Cal Poly
Information Security Program

Policy History	
Date	**Action**
October 5, 2012	Modified Separation or Change of Employment section to address data disposition guidelines
October 5, 2010	Updated to reflect CSU Information Security Policies and current regulations
October 19, 2004	Amended scope to reflect Unit 4 exception
July 8, 2004	Final approval by President Warren Baker
May 11, 2004	Policy endorsed by Information Resources Management Policy and Planning Committee (IRMPPC)
January – May 2004	Constituency Review
December 8, 2003	Draft policy released

Contents

Cal Poly
Information Security Program

Introduction and Purpose

The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets.

In accordance with the CSU Information Security Policies this Information Security Program contains administrative, technical, and physical safeguards to protect campus information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

The purpose of the Information Security Program is to:

- Document roles and responsibilities for the information security program.
- Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic).
- Document risk management strategies to identify and mitigate threats and vulnerabilities to level 1 and level 2 information assets as defined in the Cal Poly Information Classification and Handling Standard.
- Document incident response strategies.
- Document strategies for ongoing security awareness and training.
- Comply with applicable laws, regulations, Cal Poly and CSU policies.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which Cal Poly must protect from unauthorized access.
- Integrity and availability of information stored on or processed by Cal Poly information systems.
- Compliance with applicable laws, regulations, CSU policies, and Cal Poly policies governing information security and privacy protection.

The Cal Poly Information Security Program and security standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet Cal Poly's core mission and campus academic and administrative goals.

Scope

Consistent with the CSU Information Security Policies, the Cal Poly Information Security Program shall apply to the following:

- Central and departmentally-managed campus information assets.
- All users employed by Cal Poly, contractors, vendors, or any other person with access to Cal Poly's network resources or information assets. This includes non-Cal Poly-owned computing devices that may store protected information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, network resources owned or managed by Cal Poly. This includes third party service providers' systems that access or store Cal Poly's protected information.

Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the Cal Poly Information Security Program.

Cal Poly retains ownership or stewardship of information assets owned (or managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are intended to protect the confidentiality, integrity and availability of information, and are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

Information Security Policy

Consistent with the CSU Information Security Policies, Cal Poly's Information Security Program, combined with Cal Poly's Information Technology Resource Responsible Use Policy, establishes policy and sets expectations for protecting university information assets. These are supported by related policies, standards, guidelines and practices to facilitate campus compliance:

- Policies are high-level statements of principle, equivalent to organizational law, that provide technology agnostic scope and direction to the campus community.
- Standards establish specific criteria and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and they provide a basis for verifying compliance through audits and assessments.
- Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

- Practices consist of one or more series of interrelated steps to be taken to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to facilitate completing the process.

Policies should be written so as to require infrequent changes while standards, guidelines and practices are typically updated as needed to address specific changes in policy, technology or university practices.

The Information Security Officer and Vice Provost/Chief Information Officer are responsible for coordinating the development and dissemination of information security and technology policies, standards, guidelines and procedures, respectively.

Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives. Key campus stakeholders are consulted early on and research is conducted to find potential models from other universities.

Using a standard format, a draft policy is developed and shared broadly with campus constituents for review and comment. All input is considered but is not necessarily incorporated. The Information Resource Management Policy and Planning Committee (IRMPPC) is advisory and reports to the President on policies and plans related to management and use of information resources. The IRMPPC committee reviews, and forwards final draft recommendations to the President for formal campus adoptions. Standards, guidelines and practices do not require Presidential approval; campus constituents, including IRMPPC, may be asked to review and comment, but final approval rests with the ISO and VP/CIO.

Only new and substantially altered policies, standards and practices are subject to this process; minor updates and changes can be made and documented without undergoing the full review process.

Approved policies, standards, guidelines and practices will be published on the web, incorporated into security training programs, and disseminated through available campus communication methods. They will be reviewed annually to determine if any changes are required.

Information Security Policy Management

In accordance with CSU policies, the Cal Poly Information Security Officer oversees an annual review of this Program and communicating any changes or additions to appropriate Cal Poly stakeholders. The Cal Poly Information Security Program shall be updated as necessary to reflect changes in CSU policies, Cal Poly's academic, administrative, or technical environments, or applicable laws and regulations.

The program may be augmented, but neither supplanted nor diminished, by additional policies and standards.

