

# Cal Poly Information Security Program

Policy Development History	
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

## Introduction

As part of its educational mission, the University acquires, develops, maintains and archives information. University information is found throughout the campus community in various forms, including paper documentation, electronic form, and verbal communication. Therefore, this program is widespread and relies on employees to use reasonable judgment in its application.

This program, along with campus processes, is designed to ensure that Cal Poly meets the generally recognized standards known as the “fair information practice codes” and its core principles of: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress and is in compliance with the Gramm-Leach-Bliley Act.

It should be noted that this program is a general framework for information security. Implementation of information security standards and practices, including training, development of forms, templates and procedures, communication, documentation, etc. will be developed based on this framework.

## Scope

This program applies to the security of all University information that is acquired, transmitted, processed, stored, transferred, and/or maintained by Cal Poly or any Cal Poly auxiliary organization. It applies to all Cal Poly students, employees<sup>1</sup>, consultants, contractors, or any person having access to University information in any form or format.

## Purpose

The purpose of the information security program is to:

- Establish a university-wide approach to ensure the accuracy, security and protection of information in the University’s custody, regardless of format.
- Prevent and protect against any anticipated threats and hazards to the security or integrity of University information.
- Prevent and protect against the unauthorized access to or use of University information, including confidential and personal information.
- Ensure university-wide compliance to applicable laws, regulations, policies and practices.

---

<sup>1</sup> Unit 4 employees are excluded from this document at this time but continue to be subject to applicable laws such as California Government Code Section 8314, which addresses the use of public resources for unauthorized purposes.

# Cal Poly

## Information Security Program

### **Management and Control of Risk**

The University will use a layered approach of overlapping controls, monitoring, assessment, and response to ensure the overall security of its information. The University has developed the following practices necessary to reasonably safeguard confidential information.

#### Collection

Information shall not be collected or maintained unless it is appropriate and relevant to the purpose for which it will be collected. Confidential information must be initially collected, to the extent practicable, from the individual directly and not from other sources. Confidential information should have an identifiable source to confirm legitimacy.

#### Data Review

All information should be reviewed and classified according to its use, sensitivity, and importance. For example:

1. High risk – information assets that would cause severe damage to the University if disclosed or modified, including confidential and personal information protected by Federal or State law.
2. Internal – source code, data, logs, etc., that would not expose the University to liability, but should be protected to prevent unauthorized disclosure or misuse.
3. Public – information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. An appropriate level of security should be established based on the classification of the information. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University. Appropriate measures should be taken to ensure that the method for transporting data between users and systems is consistent with its classification. For example, high-risk (i.e., sensitive or confidential) data should be shielded from viewing by others at all times and encrypted during transmission. The applicable classification codes need to be well documented.

#### Access Controls and Transfer of Data

Access controls must be in place to identify and authenticate who is authorized to access the specified information, and at what level, and to ensure that individual authorization rights are continually validated based on an individual's current status (authentication). Similar controls should be in place for automated data transfer and interactions between applications and systems. Authentication schemes and system support controls should be implemented to match the level of risk associated with the information classification, e.g., stricter security must be implemented for high-risk information whereas a lower level of security is permissible for information that is publicly shared. Processes for promptly terminating access rights for invalid users must be in place.

Operating system, network software and application software logging processes must be enabled on all computer systems in order to ensure identified security controls are in use,

## **Cal Poly Information Security Program**

validated and available for audit and/or incident response purposes. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

Where possible and financially feasible, no one person should have exclusive administrative rights to any critical University-owned server.

### Records Retention and Destruction

All information shall be destroyed when retention is no longer necessary. The method of destruction should be appropriate to the classification of the information and media. If records are stored in remote on-campus or off-campus locations, periodic inspections to ensure record security must be conducted and documented.

### Records Access

The three most significant statutes governing access to University records are: (1) the California Public Records Act; (2) the Information Practices Act; and (3) the Family Educational Rights and Privacy Act (commonly known as FERPA or the Buckley Amendment). The public purposes served by these three statutes are not the same. The California Public Records Act was enacted to give the public information about how state business is being conducted; it provides for the disclosure of identifiable, non-exempt public records. The Information Practices Act and FERPA, by contrast, were enacted to protect the privacy of persons who are the subject of public records; they mandate non-disclosure of those records. These fundamental differences should be kept in mind when evaluating the disclosure of any records that are subject to these statutes.

