California State University, Sacramento

INFORMATION SECURITY PROGRAM

I. Preamble

The California State University Sacramento Information Security Program establishes appropriate and reasonable administrative, technical and physical safeguards designed to:

- ensure the security and confidentiality of personal information in its custody, whether in electronic, paper, or other forms;
- protect against any anticipated threats to the security or integrity of such personal confidential personal information; and
- guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to faculty, staff, and students.

The CSUS Information Security Program complies with CSU requirements for information security and the requirements of the following federal and state laws, regulations, and Chancellors Office directives:

- Gramm-Leach-Bliley Act (GLB Act) Compliance (Federal Trade Commission 16 CFR Part 314 Standards for Safeguarding Customer Information) requires a documented information security program, including managers responsible for program, risk identification and assessment, safeguard procedures and monitoring, service provider oversight, and evaluation and adjustment (see http://www.educause.edu/security/resources/glb.asp for additional information)
- The CSU Records Access Manual, maintained by General Counsel (http://www.calstate.edu/GC/Docs/Records_Access_Manual.doc), provides guidance on access from the perspectives of the California Public Records Act, the California Information Practices Act, and the Family Educational Rights and Privacy Act (FERPA). Sections F and G of the California Information Practices Act have been added to reflect the new SB1386 requirement (effective July 1, 2003) for notifying all California affected residents of any security breach where confidential data may have been acquired.
- Charles Reed Letter to Presidents of March 26, "Subject: Increased Security Measures for CMS", requires Executive approval for access to confidential personal information, employee signed confidentiality agreement document, filing of confidentiality documents in HR, periodic electronic audits, and PeopleSoft programmatic changes in CMS software to mask confidential data.
- Charles Reed Letter to Presidents of March 28, "Subject: Information Security Clarification" extends the March 26 requirements to ALL systems containing confidential data.
- HR 2004-08 "Requirements for Protecting Confidential Employee Data: Updated to Reflect Confidentiality Agreement Requirement" (http://www.calstate.edu/HRAdm/pdf2004/HR2004-08.pdf), includes sample confidentiality forms and definition of confidential data elements.

II. Scope

The Gramm-Leach-Bliley Act (GLB Act) Compliance (Federal Trade Commission 16 CFR Part 314 Standards for Safeguarding Customer Information) requires the development of an Information Security Program for the protection of customer non-public personal information associated with financial services (e.g., financial aid, student accounts receivable, etc). The CSUS Information Security Program meets the needs of the GLB Act, but is also extended to

apply to ALL (not just financial related) confidential personal information that is processed and/or maintained by CSU Sacramento or any CSU Sacramento auxiliary organization.

This plan applies to all students, faculty and staff, consultants or any other person having access to CSUS confidential personal information employed by CSUS or any CSUS auxiliary organization.

The unauthorized access, modification, deletion, or disclosure of confidential personal information included in CSUS data files and data systems can compromise the integrity of CSUS programs, violate individual privacy rights, and is expressly forbidden. Careless, accidental or intentional disclosure of confidential personal information may result in disciplinary action against those involved in unauthorized disclosure and civil action against CSUS.

In certain limited circumstances as specified in the California Information Practices Act of 1977, CSUS may disclose confidential personal information. The more common exceptions which permit disclosure under the California Information Practices Act are provided in Appendix A.

III. **Definitions**

Access means a personal inspection or review of the confidential personal information or a copy of the confidential personal information, or an oral or written description or communication of the confidential personal information.

Disclosure means to permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential personal information by any means, orally, in writing, or by electronic or any other means to any person or entity.

Confidential personal information as used in this document means information that identifies or describes an individual, is sensitive, or is non-public, including, but not limited to, his or her social security number, physical description, date of birth, home address, home telephone number, ethnicity, gender, education records, financial matters, medical or employment history, and performance evaluations. It includes statements made by, or attributed to, the individual. For Section F of the California Information Practices Act (SB1382), c*onfidential personal information* 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 or 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.

Information Security Program Coordinator is the individual responsible for maintaining the Information Security Program and implementing the provisions of the program.

Custodian(s) of Record(s) means the functional individual(s) or manager(s) responsible for one or more of the business processes and procedures involved in the processing of confidential personal information. The Custodian of Record is responsible for the safeguarding of specific categories of confidential personal information and is generally considered the "owner" of the data and the system containing the data.