Information Security Organization and Governance

In accordance with CSU policy, Cal Poly's president has designated an Information Security Officer (ISO) to coordinate and oversee campus compliance with the Information Security Program and related laws, policies, standards and practices. The ISO reports annually to the president on the current state of campus security relative to protecting university information assets.

Cal Poly's ISO reports to the Vice President for Administration and Finance (VP/AFD), and works closely with the Vice Provost/Chief Information Officer (CIO) to develop, implement and ensure compliance with policies, standards and practices related to the security of information technology resources.

The CIO reports directly to the Provost/Vice President for Academic Affairs and indirectly to Cal Poly's President. Both the CIO and VP/AFD are members of the senior management team that provides advice and counsel to the president. The CIO and ISO regularly brief the Academic Senate, deans, department heads/chairs, LAN Coordinators, and other campus constituents on information security issues.

Security policies, standards and practices are reviewed with campus constituents through various committees and other governance bodies. The CIO chairs, and the ISO is a standing member of, the Information Resource Management Policy and Planning Committee (IRMPPC). IRMPPC is advisory and reports to the President on policies and plans related to management and use of information resources. Members include the provost and vice presidents, the Library Services dean, one college dean, three faculty appointed by the senate, the Cal Poly Corporation executive director, vice provost for programs and planning, and chairs of computing advisory subcommittees representing students, faculty and administrative users.

The ISO chairs the Information Security Committee which reviews policies, standards and practices from a university-wide operational perspective. The ISO meets regularly with campus information authorities and reviews application data requests, IT acquisitions and other transactions from an information security perspective. The ISO hosts regular forums to brief the campus community on security issues.

The Information Security Management Team (which includes the ISO and CIO) meets regularly to review security policies and issues, discuss specific incidents, identify areas of concern, clarify and interpret policies, and develop communication and implementation strategies and plans. The team works with designated university officials, managers, technical staff and others to manage security incidents.

Administrators across the university are responsible for ensuring information security policies, standards and practices are followed by employees in their respective areas. An information security coordinator in each college and major administrative unit will provide necessary operational oversight to assist the responsible administrators.

Technical support staff and individual users are expected to follow established standards and practices and to report potential security violations.

Appendix A includes a detailed description of campus roles and responsibilities for information security.

Risk Management, Assessment and Planning

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize resources.

Information security risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk to information security assets. Once a risk has been identified, strategies are developed to reduce the risk to acceptable levels, share or shift the risk to another party, or assume the identified risk. Risks are monitored with the ongoing collection of information about the risk.

In accordance with CSU Information Security Policies, Cal Poly's risk management processes to identify information assets containing level 1 and level 2 data are defined in the Cal Poly Information Classification and Handling Standard.

Risk Assessment

Cal Poly performs periodic assessments of its information security risks and vulnerabilities. Risk assessments may be aimed at particular types of information, areas of the organization, or technologies. Risk assessments are part of an ongoing risk management process. They provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. The Cal Poly Security Risk Self-Assessment and Inventory Standard contains processes to perform annual self-assessments and inventory reporting.

The Security Risk Self-Assessments and Inventories are requested, collected, reviewed and evaluated by the Information Security Officer and the Vice Provost/Chief Information Officer. The results are shared with executive management and campus computing committees. The outcomes are produced in a Risk Assessment Report updated annually identifying control objectives, risk exposures, mitigation strategies and action plans for addressing each risk with timelines.

Risk Planning

Security must be a consideration from the very beginning of any project at the University rather than something that is added later. In addition, a control review should be performed before implementation of computer systems which store or handle protected information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.

- A risk assessment, including a review for regulatory, legal, and policy compliance.
- A contingency plan, including the data recovery strategy.
- A review of on-going production procedures, including change controls and integrity checks.

Privacy of Personal Information

Consistent with CSU Information Security Policies, all users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically, and must not assume any degree of privacy or restricted access to information they create or store on campus systems.

Cal Poly is a public university and information stored on campus information systems may be subject to disclosure under state law. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, Cal Poly acknowledges its obligation to respect and protect private information about individuals stored on campus information systems and network resources.

Collection of Personal Information

To comply with state and federal laws and regulations, individuals and processes may not collect personally identifiable information unless the need for it has been clearly established.

