CALIFORNIA STATE UNIVERSITY CHANNEL ISLANDS

ADMINISTRATIVE POLICY MANUAL

Information Technology
Policy Due for Review: <Office Use Only>

Policy Number: <Office Use Only>
Number of pages: 15
(not including this page)

Policy on Confidentiality and Security

HISTORY

	Drafted By	Approved By	Approval Date	Effective Date	Supercedes
Original	Robert Gutierrez Peter Mosinskis Dale Velador	<Office Use Only>	<Office Use Only>	<Office Use Only>	<Policy #>

Dr. Richard R. Rush – President

Approval Signature _____ Date _____

Information Technology
Approved By: <Office Use Only>
<Office Use Only>

Policy Number: <Office Use Only>
Effective Date: <Office Use Only>

Policy on Confidentiality and Security

Purpose:
The Confidentiality and Security Policy provides information to individuals about their responsibilities regarding CSU Channel Islands institutional data. The Confidentiality and Security Policy is intended to encompass all computer systems, networks, data files, web and related information utilized throughout the entire University and preclude the need for separate agreements.

The Confidentiality and Security Policy establishes appropriate and reasonable administrative, technical and physical safeguards to:

- ensure the security and protection of confidential information in its custody, whether in electronic, paper, or other forms;
- protect against any anticipated threats or hazards to the security or integrity of such confidential information; and
- protect against unauthorized access to or use of such confidential information.

Background:
The University requires the responsible use of all CSU Channel Islands institutional data. Institutional data includes data such as student records, financial aid information, as well as and applications used on campus systems to enter, view, or manipulate such data. The University's computer systems, related data files, and the information derived from them are important to the University. Anyone utilizing these systems shares the responsibility for the security, integrity and confidentiality of information.

The CSU Channel Islands Confidentiality and Security Policy is supported by the CSU Channel Islands Confidential Information Security Plan. Both are designed to protect individual privacy and safeguard confidential information. The CSU Channel Islands Human Resources Access and Compliance document provides additional detail and information about the CSU, State and Federal requirements.

All existing laws (federal, state and local), California State University and CSU Channel Islands regulations and policies apply, including Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act of 1996 (HIPAA); State of California Senate Bill 1386; California Penal Code Section 502; Information Practices Act Of 1977 (CA Civil Code Sec. 1798); California Public Records Act (CA Government Code Sec. 6250 - 6276.48); Principles of Personal Information Management (CA Code of Regulations, Title 5, Sections 42396 – 42396.5). Links to these laws may be found in Exhibit B.

Policy on Confidentiality and Security

A number of policies and procedures from higher education institutions were consulted, adapted and/or reviewed in developing this policy. Links to these policies can be found in Exhibit B.

Accountability:
President, Vice President for Finance and Administration, Vice President for Academic Affairs, Vice President for Student Affairs, Information Security Officer

Applicability:
Faculty, staff, administrators, students and others who are granted access to University information. Also applies to all information that is processed and/or maintained by CSU Channel Islands or any CSU Channel Islands auxiliary organization that contains data deemed confidential.

Definitions:
Access: the 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.

Account: That combination of user name and password that provides an individual with access to a computer system or computer network

Auxiliary: An auxiliary organization is any non-profit entity which (1) has agreed to comply with the applicable requirements of the CSU Board of Trustees and CSU Channel Islands campus; (2) is included in the list of officially recognized auxiliary organizations in good standing maintained by the Chancellor pursuant to Section 42406, infra, and (3) maintains the status of an auxiliary organization in good standing. The term auxiliary organization includes any organization described in Education Code Sections 89901 and 89300.

CMS: The California State University Common Management Systems project as implemented by CSU Channel Islands. CMS is a common set of administrative computer software applications which support human resources, financials, and student services. CMS also functions as the primary repository for human resources, financials, and student information for the University.

Policy on Confidentiality and Security

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, non-public personal data, confidential personal information or sensitive information*. It is information that identifies or describes an individual, including, but not limited to, his or her social security number, physical description, home address, home telephone number, ethnicity, gender, other telephone number, signature, passport number, bank account number, education, financial matters, medical or employment history, and performance evaluations. It includes statements made by, or attributed to, the individual. *Confidential Information* also includes computerized data that includes 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. *Confidential Information* does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. *Confidential Information* does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

***Disclosure*:** to permit access to or to release, transfer, disseminate, or otherwise communicate all or any part of confidential information by any means to any person or entity.

***Financial Information*:** information which includes but is not limited to an individual's number of tax exemptions, amount of taxes withheld, amount of OASDI withheld, amount and type of voluntary/involuntary deductions/reductions, survivor's amounts, net pay and designee for last payroll warrant.