Individuals and departments are expected to follow approved University practice when presented with a public records request, subpoena or other request to disclose University information under their control.

### Individuals' Rights

Individuals have the right to inquire and be notified about personal information a state agency maintains concerning them. Access to official files, reviewing the files, and the ability to request an amendment to a record should be available to the individual.

### Physical Security

Appropriate steps should be taken to ensure the physical security of information, regardless of format, and computer systems, taking into account the value of the resource, access control methods, proper environmental controls, redundancy, power backup, and other factors.

### Operating Systems, Networks and Application Software

Operating systems, networks, application software, and information technology infrastructure resources must be maintained at acceptable levels to ensure their reliability and accessibility, and to minimize any risk from potential vulnerabilities. For example, available security patches and anti-virus measures should be routinely and promptly applied to protect against known threats and vulnerabilities on computer systems.

# Cal Poly

## Information Security Program

### Training

Education should be provided to ensure that affected individuals understand the Information Security Program and their role in protecting University information.

### Service Provider Requirements

The University may engage vendors, third parties, and/or other CSU entities to provide services on its behalf. Further, these service providers may be engaged in the collection, processing, storage or disposal of University information. Therefore, the University shall not enter into a contractual agreement with any provider who cannot maintain appropriate safeguards for its information, especially confidential information.

### **Compliance and Consequences of Non-Compliance**

Each department must ensure that measures are taken to address security weaknesses based on the framework outlined in this program and their own risk assessment. All departments are encouraged to conduct risk assessments. If the assessment involves computer systems, [abuse@calpoly.edu](mailto:abuse@calpoly.edu) should be provided prior notification to avoid the risk of the assessment being misinterpreted as an attack.

The unauthorized modification, deletion, or disclosure of confidential and/or personal information included in data files and data systems can compromise the integrity of programs, violate individual privacy rights, and is expressly forbidden. Violations by individuals, including the careless, accidental or intentional disclosure of confidential information, will be handled in accordance with existing University policies and procedures.

University departments found to be in non-compliance with the program will be required to take specific steps to come into compliance within a specified time.

### **Security Incident Reporting**

All security incidents involving University data must be reported and investigated. Records of security incidents must be maintained and potential evidence secured to aid in future investigations by the University or law enforcement. All reports will be investigated and notification to campus officials will occur, as appropriate. An actively managed process will be used to identify, track, resolve and report all security related incidents and losses on an appropriately confidential and secure basis. Depending on the severity and nature of the risk involved measures may be taken to prevent any future recurrence.

Incidents involving digital data, computer systems, networks and/or information technology resources, must be reported to the Vice Provost/Chief Information Officer or designee via [abuse@calpoly.edu](mailto:abuse@calpoly.edu). All other incidents must be reported to the Information Security Officer.

Any information security incidents which may be criminal in nature shall be reported to the University Police Department or other law enforcement agency of appropriate jurisdiction as soon as practicable after discovery.

# Cal Poly

## Information Security Program

### Roles and Responsibilities

Following is a description of roles and responsibilities of campus entities related to information security.

#### Application Manager

The Application Manager has oversight for the overall programmatic functionality of the application. This includes ensuring that appropriate security controls and measures are in place. The Application Manager may delegate these responsibilities to other individuals, as appropriate, either on an on-going or permanent basis (e.g., The Associate Director, Facilities Services - Administration is the Application Manager for the Facilities Management application.)

- Works in conjunction with the Data Authority, Data Steward, and others, as appropriate, to determine if the storage, transfer and access of data match information security requirements.
- Informs users of the match of classification of data to appropriate use of application.
- Reviews/audits the security of all new releases of an application prior to release on campus.
- Ensures existence of appropriate business continuity capabilities
- Identifies and takes steps to mitigate exposures related to vulnerabilities.
- Reports suspected violations of security policies and procedures for University information to the Information Security Officer and/or Information Technology Services at [abuse@calpoly.edu](mailto:abuse@calpoly.edu), depending on the nature of the violation.
- Responds to requests for information from the Information Security Officer and Vice Provost/Chief Information Officer regarding security.