Where such information is collected:

- The Information Authority and individual user collecting the information will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The Information Authority and individual user collecting the information shall store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

Access to Personal Information

Except as noted elsewhere in CSU policy or Cal Poly policy, information about individuals stored on campus information systems may only be accessed by:

- The individual to whom the stored information applies or his/her designated representative(s).
- Authorized Cal Poly employees with a valid Cal Poly-related business need to access, modify, or disclose that information.
- Appropriate legal authorities.

When appropriate, authorized Cal Poly personnel following established campus procedures may access, modify, and/or disclose information about individuals stored on campus information systems, or a user's activities on campus information systems or network resources without consent from the individual. For example, Cal Poly may take such actions for any of the following reasons:

- To comply with applicable laws or regulations.
- To comply with or enforce applicable Cal Poly or CSU policy.
- To ensure the confidentiality, integrity, or availability of campus information.
- To respond to valid legal requests or demands for access to campus information.

If Cal Poly personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on campus information systems or network resources, staff will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by Cal Poly policy or applicable laws.

Information Authorities are advised to consult the CSU Records Access Manual to determine which records must be made available for public inspection under the California Public Records Act.

Access to Electronic Data Containing Personal Information

Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for Cal Poly business reasons. This prohibition does not affect:

- Authorized access to shared files and/or resources based on assigned roles and responsibilities.
- Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.
- Access to implicitly publicly accessible resources such as University websites.
- Campus response to subpoenas or other court orders.
- Campus response to a request pursuant to public record disclosure laws.

Personnel Information Security

In accordance with CSU Information Security Policies, the following are the information security pre-employment requirements and guidelines for managing separations or changes in employment status.

Employment Requirements

Hiring managers must conduct background checks on people hired into positions involving access to level 1 information assets as defined in the Cal Poly Information Classification and Handling Standard.

Separation or Change of Employment Status

Access rights must be promptly revoked from information resources upon termination or change of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy or by the Information Authority. Unless otherwise authorized in writing, when an employee voluntarily or involuntarily separates from the campus or a department, information system privileges, including all internal, physical, and remote access, must be promptly revoked.

Procedures must be implemented to ensure proper disposition of information assets upon termination or change of status. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files, and to identify appropriate methods to be used for handling and disposing of the files. If the separating employee is holding resources subject to a litigation hold, the manager, in consultation with University Legal Counsel, must ensure preservation of relevant information until the litigation hold has been revoked, at which point the resource is subject to the normal record retention schedule.

Procedures must be implemented to verify that items granting physical access such as keys and access cards are collected from the exiting employee. Any access list that grants the exiting employee physical access to a limited-access area on the campus must be updated appropriately to reflect the change in employment status.

Procedures must be established to allow for separated employees to obtain such incidental personal electronic information as appropriate.

Information system privileges retained after separation from the campus or department must be documented by management and authorized by an appropriate Information Authority.

Information Security Awareness and Training

Consistent with CSU Information Security Policies, all employees with access to the Cal Poly network and information assets must participate in information security awareness training.

The Information Security Awareness Training Program is designed to help individuals protect and respond appropriately to threats to campus information assets containing level

1 or level 2 data as defined in the Cal Poly Information Classification and Handling Standard.

The Program promotes awareness of:

- CSU and campus information security policies, standards, procedures, and guidelines.
- Potential threats against campus protected data and information assets.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets.
- CSU and campus notification procedures in the event protected data is compromised.

Within about one month of employment, new employees are provided individual access to the Information Security Awareness Training Program.

Employees are expected to complete the training within 90 days of receiving their access to the Program.

Department heads and campus executive management are responsible for and will be provided status of training compliance.

Managing Third Parties

The CSU Information Security Policies require third parties who access Cal Poly information assets to adhere to appropriate CSU and Cal Poly information security policies and standards. As appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided.

Granting Access to Third Parties

Third party service providers may be granted access to campus information assets containing protected data as defined in the Cal Poly Information Classification and Handling Standard only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by a designated Information Authority list and based on the principles of business need and least privilege.

Third party service providers must not be granted access to campus level 1 or level 2 information assets as defined in the Cal Poly Information Classification and Handling Standard until the access has been authorized, appropriate security controls have been implemented, a contract/agreement has been signed defining the terms for access, and a Cal Poly confidentiality-security agreement has been signed.

Information Technology Security

Cal Poly
Information Security Program

The CSU Information Security Policies require Cal Poly to appropriately secure its information technology resources to protect the confidentiality, integrity and availability of university information. This includes but is not limited to computer systems, network resources and software applications.