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.

Policy on Confidentiality and Security

Permitted Disclosures: disclosures of confidential information permitted under the California Information Practices Act of 1977.

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

Third Party: any individual (or individual on behalf of an organization) who is not an employee of California State University Channel Islands.

User: Anyone who has been provided access to the information technology resources of CSU Channel Islands, including the general public

Policy:

A. Guiding Principles

CSU Channel Islands users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information, as required by law or University policies.

Electronic mail and computer files are considered private to the fullest extent permitted by law. However, in the event of a sanctioned University investigation for alleged misconduct, e-mail or files may be locked or copied to prevent destruction and loss of information. Users may employ methods to increase the privacy of their files, provided they do not violate any provision of this policy or state, federal or international laws, or knowingly degrade system/network performance.

All users of CSU Channel Islands' information technology resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information. CSU Channel Islands strives to provide the highest degree of security when transferring data, but users of CSUCI information technology resources must understand these measures might be circumvented and information might be intercepted, copied, read, forged, destroyed or misused by others.

Policy on Confidentiality and Security

Reasonable, foreseeable internal and external risks to the security and integrity of confidential information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information have been identified. These risks may include, but are not limited to:

- Unauthorized access of confidential information by anyone not approved for access;
- Compromised system security as a result of system access by a computer hacker
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Poor audit trails
- Errors introduced into the systems
- Lack of transaction completeness and documentation
- Unauthorized access of confidential information by employees
- Unauthorized telephone requests for confidential information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of confidential information through third parties

It is recognized that this may not be a complete list of the risks associated with the protection of confidential information. Since technology growth is not static, new risks are created regularly.

B. Policy Provisions

1. The unauthorized modification, deletion, or disclosure of confidential information can compromise the integrity of CSU Channel Islands programs, violate individual privacy rights, and is expressly forbidden. Careless or intentional disclosure of confidential information may result in disciplinary action against those involved in unauthorized disclosure and civil action against CSU Channel Islands.

2. **Access**. All employees and non-employees, such as auxiliary employees, volunteers, and others that request and are granted access to information technology resources are required to sign the following documents:
    a. A PeopleSoft System Access Request Form;
    b. a CSU Channel Islands Human Resources Access and Compliance Form; and
    c. a statement indicating that a copy of the Confidentiality and Security Policy has been received.

Policy on Confidentiality and Security

Links to the statement and forms can be found in Exhibit B. A copy of the signed statement and forms will be retained in the individual's official personnel file. Additionally, copies of Access and Compliance Forms should be kept on file with the appropriate University/Auxiliary Manager or Administrator.

If a current or new employee refuses to sign the forms and the statement, they will not be given access to the system. If such access is an inherent part of their assigned job duties and they therefore cannot perform this part of their job, appropriate disciplinary action will be considered. If a non-employee refuses to sign the statement, they will be denied access.

No CSUCI employee or CSUCI auxiliary organization employee shall be granted access to centralized electronic data systems containing confidential information in the custody of CSUCI without review and written approval of the Vice President for Finance and Administration. The approval of access to confidential information will be based on several factors including the division executive's determination that access is required for the employee to perform a critical university or auxiliary function that is part of the employee's job duties and responsibilities and assurance that all requirements contained in the Confidential Information Security Program designed to protect individual privacy and safeguard confidential information will be met.

Questions about training regarding confidentiality and security should be referred to the Director of Human Resources.

Employees with approved access to electronic information will be assigned an account by the Information Security Officer or University/Auxiliary Manager or Administrator. Access to University data will be immediately revoked upon the separation of the employee. An employee approved for access to electronic information does not need to complete an additional Access and Compliance Form for access to non-electronic information.

All data is governed by federal, state and local laws as well as University policies. Access to data is based on the "need to know" philosophy that is directly related to an authorized user's assigned duties at the University.

Policy on Confidentiality and Security

3. Authorized users are responsible for the security of whatever data they retrieve. They will provide all necessary safeguards to all sensitive and/or confidential information including storage, reproduction, destruction or modification of data. Authorized users are responsible for ensuring the security of the equipment where such data is held or displayed.

4. Authorized users must restrict information retrieval and other computing activities only to data to which they have been permitted access as related to their assigned duties. Further, users may only use functions and utilities for which they have been authorized and trained to use. Types of training may include handouts, classroom instruction, one-on-one instruction, or online training guides.

5. Computer accounts, passwords, and other types of authorization are assigned to individual users for exclusive use only and should not be shared with, or delegated to, others. Authorized users are responsible for any student assistant, temporary help and/or production accounts issued in their name.