Handled means the access, collection, distribution, process, protection, storage, use, transmittal or disposal of information containing confidential data

Information Security Manager is the individual or manager responsible for designing, developing, and/or administering the electronic security mechanisms used to protect confidential personal information in one or more systems in the custody of the University, including the security of the equipment, network, software, and/or repository where this information is processed and/or maintained.

Service Provider means any third party person or entity that receives, maintains, processes, or otherwise is permitted access to confidential personal information through its provision of service directly to the university.

IV. **Roles and Responsibilities**

A. Vice President for Academic Affairs

The President has delegated responsibility to the Vice President for Academic Affairs for the overall administration of the CSUS Information Security Program. To effectively implement and administer the CSUS Information Security Program, the responsibility for protecting confidential personal information; the security of the equipment and/or repository where the information is processed and/or maintained; and, the related privacy of CSUS faculty, staff, students, and other stakeholders has been further delegated as follows:

B. Information Security Program Coordinator

The Manager, Administrative Computing has been appointed Information Security Program Coordinator by the Vice President for Academic Affairs and is responsible for implementing the provisions of this Plan. The coordinator shall:

- Assist the Custodians of Records and Information Security Managers in identifying reasonably foreseeable internal and external risks to the security and confidentiality of confidential personal information;
- Evaluate the effectiveness of the current safeguards for controlling these risks;
- Monitor to ensure that risk assessments are conducted by each Custodian of Record and Information Security Manager;
- Provide training to the Custodians of Records and Information Security Managers regarding the requirements of the Information Security Program;
- Provide recommendations for revisions and update/maintain the Information Security Program as appropriate;
- Prepare an annual report on the status of the Information Security Program.

C. *Custodian(s) of Record(s)*

The Custodian of Record is the functional manager or individual responsible for the business processes and "owned" systems covering a particular category of confidential personal information. With the technical assistance of the appropriate Information Security Managers, the Custodians of Records are responsible for:

- Protecting the privacy rights of University faculty, staff and students;

- Protecting the confidentiality of information in their "owned" systems and functional areas;
- Identifying and monitoring risks to the security of confidential personal information;
- Developing plans and procedures to preserve the information in the event of natural or man-made disasters;
- Ensuring the protection and safeguarding of confidential personal information in the design and administration of business processes;
- Ensuring the appropriate handling, storage, retention, and destruction of physical records containing confidential personal information in the various offices;
- Promoting and encouraging good security practices and procedures;
- Providing appropriate training to those individuals who may have access to the confidential personal information;
- Ensuring compliance with the CSUS Information Security Program; and
- Preparing an annual report to critically evaluate the adequacy of existing safeguards, compliance with campus safeguarding policies and procedures and recommendations for implementation of addition safeguards for the categories of confidential personal data maintained within their "owned" systems.

Individuals in the following positions have been identified as campus Custodians of Records:

- Associate Vice President, HR - Faculty Affairs is responsible for safeguarding the confidential personal information maintained in the HR component of the CMS HRSA system;
- Associate Vice President, Financial Services and Management Services is responsible for safeguarding the confidential personal information maintained in the CMS Financials System.
- Registrar is responsible for safeguarding the confidential personal information maintained in the Student Information System and the SA component of the CMS HRSA system;
- Program Center Executives are responsible for safeguarding non-centralized confidential personal information maintained in program center or other ancillary data systems, equipment, and records within their program center

D. Information Security Manager(s)

Information Security Managers are primarily responsible for the technical aspects of system security, including the following:

- Protecting the privacy rights of University faculty, staff and students;
- Protecting confidential personal information in the electronic systems within the custody of the University;
- Providing and administering security for the electronic equipment, network, software, and/or repository where the information is processed and/or maintained;
- Working with CSU and campus centralized data base administration, operating systems support, desktop support, and network support groups in developing and implementing the most appropriate and current system security procedures;
- Identifying and monitoring risks for which the University must be prepared;
- Promoting and encouraging good security procedures and practices;
- Developing plans and procedures to preserve the information in case of natural or man-made disasters;

- Assisting the Custodian of Record in preparing an annual report which critically evaluates the adequacy of existing safeguards, compliance with campus safeguarding policies and procedures; and recommendations for implementation of additional safeguards.

V. **Risk Assessment**

The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control risks. The Information Security Program Coordinator will work with all relevant area Custodians of Records and Information Security Managers to carry out comprehensive risk assessments. Risk assessments will include system-wide risks (the Coordinator will facilitate assistance from UCCS in conducting network, operating system, and dba system-wide risk assessment), as well as risks unique to each area with covered data. The Coordinator will ensure that risk assessments are conducted at least annually and more frequently where required.