Each member of the campus community and third party providers are responsible for the security and protection of information technology resources over which they have control. The physical and logical integrity of these resources must be protected against potential threats such as unauthorized access, malicious or criminal action, inadvertent compromise, and inappropriate use.

Protection of information technology assets must be commensurate with the criticality of the function performed, the nature and level of access provided, information classification associated with the asset, exposure of the asset to potential risks, and the liability to the university if the asset is compromised. In general, a combination of administrative, operational and technical security safeguards will be required.

Under the direction of the Vice Provost/Chief Information Officer and Information Security Officer, Information Technology Services will develop policies, standards, guidelines and practices for securing university information technology assets. Areas to be covered include but are not limited to:

- Access and authentication controls
- Configuration settings and protection schemes
- Change management processes
- System and software acquisition, development and maintenance processes
- Network design and implementation considerations
- Threat identification and prevention measures
- Monitoring, detecting, reporting, and mitigating vulnerabilities
- Equipment transfer and disposition protocols

Combined with Cal Poly's Information Technology Resources Responsible Use Policy, said policies and related standards and practices set expectations and define minimum requirements for securing Cal Poly's information technology infrastructure and resources.

<u>Protections Against Malicious Software Programs</u>

Each device with the effective capability must have controls in place to detect, prevent, and report malicious software effectively. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a non-quarantined location on a campus network or information system.

<u>Network Security</u>

Storing protected information assets must ensure confidentiality, integrity, and availability. Transmission of protected data over the campus network must ensure confidentiality, integrity, and availability.

Mobile Devices

Protected data must not be stored on mobile devices unless effective security controls have been implemented to protect the data. Individuals must use encryption, or equally effective measures, on all mobile devices that store level 1 data as defined in the Cal Poly Information Classification and Handling Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the Information Security Office. Other effective measures include physical protection that ensures only authorized access to protected data.

Information Asset Event Monitoring

Event monitoring must not be conducted for the purpose of gaining unauthorized access, "snooping", or for other activities that violate the CSU Responsible Use Policy or Cal Poly Responsible Use Policy. Records created by monitoring controls (e.g. event logging) must be protected from unauthorized access and reviewed regularly. Access to the data generated by the monitoring controls (e.g. logging) must be restricted to those who have a business need.

Data generated by event monitoring must be retained for a period of time that is consistent with effective use, Cal Poly records retention schedules, regulatory, and legal requirements such as compliance with litigation holds, or with IT Security Standards.

At a minimum, server administrators are required to scan regularly, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within each quarter. The risk level of a system determines the frequency at which logs must be reviewed. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).

Configuration Management

Configuration standards to ensure that information technology systems, network resources, and applications are appropriately secured to protect confidentiality, integrity, and availability are provided in the IT Security Standards.

Change Control

Consistent with CSU Information Security Policies, the following provides direction and support for managing changes to information assets and provides guidance for implementing emergency changes to information assets.

Changes to information technology systems, network resources, and applications need to be appropriately managed to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. Change control processes are documented in the IT Security Standards.

Emergency Changes

Only authorized persons may make emergency changes to campus information assets containing level 1 data as defined in the Cal Poly Information Classification and Handling Standard. Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the campus' formal change management process.

Such emergency changes must be appropriately documented and promptly submitted, after the change, to the campus normal change management process.

Access Control

The CSU Information Security Policies require controlled access to Cal Poly information assets and guidance for: granting access to Cal Poly information assets; separating duties of individuals who have access to Cal Poly information asset; conducting reviews of access rights to Cal Poly information assets; and modifying user access rights to Cal Poly information assets.

Access Control

On-campus or remote access to information assets containing level 1 or level 2 data as defined in the Cal Poly Information Classification and Handling Standard must be based on operational and security requirements. Appropriate controls must be in place to prevent unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, but also data extracts and backup copies. IT Security Standards define requirements for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders. Access to campus protected information assets must be denied until specifically authorized.

Access to public and shared resources may be excluded from this requirement. Information Authorities are required to identify and document public or shared resources that are excluded from this requirement. Authorized users and their access privileges must be specified by the Information Authority, unless otherwise defined by CSU or Cal Poly policy.

Access Control

Access to campus information assets containing protected data as defined in the Cal Poly Information Classification and Handling Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of business need and least privilege.

Authentication controls must be implemented for access to campus information assets that access or store protected data, must be unique to each individual and may not be shared unless authorized by appropriate the Information Security Officer or the Vice Provost/Chief Information Officer. Where approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved in writing at least annually.