6. Users may not:
    a. run or otherwise configure software or hardware to intentionally allow access by unauthorized users;
    b. disclose data or information in a way which violates applicable policy, procedure or other relevant regulations or laws; and
    c. inappropriately modify or destroy data or information

7. **Physical Security of Records.** All printed material containing confidential information must be protected against destruction, loss, or damage from potential environmental hazards such as fire, or water damage, to the extent possible and as determined by the appropriate University/Auxiliary Manager or Administrator.

8. **Collection of Confidential Information.** Confidential 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 information was obtained.

    There shall be no confidential information collected or maintained which has not been approved by the Information Security Officer.

Policy on Confidentiality and Security

9. **Record Destruction.** Record destruction is the responsibility of University/Auxiliary Managers and Administrators. All printed material containing confidential information shall be destroyed when retention is no longer required. Destruction must prevent unauthorized access to confidential information (i.e., destroying papers by 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 format utility to remove the operating system, software applications installed on the computer and any personal files which were stored on the computer.

   Questions regarding desktop security procedures may be directed to the campus office of Information Technology Services.

10. **Common Management System (CMS).** CMS security contains components that are managed locally by campuses as well as components that are managed centrally by the Chancellor's Office CMS staff. Campus CMS security responsibilities are managed by security designees in the CMS functional areas and Information Management department. CMS security at the Chancellors Office is managed by Software Operations Support Services (SOSS), Hardware Operations Support Services (HOSS), Network Services (CENIC), and the outsourced data center service provider (Unisys).

    Detailed CMS security requirements and management responsibilities have been identified by responsible area and are documented in *CMS Security Requirements*, a document developed and maintained by HOSS. A link to this document can be found in Exhibit B.

    This document outlines security requirements and management responsibilities for the following:
    1. CMS Application Security
    2. CMS Logon Security
    3. Network Security
    4. CMS Database Security
    5. CMS Web Server Security
    6. CMS Unix Security

11. **Department Privacy and Safeguarding Plan for non-CMS Systems.** Any University department, organization or auxiliary that utilizes confidential information outside of the

University CMS must develop and implement a written department Privacy and Safeguarding Plan. Plan development and implementation is the responsibility of each University/Auxiliary Manager or Administrator. While there is no prescribed document format, at a minimum, the plan must be dated and signed by the appropriate University/Auxiliary Manager or Administrator and must include:

1. name of the office, department, or operation where confidential information is handled;
2. identification of confidential information handled;
3. number of individuals with access to confidential information;
4. administrative controls implemented to minimize the number of individuals with access to confidential information;
5. description of physical security of records methods;
6. discussion of records retention and destruction methods; and
7. discussion of training content, frequency, delivery method, etc.

12. **Service Provider Requirements**. Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the University is unable to provide on its own. Further, vendors may be needed to assist in the disposal of the volumes of hard-copy confidential information that is generated by the University and its auxiliaries. In recognition of its responsibility for the performance and actions of these vendors, the following actions are required:

    Due Diligence of Service-Providers – The adequacy of the service provider's system of safeguarding information shall be determined prior to the University or its auxiliaries entering into a contractual relationship with the service provider. The University shall not contractually engage a service provider who cannot demonstrate that they have a system to safeguard student information. Depending on the service provider, the University and University Auxiliary may wish to review the service provider's audits, summaries of its test results for security, or other internal and external evaluations. The University or University Auxiliary shall not enter into contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

    Service Provider Agreements – 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. Current provider contracts without a privacy clause are valid until September 1, 2005.

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.

13. **Permitted Disclosures of Confidential Information.** The California Information Practices Act was enacted in 1977 to protect individual's privacy rights in "personal information" contained in state agency records. The Act reflects the Legislature's determination that the right to privacy is in jeopardy and that the maintenance and dissemination of private information should be subject to strict limits. The Act prohibits disclosure of personal information except in certain limited circumstances. The more common exceptions which permit disclosure are contained in Exhibit A. Some of these disclosures may impose requirements not included in this document. Consultation with the Information Security Officer is required before releasing personal information covered by the Information Practices Act.

14. **Required Disclosure of Security Breach**. The University is required to disclose any breach of system security to individuals 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 CSUCI confidential information employed by CSUCI or any CSUCI auxiliary organization shall immediately notify the Information Security Officer **and** the Vice President for Finance and Administration. The Vice President for Finance and Administration or the Information Security Officer shall, without unreasonable delay, notify the CSU Office of General Counsel.