#### Data Authority

The campus designated authority for designated information (e.g., The Registrar/Director of Academic Records is the Chief FERPA Officer and Custodian of Student Records)

- Identifies and classifies data under their control.
- Identifies authorized access and transfer of data under their control.
- Identifies and takes steps to mitigate exposures related to vulnerabilities.
- Establishes policies and procedures for securing confidential and personal information in the custody of the University.
- Acts as the campus authority on data under their control and responds to questions regarding such.
- Protects the privacy rights of the data of the constituent group they have authority over.
- Reports security breaches to individuals whose encrypted personal information, was, or is reasonably believed to have been, acquired by an unauthorized person in accordance with *Implementation Practices and Procedures* of Cal Poly's *Information Technology Resources Responsible Use Policy* or other applicable policies/laws.
- Confers with Information Security Officer and Vice Provost/Chief Information Officer, as needed.

# Cal Poly

## Information Security Program

### Data Stewards

A Data Steward is any individual responsible for keeping University data secure assigned to them by a Data Authority or multiple Data Authorities (e.g., The Health Records Technician is a Data Steward for Medical Records).

- Identifies and takes steps to mitigate exposures related to vulnerabilities.
- Determines and maintains the level of security required to meet identified classifications.
- Documents and implements access controls and processes based on rules established by Data Authority(ies).
- Works with the Application Managers to determine if the storage and transfer of data match information security requirements and recommend appropriate use.
- Promotes and encourages good security procedures and practices associated with storage, access and transmission of data.
- Reports suspected violations of security policies and procedures for University information to the Information Security Officer and/or Information Technology Services at [abuse@calpoly.edu](mailto:abuse@calpoly.edu), depending on the nature of the violation.
- Responds to requests for information from the Information Security Officer and Vice Provost/Chief Information Officer regarding security.

### 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.

### Information Security Officer

- Coordinates, administers, and communicates the Information Security Program.
- Maintains and updates the Information Security Program.
- Provides training regarding the requirements of the Information Security Program.
- Promotes and encourages good security policies and procedures.
- Investigates, assesses, tracks, resolves, and reports suspected violations of policies and procedures in coordination with appropriate entities.
- Promptly reports potential criminal violations involving information security to the University Police Department or other law enforcement agency of appropriate jurisdiction.
- Reviews computing equipment loss reports and security incidents and determines action needed, if any.
- Provides an annual report of computing equipment losses (Summary of Computing Equipment Loss Reports) and University information incidents (Incident Record Report Summary) to the President, the Vice President for Administration and Finance, and the Vice Provost/Chief Information Officer.
- Chairs the Security Committee.
- Confers with Data Authority and Vice Provost/Chief Information Officer, as needed.

# Cal Poly

## Information Security Program

### IRMPPC

- 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.

### President

- Reviews annual report of computing equipment losses (Summary of Computing Equipment Loss Reports), computer system incidents and University information incidents (Incident Record Report Summary) provided by the Information Security Officer.

### Security Committee

- Recommends security policies and procedures related to digital information assets and information technology resources to IRMPPC.
- Recommends security policies and procedures related to University information to the Vice President for Administration and Finance.

### System and Equipment Stewards (Network/System Administrators)

- Identifies and takes steps to mitigate exposures related to vulnerabilities and to secure all computer systems, networks and information technology resources in their area, e.g., applying security patches and updating anti-virus software.
- Strictly observes all laws, regulations, policies and procedures related to security of information and information technology resources in their area.
- Prepares and maintains a manual of security procedures for their area.
- Ensures establishment of backup, disaster, and recovery capabilities.
- Tests existing security safeguards.
- Regularly inventories computing equipment and reports losses to University Property Services by completing an Equipment Loss Report. If there is the possibility that the loss is due to theft, files a report with University Police.
- Assures University information and licensed software are appropriately removed upon transfer or survey of equipment and data storage items.
- Reports suspected violations of security policies and procedures for University information to the Information Security Officer and/or Information Technology Services at [abuse@calpoly.edu](mailto:abuse@calpoly.edu), depending on the nature of the violation.
- Responds to requests for information from the Information Security Officer and Vice Provost/Chief Information Officer regarding security.