Separation of Duties

Separation of duties principles must be followed when assigning job responsibilities relating to restricted or essential resources. Information Authorities must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data. Information Authorities must avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee's job duties.

Access Review

Information Authorities and others as appropriate must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

Modifying Access

Modifications to user access privileges must be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked.

Information Asset Management

In accordance with the CSU Information Security Policies, Cal Poly Property Accounting maintains an inventory of information assets. These assets are categorized and protected throughout their entire life cycle, from origination to destruction.

The Cal Poly Information Classification and Handling Standard at http://security.calpoly.edu contains data classification categories, practices for handling protected data, and identifies responsibilities for information authorities and data stewards.

The Cal Poly Security Risk Self-Assessment and Inventory Standard contains processes for performing annual self-assessment risk assessment and inventory reporting.

The Cal Poly Retention and Disposition Standard contains record retention schedules and Information Authority responsibilities.

Information Systems Acquisition, Development and Maintenance

The CSU Information Security Policies require Cal Poly to integrate information security requirements into the software life cycle of information systems that contain protected data. The security requirements must identify controls that are needed to ensure confidentiality, integrity, and availability. These controls must be appropriate, cost-effective, and mitigate risks that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data.

Acquisition controls are located at:
http://www.afd.calpoly.edu/cprm/computers.asp?pid=2

Systems Development and Maintenance controls are located at:
http://security.calpoly.edu

Information Security Incident Management

In accordance with CSU Information Security Policies, security incidents involving loss, damage or misuse of information assets or improper dissemination of protected data, regardless of medium, must be properly reported and investigated to mitigate adverse impacts, protect the university from similar incidents, and comply with existing policies and laws.

Security incidents will be managed by the Information Security Management Team and reported to abuse@calpoly.edu. The team will develop and maintain an incident response program to ensure that security incidents are promptly reported, investigated, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions. Cal Poly's incident response program will be reviewed annually and modified as needed to comply with applicable laws and university policies and standards.

The campus incident response program will incorporate the following standards and practices:

- Incident discovery and reporting protocols;
- Establishment of a security incident response team (SIRT) with defined roles and responsibilities that, based on the severity of the incident, may take priority over normal duties;
- Identification and classification of incidents based on type and severity and level of risk;
- Containment strategies to prevent further loss or disruption;

- Incident investigation protocols, including for not limited to,
    - Proper evidence collection, handling and storage;
    - Analysis and assessment strategies;
    - Problem identification, remediation and mitigation strategies;
    - Escalation and communication strategies;
- Resolution and closure protocols, including documenting incidents; ensuring corrective actions are taken; notifying affected parties, campus authorities, law enforcement, or others if required by policy or law; and identifying and applying lessons learned.

Cal Poly will disclose security breaches and notify affected users if required by law or policy to do so.

Cal Poly users shall report promptly any unauthorized or inappropriate disclosure of protected data to abuse@calpoly.edu. If the campus investigation determines that Level 1 data has been disclosed, the President or designee will notify the CSU Chancellor and the Vice Provost/Chief Information Officer will notify the CSU Assistant Vice Chancellor for Information Technology Services. The Information Security Officer will notify the Senior Director of System-wide Information Security Management if the campus determines that Level 1 data has been disclosed.

All security incidents will be treated as confidential. Information Technology Services staff will prepare a summary report documenting the number and type of incidents, estimated time and costs, and other information as requested. This report will be reviewed quarterly with the Information Security Management team, executive management and included in the annual report prepared by the Information Security Officer for the President.

Physical Information Security

Consistent with CSU Information Security Policies, the physical areas where information assets containing protected data are located must be protected from unauthorized physical access. These physical areas include data centers, office areas, and other locations. Information assets which access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. Information Authorities must review and document physical access rights to campus limited-access areas annually.

Business Continuity and Disaster Recovery

In accordance with CSU policies, Cal Poly must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users.

Cal Poly will develop, document, test and maintain a business continuity plan. The plan will ensure the continuance of critical campus functions, systems, and services when a disruption to campus operations occurs after a disaster or emergency situation.

