Cal Poly
Information Security Program
DRAFT – 12/8/2003

Scope
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, the application of this program is widespread. It applies to the security of all University information that is acquired, transmitted, processed, stored, and/or maintained by Cal Poly or any Cal Poly auxiliary organization. It applies to all Cal Poly students, employees, consultants, contractors, or any person having access to University information in any form or format.

Purpose
The objectives of the information security program are to:

- Establish a university-wide approach to ensure the 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.

Risk Assessment
An information security risk assessment is a project, which identifies:

- The nature and value of information assets
- The threats against those assets, both internal and external
- The likelihood of those threats occurring
- The impact upon the organization

Anticipated threats or hazards to the security or integrity of information may include, but are not limited to:

- Unauthorized access to confidential/personal information by anyone not explicitly approved for such access
- A vulnerable or compromised computer system
- Interception of data on a computer system or network during transmission
- Collection of inappropriate or non-essential information
- Physical loss of data in a disaster and/or by criminal or negligent action
- Errors introduced into the systems or that corrupts the data
- Lack of transaction completeness and documentation
- Unauthorized access to electronically stored information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer or disclosure of information by anyone, including through third parties
- Inappropriate classification of information
- Lack of authentication of individuals
- Invalid security controls in place to prevent actions such as these
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.

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 collected, to the extent practicable, from the individual directly and not from other sources. Where confidential information is obtained from other sources, a record must be maintained of the sources from which the Data Steward obtained the confidential information.

Data Review
All information should be reviewed on a periodic basis 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 loss if disclosed, but should be protected to prevent unauthorized disclosure.
3. Public – information that may be freely disseminated.

All information resources should be categorized and protected by the relevant data steward 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
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). 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, 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. Data stewards may enact more restrictive policies for end-user access to their data, provided they are consistent with this program and any applicable laws, regulations, policies and practices of the California State University (CSU) system and Cal Poly.

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. Due to space limitations, records are sometimes stored in remote on-campus or off-campus locations. Periodic inspections to ensure record security must be conducted and documented. Requirements for record retention is set for thin the CSU Records Disposition Schedule (http://cusco.calstate.edu/Operations/archive_infor.shtml).

The Data Steward is responsible for determining, documenting and communicating the appropriate retention schedule and methods for disposing of the University information under their control. Data retention and destruction must be consistent with this program and any applicable laws, regulations, policies and practices of the CSU system and Cal Poly.

Records Access
The Records Access Manual prepared by the CSU Office of General Counsel (http://www.calstate.edu/GC/Docs/Records_Access_Manual.doc) provides an overview of the three most significant statutes governing access to University records: (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 Public Records Act was enacted to give the public information about how state business is being conducted; it calls for the disclosure of 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 by the steward of the information 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. For more information, see [practice under development].
Individuals’ Rights
Individuals have the right to inquire and be notified about whatever personal information a state agency maintains concerning them. An opportunity to inspect any such personal information must be afforded within 30 days of any request. If the record containing their personal information also contains personal information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies and/or views of records containing any personal information about them, and this information must be provided within 15 days of the inspection. The University may charge a reasonable cost for providing this information. Individuals may request that the appropriate Data Steward amend their personal information, and, if the request is denied, the individual may request a review of that decision by the President or his designee.

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.

Training
Education should be provided to ensure that affected individuals understand the Information Security Plan and their role in protecting University information. Periodic updates should be provided to ensure awareness of any changes. The appropriate Data Steward should keep documentation of training.

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. All contracts with service providers must include a privacy clause, which requires the service provider to implement appropriate measures to safeguard confidential information, and to refrain from sharing any such information with any other party. Contracts must, when appropriate, include the requirement that in addition to the CSU insurance requirements for service agreements, the service provider be bonded and
maintain personal liability insurance, which protects against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of the service provider to protect University information. In addition, contracts must include the requirement that any breach of security be immediately reported to the University.

**Compliance and Consequences of Non-Compliance**

Each department will develop policies and procedures addressing risk assessment, access, physical security, training and security awareness and any other issues deemed necessary to protect data, computer systems and networks under their control from internal and external threats based on the classification of data and value of the physical assets.

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 periodic risk assessments. If the assessment involves computer systems, 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. Suspected violations of law may be referred to appropriate law enforcement agencies. Records of security incidents must be maintained and potential evidence secured to aid in future investigations by the University or law enforcement.

