

## CSU INFORMATION SECURITY POLICY

The Board of Trustees (BOT) of the California State University (CSU) is responsible for protecting the confidentiality of information in the custody of the CSU, the security of the equipment where this information is processed and maintained, and the related privacy rights of the CSU students, faculty and staff concerning this information. This policy applies to all students, faculty and staff, consultants employed by the CSU or any other person having access to CSU information technology resources. The unauthorized modification, deletion, or disclosure of information included in CSU data files and data bases can compromise the integrity of CSU programs, violate individual privacy rights and possibly constitute a criminal act. This responsibility is delegated to the campus Presidents in accordance with CSU policies. In order to implement these policies and procedures, each campus President and the Chancellor should designate an Information Security Officer (ISO) to oversee this important program.

To ensure that the Information Security Officer is not in a position of conflict of interest, he/she should not have immediate direct responsibility for a data processing facility (e.g. computer operations manager) nor should he/she be an official having program responsibility for the confidential information. If possible, he/she should be independent of, and have no personal responsibility for campus programs that rely on the confidential information or computer operations which manipulate and store the information. The responsibilities and duties of the Information Security Officer are delineated, at a minimum, in this policy statement.

If the campus Information Security Officer and the campus Information Resource Manager are not the same person, the Information Security Officer should keep the Information Resource Manager informed of any changes of security and confidentiality procedures affecting the Information Resource Management program. Similarly, the campus Information Resource Manager should provide coordination and services support to the Information Security Office in the area of security and confidentiality as requested.

### REFERENCES

Article 1, Section 1, of the Constitution of the State of California, defines pursuing and obtaining privacy as an inalienable right.

The Information Practices Act of 1977 (Civil Code Section 1798, et seq.) places specific requirements on State agencies in the collection, use, maintenance and dissemination of information relating to individuals.

The California Public Records Act (Government Code Sections 6250-6265) provides for the inspection of public records.

The Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502) affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer information systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.

Title V Section 42396.2(d) of the California Code of Regulations confirms the right to privacy in California and states an intent to implement it within the CSU.

The Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g) (commonly referred to as FERPA or the Buckley Amendment) is a federal statute applicable to every institution which receives federal funds. It protects students (and former students) from the release of personal information about them. It provides for the right of a student to inspect and review his or her own education record, the right to request the records be amended, and the right to some control over the disclosure of personally identifiable data from such records.

### SECURITY PROCEDURES

Each campus and the Chancellor's Office should develop and maintain a written set of security policies and procedures that at a minimum implement information security and confidentiality practices consistent with these guidelines.

### SECURITY GUIDELINES

Security procedures at a minimum, should address the following topics:

1. Physical Security:
  - a. Protection against natural/accidental disasters:
    - Fire prevention, detection, suppression and warning.
    - Smoke detection and warning.
    - Water detection and warning.
    - High temperature detection and warning.
    - HVAC malfunction warning.
    - Electrical power monitoring and warning.
    - Environmental contamination (food, drink, etc.).
    - Emergency power usage warning.
  - b. Protection against intentional disasters:
    - Employee and student facility access control.
    - Annual review of all personnel access needs.

- Operating system software access control.
- Magnetic media access control.
- c. Management controls and procedures:
  - Security procedures.
  - Emergency procedures.
  - Record keeping.
  - Risk analysis (cost/benefit).
  - Reporting computer equipment thefts and breaches of security.
  - Disaster recovery planning (computers, networks, terminals and data).
  - Management audit.
- d. User controls and procedures:
  - Terminal access control.
  - Terminal logon/logoff control.
- 2. Data Security:
  - a. Definitions:
    - Confidential information.
    - Critical applications.
    - Critical information.
    - Other critical resources.
  - b. Data Security Policy:
    - Implementation of cost/effective data security systems (RACF, firewalls, routers, etc.).
    - Assumption that all data is confidential and private and must be secured.
    - Standard internal labeling of all magnetic media.
    - Backup and off-site storage of all data in secure data vaults.
  - c. Responsibilities of the following for Data Security:
    - President.
    - Information Security Officer.
    - Program Managers.
    - System Development and Programming Managers.
    - Data Processing Managers.
    - Users.
    - Public Safety.
    - Human Resources.
  - d. Identification of Security Requirements:
    - Category of threats.
    - Risk analysis.
    - Cost effective solutions.
    - Testing of security procedures.