The campus business continuity plan will incorporate the following standards and practices:

- A standard template will be used for the consistent development of the University's Business Continuity Plan. The template will be used to document key information (i.e., staff contact information, critical functions, critical function recovery procedures, vital records, assets) within a department in order to ensure the campus' ability to recover from a disruption.
- Emergency activities of departments, including requests for resources or services and documentation of financial impact, will be coordinated through the Emergency Operations Center and in compliance with the Campus Emergency Management Plan.
- The Departmental Business Continuity Plans, Department Emergency Plans, and the Campus Emergency Management Plan are interrelated and together provide for preparation, response and recovery to a campus emergency.
- The Business Continuity plan contains confidential information that should not be shared publicly. It is the responsibility of each department to ensure that the plan be held, developed, and reviewed by designated individuals only.
-

Responsibility

Each Vice President will have the responsibility for the development, testing and maintenance of Business Continuity plans within his/her division. A representative from each department should be assigned to develop and maintain the plan. The Business Continuity Director will be responsible for the central review of all Business Continuity plans in conjunction with each Cal Poly Business Continuity Program to ensure the continuity of essential functions and operations following a catastrophic event.

Compliance

Cal Poly's information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver's license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

There are many individual laws, regulations, and policies that establish our information security requirements. Some of the most notable include:

California Code of Regulations, Title V, Sections 42396 - 42396.5

Title V of the California Code of Regulations, specifically sections 42396 - 42396.5 addresses privacy and principles of personal information management applicable to the California State University.

California Information Privacy Act

The California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is acquired by an unauthorized person. The Act, which went into effect July 1, 2003, was created to help stem the increasing incidence of identity theft. Found in the California Civil Code (Sections 1798.29).

California Public Records Act

The California Public Records Act addresses exclusions to the disclosure of public information of personally identifying information that may be a violation of personal privacy.

California Senate Bill 25 (SB 25)

SB 25 extends those Social Security number restrictions to all government agencies, including public colleges and universities. Under SB 25, public entities will have to ensure that Social Security numbers don't get posted or displayed on any printed material, or used on identification cards.

Fair and Accurate Credit Transactions Act (FACTA)

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which required “creditors” to adopt policies and procedures to prevent identity theft. These requirements are described in section 114 of FACTA and are known as the “Red Flags Rule”.

The Red Flags Rule applies to financial institutions and “creditors” that offer or maintain accounts that provide for multiple transactions primarily for personal, family, or household purposes. Institutions are considered creditors if they provide goods or services that are not fully paid for in advance or allow individuals to defer payment for goods or services.

Family Educational Rights and Privacy Act (FERPA)

Responsible for Enacted in 1974, FERPA protects the privacy of student education records and affords students (or parents if the student is a minor) certain rights with respect to the student's "education records." More information about the Cal Poly FERPA program can be found at: http://www.ess.calpoly.edu/_records/stu_info/ferpa.htm

Gramm-Leach-Bliley Act (GLBA)

Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure.

Information Practices Act of 1977 (IPA)

Found in the California Civil Code (Sections 1798.14-1798.23), the IPA requires State agencies to record only personal information that is relevant and necessary to accomplish the purpose of the agency. Additionally, the agency should collect personal information directly from the individual who is the subject of the information rather than from any other source.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. It applies to American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International.

Additional laws and regulations specify the disclosure of employee and student information and require the University to take specific actions in the event Cal Poly suspects protected information may have been disclosed either accidentally or maliciously to unauthorized parties. Individuals who handle protected information are encouraged to speak with their managers, Information Authorities, or the Information Security Officer to familiarize themselves with relevant laws and regulations.

Policy Enforcement

Consistent with CSU policies, the Information Security Officer is authorized by the President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the University community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the Information Security Officer. Approved requests will be reviewed annually to determine if an exception is still warranted.

Cal Poly reserves the right to temporarily or permanently suspend, block, or restrict access to campus information assets, independent of such procedures, when it reasonably

appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of Cal Poly information assets; to protect Cal Poly from liability; or to enforce this policy and its related standards and practices.

The Information Security Officer will work with the Vice Provost/Chief Information Officer to develop supplemental standards and practices to facilitate campus compliance with this policy; develop communication plans to inform users about the policy and its related standards and practices; advise departments on the interpretation and enforcement of this policy; and confer with University Legal Counsel and other university officials on matters involving potential violations.

Potential violations will be investigated in a manner consistent with applicable laws and regulations, collective bargaining agreements, and CSU and campus policies, standards, guidelines and practices.