**Security Incident Reporting**

All security incidents involving University data must be reported to the appropriate Data Steward. The Data Steward will investigate and notify the Information Security Officer and other campus officials as appropriate. 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.

All security incidents involving a potential threat to computer systems, networks and/or information technology resources, must be reported to the Vice Provost/Chief Information Officer or designee via abuse@calpoly.edu. The Vice Provost/Chief Information Officer will investigate and notify the Information Security Officer and other campus officials as appropriate. University departments found to be in non-compliance with the program will be required to take specific steps to bring computer systems, networks or other information technology resources into compliance within a specified time. Depending on the severity and nature of the risk involved, non-compliant systems may be removed from the University network until the risk is fully addressed and measures are taken to prevent any future recurrence.
Security incidents involving University data and computer systems or networks must be reported to both the appropriate Data Steward and the Vice Provost/Chief Information Officer (abuse@calpoly.edu) for investigation and, if warranted, reporting to other entities. 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.

Roles and Responsibilities

Vice President for Administration & 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 (Computing Equipment Loss Report Summary), computer system incidents and University information incidents (Incident Record Report Summary) provided by the Information Security Officer.
- Provides an annual report to the University President.

Information Security Officer
- Coordinates, administers, and communicates the Information Security Program.
- Maintains and updates the Information Security Program, as needed.
- Informs Vice Presidents, Deans, Department Heads and Data Stewards about the Information Security Program and related policies and procedures.
- Provides training regarding the requirements of the Information Security Program.
- Promotes and encourages good security policies and procedures.
- Monitors campus compliance with information security policies and procedures.
- Investigates, tracks, resolves, and reports suspected violations of policies and procedures in coordination with Data Stewards and/or the Vice Provost/Chief Information Officer.
- Reviews quarterly records of computing equipment losses and security incidents and determines action needed, if any.
- Provides an annual report of computing equipment losses (Computing Equipment Loss Report Summary), computer system incidents, and University information incidents (Incident Record Report Summary) to the Vice President for Administration & Finance and the Vice Provost/Chief Information Officer.
- Provides coordination support between the various Data Stewards on campus as Chair of the Security Committee.

Vice Provost/Chief Information Officer
- Provides policy and operational guidance to the University 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 all digitally-based information and the computing resources, networks, and applications that support and enable its use as required by the Data Steward.
Coordinates with the Information Security Officer on the investigation, tracking, resolution, and reporting of security issues involving information technology resources.

Informs System and Equipment Stewards and Users about the Information Security Plan and related policies and practices.

Receives and responds to suspected violations within areas of direct responsibility and as requested or assigned by the University.

Maintains an Incident Record Report that contains a record of each incident and its resolution, including any new security measures implemented in response to the incident.

Provides a quarterly Incident Record Report summary report to the Information Security Officer.

Maintains the Incident Record Reporting system and/or related information technology systems as appropriate.

---

Vice Presidents/Deans/Department Heads

- Responsible for maintaining information as an asset of the University.
- Informs Data Stewards, System and Equipment Steward, and Users about the Information Security Program.
- 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.
- Conducts periodic risk assessments.

---

Data Stewards

- Identifies and classifies sensitive data under their control.
- Identifies authorized users of data under their control.
- Identifies and takes steps to mitigate exposures related to vulnerabilities.
- Determines level of security required.
- Maintains the required level of security.
- Prepares and maintains a manual of security procedures for their area.
- Ensures existence of backup, disaster, and recovery capabilities.
- Assists in the investigation and resolution of suspected violations of policies and procedures in coordination with the Information Security Officer and, if applicable, the Vice Provost/Chief Information Officer.
- Tests existing security safeguards.
- Reports suspected violations of security policies and procedures involving computer systems to Information Technology Services at abuse@calpoly.edu.
- Responds to requests for information from the Information Security Officer regarding security.
- Protects confidential and personal information in custody of the University.
Ensures security of the repository or equipment where the information under their control is stored, transmitted and/or processed.

Protects the privacy rights of University faculty, staff and students.

Promotes and encourages good security procedures and practices.

Provides training to employees on information security requirements and procedures, including compliance with the Information Security Program.

Reports security breaches to individuals whose unencrypted personal information, was, or is reasonably believed to have been, acquired by an unauthorized person in accordance with Appendix D, Implementation Practices and Procedures of Cal Poly’s Information Technology Resources Responsible Use Policy (http://security.calpoly.edu/policies/index.html).