Risk assessments will include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; systems for detecting, preventing, and responding to attacks, intrusions, or other system failures; and the appropriate handling, storage, retention, and destruction of physical media containing confidential personal data.

Example risks to assess include, but are not limited to:

- Online access of confidential personal information by unauthorized personnel;
- Unauthorized disclosure or misuse of confidential personal information by employees;
- Unauthorized access to hardcopy files or reports;
- Unauthorized use of another's account and password;
- Compromised system security as a result of system hacker intrusion;
- Denial of service attacks;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data in a disaster;
- Inadequate audit trails for detection and investigation;
- Unauthorized transfer of confidential personal information through third parties

VI. **Information Safeguards and Monitoring**

The CSUS Information Security Program is expected to verify and document that safeguards exist and are sufficient to protect covered data. The Information Security Program Coordinator will ensure that appropriate safeguards are implemented in each of the areas where risks to the security of covered data have been identified.

CSUS has developed the following general policies and practices necessary to reasonably safeguard confidential personal information:

A. Collection

As specified in the California Information Practices Act of 1977, confidential personal information shall not be collected unless it is appropriate and relevant to the purpose for which it will be collected. It must be collected, to the extent practicable, from the individual directly and not from other sources. Where information is obtained from other sources, a record must be maintained of those sources from which the confidential personal information was obtained.

There shall be no confidential personal information collected or maintained which has not been approved by the appropriate Custodian of Records.

B. Access

No CSUS employee or CSUS auxiliary organization employee shall be granted access to centralized electronic data systems or physical media containing confidential personal information in the custody of CSUS without review and written approval by the Vice President for Administration and Business Affairs. Such approval will only be granted in cases where the access is required for the employee to perform a critical university or auxiliary function that is part of the employee's job duties. CSUS employees or CSUS auxiliary organization employees who currently have such access to information are subject to this review and written approval process in order to continue their access capability.

Employees approved for security access must receive appropriate training and sign a confidentiality agreement.

Employees with approved access to electronic information will be assigned an account by the appropriate Custodian of Record or Information Security Manager. Accounts will be immediately deactivated upon the separation of the employee.

A current list of employees with copies of their written access approval documents and confidentiality agreement must be kept on file in Faculty Staff Affairs.

C. Training

All CSUS employees and CSUS auxiliary organization employees having access to confidential personal information will receive training at least annually regarding the University's policy for safeguarding confidential personal information. Training shall include controls and procedures to prevent employees from providing customer information to an unauthorized individual and how to properly handle, store and dispose of documents that contain personal identifying information. Information on the university's Information Security Program shall be presented at new employee (faculty and staff) orientation and the importance of confidentiality shall be stressed.

D. Physical Security of Records

All printed material containing confidential personal information must be protected by the appropriate level of physical security as determined by the Custodian(s) of Record(s).

E. Record Retention

The maintenance of records beyond the retention requirements set forth in the CSU Records Disposition Schedule presents a significant risk to the security and integrity of confidential personal information. Due to space limitations, "historic records" are sometimes stored in remote campus locations and periodic inspections to ensure record security must be conducted and documented. Unless longer retention is specifically approved by the appropriate Custodian(s) of Record(s), records containing confidential personal information shall be destroyed within 3 months following the required period of retention.

F. Record Destruction

Record destruction is the responsibility of the Custodian(s) of Record(s). All printed material containing confidential personal information shall be destroyed when retention is no longer necessary. Destruction must prevent unauthorized access to confidential personal information (i.e., shredding).

Prior to the survey and disposal of a campus computer or the transfer of a computer from one campus user to another user, the computer's hard drive shall be wiped clean using a low level formal utility to remove the operating system, software applications installed on the computer and any personal files which were stored on the computer.

Questions regarding desk top security procedures may be directed to the Desktop Services of UCCS.

G. Information Systems Security

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This will include designing limitations to access, using roles and permission lists to refine levels of authentication and authorization, maintaining appropriate screening programs to detect computer hackers and viruses, and implementing security patches.

Safeguards for information processing, storage, transmission, retrieval and disposal may include: requiring electronic covered data be entered into a secure, password-protected system; using secure connections and encryption to transmit data both inside and outside the University; using secure servers; using firewalls and DMZs; using updated anti-virus software; minimizing the use of transportable media (floppy drives, zip drives, etc) to store covered data; permanently erasing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them; providing safeguards to protect covered data and systems from physical hazards such as fire or water damage; maintaining an inventory of servers or computers with covered data; and other reasonable measures to secure covered data during its life cycle in the University's possession or control.