The Information Security Officer or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate University officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Allegations against employees that are sustained may result in disciplinary action. Such actions will be handled by the appropriate human resources office using existing disciplinary processes consistent with the terms of the applicable collective bargaining agreement and the California Education Code. Student infractions will be handled by the Office of Student Rights and Responsibilities using established policies and practices. Auxiliary organization employees may be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to Cal Poly.

Non-compliance may result in personal, criminal, civil, or other administrative liability. Departments may be held accountable for remediation costs or other financial penalties incurred due to non-compliance.

Appeals of University actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for Cal Poly students and employees.

Appendix A – Information Security Roles and Responsibilities

Administrative Advisory Committee on Computing (AACC)
Membership: http://president.calpoly.edu/committees/Member_AACC.pdf

- Reviews, provides feedback, and recommends action to the Vice Provost/Chief Information Officer to improve security policies and practices to protect Cal Poly's digital information assets, and the information technology resources used to access, transmit, and store them.

- Detailed functions and meeting information located at: http://president.calpoly.edu/committees/AACC.pdf

Information Authority/Owner
The Information Authority is identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate use of the information.

- Responsibilities are identified in the Cal Poly Information Classification, Handling, Retention, Inventory Standards.

Information Custodian / Steward
The information custodian / steward has operational responsibility for the physical and electronic security of information.

- Responsibilities are identified in the Cal Poly Information Classification, Handling, Retention, Inventory Standards.

Information Users
Individuals who need and use University information as part of their assigned duties, or in fulfillment of assigned roles, or functions within the University community.

- Responsibilities are identified in the Cal Poly Information Classification, Handling, Retention, Inventory Standards.

Instructional Advisory Committee on Computing (IACC)
Membership: http://president.calpoly.edu/committees/IACC.pdf

- Reviews, provides feedback, and recommends action to the Vice Provost/Chief Information Officer to improve security policies and practices to protect Cal Poly's digital information assets, and the information technology resources used to access, transmit, and store them.
- Detailed functions and meeting information located at: http://president.calpoly.edu/committees/Member_IACC.pdf

Information Resource Management Policy and Planning Committee (IRMPPC)
Membership: http://president.calpoly.edu/committees/IRMPPC.pdf

- Reviews, endorses, and recommends action to the Vice Provost/Chief Information Officer to improve security policies and practices to protect Cal Poly's digital information assets, and the information technology resources used to access, transmit, and store them.
- Detailed functions and meeting information located at: http://president.calpoly.edu/committees/Member_IRMPPC.pdf

Information Security Committee
Membership: http://www.security.calpoly.edu/contacts/info_secure_comm.html

- Reviews, provides feedback, and recommends action to the Vice Provost/Chief Information Officer to improve security policies and practices to protect Cal Poly's digital information assets, and the information technology resources used to access, transmit, and store them.

- Detailed functions and meeting information located at: http://www.security.calpoly.edu/contacts/info_secure_comm.html

Information Security Coordinator

- Coordinates information security awareness training program.
- Reports on security incidents and training.
- Develops training materials and documents.
- Coordinates and assists with assuring campus security compliance requirements are met.
- Assists the ISO in responding to information security audits

Information Security Officer (ISO)

- Coordinates, administers, communicates, and maintains the Information Security Program on behalf of the President.
- Advises the President and campus leadership on information security matters.
- Consults with campus administrators to ensure campus information security policies and standards meet campus goals.
- Investigates, assesses, tracks, resolves, and reports suspected violations of policies and procedures in coordination with appropriate entities.
- Confers with Vice Provost/Chief Information Officer and Information Authorities, on information security policies, standards, procedures, security violations, campus security risks, and other security matters as needed.
- Provides input to the campus budget process regarding prioritization and required resources for security risk mitigation.
- Responds to information security related requests during an audit and coordinates the CSU information security audits.
- Serves as the campus representative on the CSU Information Security Advisory Committee.
- Serves as chairperson for the Cal Poly Information Security Committee.
- Reviews and approves application data requests and authentication requests.
- Notifies the CSU Senior Director for Information Security Management if a breach of level 1 data has occurred.
- Oversees the campus incident response program, the information security awareness and training program, and annual self-assessment inventory processes.
- Reviews computing equipment loss reports and security incidents and determines action needed, if any.
- Provides annual Information Security Report, and Risk Assessment and Action Plan to President, Vice President of Administration and Finance and Vice Provost/Chief Information Officer

Information Security Management Team

Membership: Chief Information Officer, Information Security Officer, Information Technology Policy Assurance Officer, Security Implementation Officer, Technical Security Officer

- Prepare proposals and recommendations for implementation of Information Security Program.

