Law enforcement for investigation or prosecution.
- Governmental organizations for notification or further reporting.
- Everybody who has a vested interest, so they are aware of ongoing activity and recommended mitigation or prevention strategies.

5.5.3 Advance Notification to the Media

Though not required, in breaches likely to receive greater attention, the University may consider providing advance notification to the media as notifications are mailed to affected individuals. Providing accurate information through the news media is another way to reach those affected. Information for the media will be provided to the Office for Communications and Public Affairs and all press-related incident queries will be handled by the executive director of Communications and Public Affairs or designee unless an alternate contact is identified.

5.5.4 University Community Announcements

The CSIRT is committed to informing the University community, whenever possible, of potential vulnerabilities (i.e., vulnerabilities before they are actively exploited) and will distribute announcements, as needed. The following are types of announcements that may be utilized:

ITS Alerts and Twitter

These are short-term notices about critical developments containing time-sensitive information about recent attacks, successful break-ins, or warnings of a potential issue or threat.

Advisories

Advisories provide mid-term and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. Advisories are often thoroughly researched and include substantial technical details or may be shorter and less technical to address a wider audience.

User Guidelines

User Guidelines provide a sequence of steps that lead someone through a process meant to expand that person's knowledge and to improve their fundamental understanding of information security and their day-to-day practices.

Technical Procedures

Technical procedures are lengthier than guidelines and provide more technical details addressing an expert audience and often target a specific problem.

5.5.5 Breach Notification

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

Breach Notification Requirements

A security breach notification shall include the following information:

- University contact information including the name, title and email address of the responsible party, as well as a telephone number for inquiries.
- The date of the notice.
- The number and title of affected individuals (e.g., former students, students, faculty, employees, etc.)
- The types of personal information that were or are reasonably believed to have been the subject of the breach.
- If the information is possible to determine at the time the notice is provided:
    - The date of the breach, the estimated date of the breach, or the date range within which the breach occurred.
    - Whether the notification was delayed as a result of a law enforcement investigation.
    - A general description of the breach incident.
- The addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

A security breach notification may also include what has been done to protect individuals whose information has been breached and referral to a website that provides additional information and answers frequently asked questions.

Cal State LA has available a template for breach notifications that satisfies these requirements. The breached department representative should request the template from the coordinator.

Breach Notification Methods

Breach notification may be provided electronically or in writing.

A substitute notice method may be used if the following conditions exist:

- The cost of providing notice would exceed $250,000,
- The number of persons to be notified exceeds 500,000, or
- There is not sufficient contact information available.

A substitute notice shall be composed of the following:

- Email notice when email addresses are available for the affected persons.
- Conspicuous posting of the notice on Cal State LA's website.
- Notification to major statewide media and the Office of Information Security within the California Technology Agency.

When more than 500 California residents are to be notified of a security breach as a result of a single breach of the security system, the breached department representative shall electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the State Attorney General.

6. Contacts

a. For questions regarding specific department procedures, contact the Information Technology Consultant (ITC).

b. Address questions regarding these standards to: ITSecurity@calstatela.edu.

7. Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Federal Privacy Act of 1974	**Federal Privacy Act of 1974** http://www.usdoj.gov/opcl/privacyact1974.htm

	This is a federal act that establishes a code of fair information practices governing the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Gramm-Leach-Bliley Act 15 USC, Subchapter 1, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8** http://leginfo.legislature.ca.gov/ This is a state law that, as amended by SB 1386 (2003), AB 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.
Information Practices Act of 1977	**Information Practices Act of 1977** http://leginfo.legislature.ca.gov/ This act established California Civil Code, (sections 1798 et seq.), which requires government agencies to protect the privacy of personal information maintained by state agencies.