H. Monitoring and Testing

Systems and controls will be implemented to test and monitor the effectiveness of information security safeguards. Monitoring will be performed to ensure that safeguards are being followed and to detect breakdowns in security. The level and frequency of monitoring will be appropriate to the potential impact and probability of risk identified, and the sensitivity of the information involved. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, as well as other measure to verify that the CSUS Information Security Program's controls are working.

I. Service Provider Requirements

The University will require service providers that are permitted access to covered data to provide adequate safeguards. Contracts with such service providers will include the following elements regarding data security:

- Explicit acknowledgement that the contract permits the contractor to have access to confidential information
- A definition of the confidential information to which access is granted
- A stipulation that the confidential information must be held in confidence and accessed and used only for the explicit business purpose specified in the contract
- A stipulation from the contractor that it will ensure compliance with the protective conditions specified in the contract
- A provision requiring the contractor to return and/or destroy all confidential information upon completion or termination of the contract
- A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the University to immediately terminate the contract without penalty
- A provision allowing auditing of the contractor's compliance with protective conditions
- A provision ensuring that the contract's protective requirements shall survive any termination agreement.

VII. Required Disclosure of Security Breach

CSUS is required to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Any university student, faculty, staff, consultant or any other person having access to CSUS confidential personal information employed by CSUS or any CSUS auxiliary organization shall immediately notify the appropriate Custodian of Records, Information Security Manager, or Information Security Program Coordinator, who in turn must notify the Vice President for Academic Affairs and the campus Internal Auditor of any such unauthorized acquisition. The Vice President for Academic Affairs or the campus Internal Auditor shall, without unreasonable delay, notify the CSU Office of General Counsel.

VIII. Periodic Evaluation and Revision of the Information Security Program

The University shall periodically evaluate, test, and adjust the Information Security Program to validate that equipment and systems function properly and produce the desired results. Each Custodian of Record and Information Security Manager shall perform ongoing assessments to

ensure that employees follow written procedures for information security. Information security shall be included in internal audits. The campus shall conduct an annual review of the Information Security Program to ensure that it remains appropriate and relevant. An annual report to critically evaluate the adequacy of existing safeguards, compliance with campus safeguarding policies and procedures and recommendations for implementation of additional safeguards shall be completed by each Custodian of Record, Information Security Manager, Information Security Program Coordinator and reviewed by the Vice President for Academic Affairs.

IX. Effective Date

The campus Information Security Program is effective October 2004.

X. References

CSU Coded Memo: HR 2004-08, March 1, 2004
CSU Memo, Increased Security Measures for CMS, March 26, 2003
CSU Memo, Information Security Clarification, March 28, 2003
CSU Memo, Compliance with the Gramm-Leach-Bliley Act-Safeguarding Confidential Personal Data, May 21, 2003
CSU Information Security Policy, August 2002
CSU Records Access Manual, February 2003

Appendix A - Authorized Disclosures

The following list is a general summary of permitted disclosures under the California Information Practices Act of 1977. Consultation with University Counsel before releasing confidential personal information covered by either Act is required.

- to the individual to whom the information pertains;
- where the individual to whom the information pertains has given voluntary written consent to disclose the information to an identified third party no more than 30 days before the third party requested it, or within the time limit agreed to by the individual in the written consent;
- to an appointed guardian or conservator of a person representing the individual provided it can be proven with reasonable certainty through CSU forms, documents or correspondence that the person is the authorized representative of the individual to whom the information pertains;
- to persons within the CSU who need the information to perform their functions;
- to another government agency when required by law;
- in response to a request for records under the California Public Records Act (unless the Public Records Act provides an exception);
- where there is advance written assurance that the information is to be used for purposes of statistical research only and where the information will be redisclosed in a form that does not identify any individual;
- where the CSU has determined that compelling circumstances exist which affect the health or safety of the individual to whom the information pertains, and notification is transmitted to the individual at his or her last known address, and disclosure does not conflict with other state or federal laws;
- pursuant to a subpoena, court order, or other compulsory legal process it, before disclosure, the CSU notifies the individual to whom the record pertains, and if the notification is not prohibited by law;
- pursuant to a search warrant;
- to a law enforcement or regulatory agency when required for an investigation of unlawful activity of or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.