- Respond to information security incidents.
- Perform security review/audits (i.e. Health Center web application review, environment reviews past data breaches, Athletics audit finding assistance).
- Provide information security training for campus staff (attendees at: information security forum, LAN coordinator meetings, etc).
- Create security materials for dissemination (via RSS feed, security.calpoly.edu or other means).

Information Technology Policy Assurance Officer

- Oversees development and implementation of information technology (IT) policies and related standards and practices, including assessing the impact of new laws and technologies and participating in CSU and other external policy development.
- Represent the CIO to coordinate with campus administrative and technical staff, and appropriate campus officials, to investigate and act on complaints, suspected policy violations, and specific incidents involving misuse of campus IT resources.

Human Resources/Academic Personnel/Judicial Affairs

- Investigates alleged security violations by individual students, faculty and staff to determine if disciplinary action is appropriate.
- Interprets, recommends and imposes sanctions and discipline regarding security violations in accordance with existing policy and practice.

President

- Establishes an information security program, which is compliant and consistent with the CSU information security policy.
- Reviews information security risks at least annually.
- Reviews Information Security Annual Report provided by the Information Security Officer.
- Notifies the Chancellor if a breach of level 1 data has occurred.

Property Accounting Services

- Provides a copy of the Computing Equipment Loss Report to the Information Security Officer that contains information about lost or stolen computing equipment.

Security Implementation Officer

- Work with the CIO, ISO, Technical Security Officer, Policy Assurance Officer, and ITS Management to help scope security related projects, determine resources required, prioritize these projects with respect to other initiatives, and schedule them for implementation.
- Assist the ISO in responding to security audits, following up on security related incidents, and planning for future security activities.

Technical Security Officer

- Provide consulting to ITS management, the ISO, and the campus as a whole on technology and information security items.
- Help the campus understand risks, threats, and safeguards and participate in the development of preventative measures (policies, procedures, technical solutions).
- Respond to specific security incidents (forensic analysis, cooperation with campus and CSU groups, and regulatory and enforcement organizations).

University Police

- Receives and investigates all reports of potential criminal law violations involving any computing device containing University information and any University information resources.

Users

- Observes all laws, regulations, policies and procedures related to security of information and systems.
- Protects the privacy rights of University faculty, staff, and students.
- Protects the physical security of information and systems assigned to them.
- Reports suspected violations of security policies and procedures for University information to their supervisor who will report it to the Information Security Officer and/or Information Technology Services at abuse@calpoly.edu, depending on the nature of the violation.

Vice President for Administration and Finance

- Notifies the CSU Office of General Counsel of a breach of security to California residents whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.
- Reviews information security risks at least annually.
- Reviews Information Security Annual Report provided by the Information Security Officer.
- Reviews and endorses security policies and procedures.

Vice Provost/Chief Information Officer (CIO)

- Provides policy and operational guidance to the University.
- Provides security standards and guides for protecting information assets.
- Ensures compliance to existing campus information security policies, standards, and procedures.
- Coordinates with Information Security Officer to develop and implement information security policies, standards, and procedures.
- Coordinates with the Information Security Officer, if needed, on the investigation, assessment, tracking, resolution, and reporting of security issues involving information technology resources and reports potential criminal violations to the appropriate entities in a timely manner.
- Coordinates with the campus Information Security Officer to evaluate the risk introduced by any changes to campus operations and systems.
- Serves as the chairperson for the Cal Poly IRMPPC.

- Notifies the Assistant Vice Chancellor for Information Technology Services if a breach of level 1 data has occurred.
- Reviews information security risks at least annually.
- Reviews Information Security Annual Report provided by the Information Security Officer.

Vice Presidents, Deans, Department Heads and Program Managers

- Responsible for maintaining information as an asset of the University.
- Responsible for and shall take reasonable measures for implementation of, and compliance with, the Information Security Program, applicable laws, regulations, policies and procedures, within their areas.
- Applies sanctions and discipline for security violations in accordance with existing policy and practice in coordination with Human Resources, Academic Personnel, or Judicial Affairs.
- Supports the Information Security Officer and the Vice Provost/Chief Information Officer in the reporting, investigating, assessing, and resolving potential security violations.