- e. Required Security Measures:
  - Organization and administration.
  - Control of operating system software.
  - Control of application software and data.
  - Control of Transaction systems (CICS).
  - Control of Timesharing systems (TSO).
  - Control of Database systems (DB2, Oracle).
  - Control of magnetic media storage.
- f. Guidelines for System Design:
  - Completeness of data.
  - Integrity of data.
  - Accuracy of data.
  - Audit trails of critical data changes (grade changes, residency determination, etc.).
- g. Personnel Policies and Procedures:
  - Background checks.
  - Use of resources for authorized, sanctioned and approved activities only.
  - Signed statements of published security guidelines.
  - Individual unique user ID/passwords (no shared IDs).
  - Access privileges controlled on a need to know basis (files, records, data elements, data bases, applications, screens, terminals, etc.).
  - Security training to ensure understanding of standards.
  - Limited password life (semester, 90 days, etc.).
  - Assignment of responsibilities (access privileges granted).
  - Reassignment of responsibilities (access privileges reviewed).
  - Termination of employment (access privileges removed).
  - Annual review of access privileges for all students and employees.

## **SUGGESTED LIST OF RESPONSIBILITIES FOR CAMPUS INFORMATION RESOURCE PERSONNEL**

### PRESIDENT

1. Responsible for protection of all campus information resource assets and proper reporting of all losses and violations of information confidentiality, security and privacy policies and procedures.
2. Appoints Information Security Officer.
3. Delegates review and investigative authority to Information Security Officer.
4. Ensures independence of Information Security Officer and the compliance function.
5. Provides necessary resources for the Information Security Officer to carry out his/her function.
6. Provides necessary training for the Information Security Officer to carry out his/her function.

### INFORMATION SECURITY OFFICER

1. Promotes and encourages good security policies and procedures.
2. Performs appropriate risk analysis.
3. Prepares and maintains a manual of campus security procedures for applications, data bases, remote access, distributed processors, and microcomputers.
4. Monitors to ensure compliance of privacy and information security policies and procedures.
5. Identifies and reduces vulnerabilities.
6. Informs campus President and others about security matters.
7. Coordinates determination of the priority and data sensitivity of applications and other information processing activities.

8. Coordinates cost/benefit analysis to determine level of security required.
9. Ensures establishment and existence of backup, disaster, and recovery capabilities.
10. Develops campus-specific public access implementation policies and procedures.
11. Following notification by Public Safety, investigates violations of security and confidentiality policies and procedures.
12. Annually develops a summary report of computing equipment losses and violations of security and confidentiality policies and procedures.
13. Implements procedures to assist in the development of security awareness in personnel.
14. Develops plans to test existing security safeguards.
15. Annually, performs audit of all confidentiality and security policies and procedures to ensure highest confidence in those policies and procedures.

#### PROGRAM MANAGEMENT

1. Identifies and classifies sensitive data.
2. Identifies authorized users of data.
3. Assists with the identification of exposures related to vulnerabilities.
4. Makes public access decisions based on decision-making criteria with the concurrence of the Information Security Officer.
5. Maintains required level of security.
6. Applies sanctions and disciplines for security violations.
7. Reports to Public Safety all computing equipment losses due to theft.
8. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.

9. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data and information.

## SYSTEM DEVELOPMENT AND PROGRAMMING MANAGEMENT

1. Understands and implements CSU security policies and procedures.
2. Understands security problems in a data processing environment.
3. Addresses data security requirements in all systems development.
4. Explains available security tools to program managers.
5. Tests security measures.
6. Implements technical security measures specified by program manager.
7. Reports to Public Safety all losses of equipment due to theft.
8. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.
9. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information.

## DATA PROCESSING MANAGEMENT

1. Provides logical security features and tools for use by program managers.
2. Describes procedure requirements to protect against natural, accidental, and intentional disasters.
3. Describes required facilities management controls and procedures.
4. Reviews system development designs for adequacy of security provisions.
5. Ensures that security provisions are implemented as designed.
6. Performs risk analysis with Information Security Officer.
7. Provides assurance that computer information is adequately secured prior to implementing general public access.
8. Regularly inventories computing equipment and reports unexplained losses to the Information Security Officer and other proper officials.

9. Reports to Public Safety all equipment losses due to theft.
10. Reports to the Information Security Officer all violations of security and confidentiality.
11. Develops and implements procedures to foster awareness in personnel of the importance of, and responsibility for, the security of computing equipment, data, and information.
12. Insures adequacy of safeguards of irrecoverable corporate data assets.

#### INDIVIDUAL USERS

1. Strictly observes all laws, policies and procedures related to privacy, confidentiality and security of information.
2. Reports to Public Safety all losses of equipment due to theft.
3. Reports to the Information Security Officer all violations of security and confidentiality policies and procedures.
4. Develops and implements procedures to foster awareness in personnel of the importance of and responsibility for, the security of computing equipment, data, and information resources.

#### PUBLIC SAFETY

1. Participates in the development of the campus' statement of security procedures.
2. Receives and investigates all reports of computing equipment thefts.
3. Responsible for, at a minimum, annual reporting to the Information Security Officer of thefts, specifically identifying information technology resources.