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.
- Protects the privacy rights of University faculty, staff and students.
- Prepares and maintains a manual of security procedures for their area.
- Ensures establishment of backup, disaster, and recovery capabilities.
- Assists in the investigation of suspected violations of policies and procedures related to support systems.
- Tests existing security safeguards.
- Reports suspected violations of security policies and procedures involving computing systems to Information Technology Services at abuse@calpoly.edu
- Develops and implements procedures to foster awareness in personnel in their area of the importance of, and responsibility for, the security of computing equipment, data, and information.
- 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.
- Responds to requests for information from the Information Security Officer and Vice Provost/Chief Information Officer regarding security.

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.
- 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.
- Reports suspected violations of security policies and procedures for University information to the appropriate Data Steward.
Cal Poly
Information Security Program
DRAFT – 12/8/2003

➢ Reports suspected violations of security policies and procedures of computer systems to Information Technology Services at abuse@calpoly.edu.
➢ Protects the physical security of data and systems assigned to them.

University Property Services
➢ Provides quarterly a Computing Equipment Loss Report Summary to the Information Security Officer that contains information about lost or stolen computing equipment.

Human Resources/Academic Personnel/Judicial Affairs
➢ Investigates alleged security violations by individual students, faculty and staff
➢ Interprets and recommends sanctions and discipline regarding security violations in accordance with existing policy and practice.

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.

Security Committee
➢ Informs Users about the Information Security Program.
➢ 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 & Finance.
➢ Develops and implements procedures and educational material to foster awareness in personnel of the importance of, and responsibility for, the security of University information under their control.

University Police
➢ Receives and investigates all reports of computing equipment thefts.
➢ Investigates security violations if illegal activities are suspected.

Exceptions and Plan Review
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. Exceptions involving digital information assets and information technology resources must be reviewed and approved by the Vice Provost/Chief Information Officer. All requests for exceptions will be responded to in writing. This plan will be reviewed annually and updated by the Information Security Officer, as needed.

Appendix A - Definitions
Appendix B - References
Appendix A

Definitions

Access
Ability given to individual or groups of users to use information stored on or via University resources. This includes, but is not limited to, the ability to read, write, view, create, alter, store, 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.

Computing System / Network / Information Technology Resources
Any computing resource, service, or network system, including workstations, servers, networks, storage devices, peripheral equipment, input/output and connecting devices, data processing functions, and related records, programs, software and documentation.

Digital Information Assets
Information transmitted, stored, accessed, retrieved 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.

Education Records
Any information or data recorded in any medium that is directly related to a student.

Individually Identifiable Health Information
Any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provisions of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
Personal Information
Any information maintained by an agency 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, and medical or employment history. It includes statements made by, or attributed to, the individual.

Personal information in the context of a security breach 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
Any person or entity that receives, maintains, processed, or otherwise is permitted access to customer information through its direct provision of services to a financial institution.

University Information
Information related to the function or purpose of the University. Includes information about individual students and employees.
Appendix B

References

Cal Poly, Information Technology Resources Responsible Use Policy (RUP)
Cal Poly, Confidentiality-Security Agreement
Cal Poly, Computer Crimes Policy
Cal Poly, Password Management Criteria
CSU 4CNET Responsible Use Policy
CSU Security Policy, May 15, 1997
CSU Memo, Increased Security Measures for CMS, March 26, 2003
CSU Memo, Compliance with the Gramm-Leach-Bliley Act-Safeguarding Confidential Personal Data, May 21, 2003
CSU Information Security Policy, August 2002
California Information Practices Act of 1977
California Code of Regulations, Title V, Sections 42396 through 42396.5
California Education Code, Section 89546, Employee Access to Information Pertaining to Themselves
CMS Security Requirements
Comprehensive Computer Data Access and Fraud Act (California Penal Code, Section 502)
Health Care Portability and Accountability Act of 1996 (HIPAA) – Privacy Rule
Family Education Rights and Privacy Act of 1974 (FERPA)

Patriot Act of 2001

Records Disposition Schedule

Requirements for Protecting Confidential Employee Data: Updated to Reflect Confidentiality Agreement Requirements; CSU Coded Memo: HR 2003-05, March 13, 2003

Student Records Administration; CSU Executive Order No. 382