### University Police

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

### University Property Services

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

# Cal Poly

## Information Security Program

### Users

- Strictly 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 data 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](mailto: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 annual report of computing equipment losses (Summary of Computing Equipment Loss Reports), computer system incidents and University information incidents (Incident Record Report Summary) provided by the Information Security Officer.
- Reviews and endorses security policies and procedures related to non-digital University information.

### Vice Presidents, Deans and Department Heads

- 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 and applicable laws and 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, investigation, assessment, and resolution of potential security violations.

### Vice Provost/Chief Information Officer

- Provides policy and operational guidance to the University, the IRMPPC, and the Information Security Officer on all Cal Poly information resources, systems and networks supporting campus uses of digitally-based information addressed in this program.
- Ensures the physical and virtual security, accessibility, integrity and protection of information in digital form and the computing resources, networks, and applications that support and enable its use as required.
- Coordinates with the Information Security Officer, if needed, on the investigation, assessment, tracking, resolution, and reporting of security issues involving

## **Cal Poly Information Security Program**

- information technology resources and reports potential criminal violations to the University Police Department in a timely manner.
- Provides a quarterly Incident Record Report summary report to the Information Security Officer.
  - Maintains the Incident Record Reporting system that contains a record of each incident and its resolution, including any new security measures implemented in response to the incident.
  - Reviews annual report of computing equipment losses (Summary of Computing Equipment Loss Reports), computer system incidents and University information incidents (Incident Record Report Summary) provided by the Information Security Officer.
  - Confers with Information Security Officer, as needed.
  - Reviews and endorses security policies and procedures related to digital information assets and the information technology resources used to access, transmit, and store them.

### **Exceptions**

Requests for exceptions to this policy must be submitted in writing by the department to the Information Security Officer for review and include an explanation of the compliance issue and a plan for coming into compliance in a reasonable amount of time. All requests for exceptions will be responded to in writing.

This program applies to non-University entities, including auxiliaries and affiliates, under the following circumstances:

- a. They are acting as the agent of the University,
- b. They are using assets or resources funded by the University (State) such that campus policies do apply (e.g., e-mail, network, etc.), or
- c. University information is involved.

This program does not apply to resources solely owned and operated by the non-University entity, except as noted above, and law enforcement records.

### **Plan Review**

This plan will be reviewed annually and updated by the Information Security Officer, as needed.

### **Appendix A - Definitions**

### **Appendix B - References**

# Cal Poly Information Security Program

Appendix A

## Definitions

### **Access**

Ability given to an individual, a group of users, or application to use University information transmitted. This includes, but is not limited to, the ability to read, write, view, create, alter, store, transmit, retrieve, and disseminate information.

### **Authentication**

The process used to determine whether someone is, in fact, who it is declared to be. In computer networks, authentication is commonly done through the use of unique logon identifiers and passwords.

### **Digital Data/Information Assets**

Information transmitted, stored, accessed, retrieved by, on, or from in any computing resource, service, or network system.

### **Confidential Information**

Any information identified in governing law, regulation or policy as personal information, individually identifiable health information, confidential information, education records, personally identifiable information, non-public information, confidential personal information or sensitive information.

### **Disclose**

To disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

### **Personal Information**

Any information that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history and demographic data such as birth date and ethnicity.

Personal information in the context of Senate Bill 1386 which involves a security breach of non-encrypted computerized data means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number; (2) driver's license number of California Identification Card number; (3) account number (which could include a student or employee identification 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.

### **Service Provider**

## **Cal Poly Information Security Program**

Any person or entity that receives, maintains, processes, or otherwise is permitted access to University data through its direct provision of services.

### **University Information**

Information related to the function or purpose of the University. University information includes information about individual students and employees. Law enforcement and auxiliary organization records are not considered university information within the context of this policy.

# Cal Poly Information Security Program

Appendix B

## References

California Information Practices Act of 1977

Cal Poly, Information Technology Resources Responsible Use Policy (RUP)  
<http://www.its.calpoly.edu/Policies/RUP-INT/>

California Public Records Act (California Government Code Sections 6250 through 6270)

CSU Memo, Compliance with the Gramm-Leach-Bliley Act-Safeguarding Confidential Personal Data, May 21, 2003