15. **Individuals' Rights**. Individuals have the right to inquire and be notified about whatever confidential information CSUCI maintains concerning them. An opportunity to inspect any such confidential information must be afforded within 30 days of any request. If the record containing the confidential information also contains confidential information about another individual, that information must be deleted from the record before it is disclosed. Individuals may request copies of records containing any confidential information about them, and those copies must be provided within 15 days of the inspection. The University/Auxiliary may charge a reasonable per page cost for making any copies. Individuals may request that their personal information be amended and, if the request is denied, the individual may request a review of that decision by the Vice President for

Finance and Administration or designee. The viewing of personnel files is governed by the respective collective bargaining agreements for represented employees.

16. **Periodic Evaluation and Revision**. The University shall periodically evaluate, test, and adjust the *Confidential Information Security Program* to validate that equipment and systems function properly and produce the desired results. The Information Security Officer and each University/Auxiliary Manager shall perform ongoing assessments to ensure that employees follow written procedures for information security. The campus shall conduct an annual review of the *Confidential Information Security Program* to ensure that it remains appropriate and relevant.

Exhibit(s):

Exhibit A
Permitted Disclosures
The University may not disclose confidential information except in certain limited circumstances. The more common exceptions permit disclosure in the following circumstances:

- 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 if, 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 or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

Exhibit B
Laws
A partial list of applicable laws are provided for reference.

Family Educational Rights and Privacy Act (FERPA)

- US Code (USC): http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+20USC1232
- Code of Federal Regulations (CFR): http://www.access.gpo.gov/nara/cfr/waisidx_03/34cfr99_03.html

State of California Senate Bill 1386

- http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Comprehensive Computer Data Access and Fraud Act (California Penal Code Section 502)

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9

Information Practices Act Of 1977 (CA Civil Code Sec. 1798)

- http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=1798&hits=20

California Public Records Act (CA Government Code Sec. 6250 - 6276.48)

- Full law text: http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=gov&codebody=public+records+act&hits=20
- Summary: http://www.thefirstamendment.org/capra.html

Policy on Confidentiality and Security

Principles of Personal Information Management (CA Code of Regulations, Title 5, Sections 42396 – 42396.5)

- http://ccr.oal.ca.gov/

Gramm-Leach-Bliley Act of 1999 (Federal Trade Commission Regulations – 16CFR, Part 314 – Standards for Safeguarding Customer Information; Final Rule, May 23, 2002)

- http://www.sec.gov/rules/final/34-42974.htm

Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002

California Education Code, Section 89546, Employee Access to Information Pertaining to Themselves

- http://www.leginfo.ca.gov/.html/edc_table_of_contents.html

Health Care Portability and Accountability Act of 1996 (HIPAA)-Privacy Rule

- http://aspe.hhs.gov/admnsimp/pl104191.htm#1177

California Civil Code, Sections 1798.80-1798.84 and Section 1798.29

- http://www.leginfo.ca.gov/calaw.html

CSU System-wide References

"Requirements for Protective Confidential Employee Data: Updated to Reflect Confidentiality Agreement Requirement" (CSU System-wide Human Resources Memoranda, HR 2003-05)

- http://www.calstate.edu/HRAdm/pdf2003/HR2003-05.pdf

CSU Coded Memo: HR 2004-08, March 1, 2004
CSU Coded Memo: HR/PR 93-01, March 8, 1993
CSU Coded Memo: HR/PR 93-04, Supplement #1, March 18, 1993
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

Policy on Confidentiality and Security

CSU Executive Order 877, Designation of Health Care Components for Purposes of the Health Portability and Accountability Act of 1996 (HIPAA)
CSU Executive Order 698, Policy for The California State University Auxiliary Organizations.

CMS Security Requirements. Hardware Operations Support Services (HOSS), Chancellor's Office

- http://cms.calstate.edu/T3_Documents/TechnicalOverview/CMS%20Security%20Requirements%2011062001.doc

Links to Required Access Forms

- PeopleSoft System Access Request Form (http://www.csuci.edu/cicms/CSUCI_PSoft_System_Access_Request_Form.pdf)
- CSU Channel Islands Human Resources Access and Compliance Form (http://www.csuci.edu/hr/hrforms.htm)
- Statement indicating that a copy of the Confidentiality and Security Policy has been received

Computer policies and procedures from the following institutions were consulted, adapted and/or reviewed in developing this policy:

- California Polytechnic State University, San Luis Obispo Confidentiality and Security Policy (http://www.afd.calpoly.edu/risk/info_security.html)
- California Polytechnic State University, San Luis Obispo Responsible Use Policy (http://its.calpoly.edu/Policies/RUP-INT/)
- SUNY Potsdam Acceptable Use Policy (http://www.potsdam.edu/CTS/Policies/AUP.html)
- University of California Berkeley Administrative Applications and Data Security Policy (http://socrates.berkeley.edu:7015/admsecpol.html)
- CSU Long Beach Confidential Information Security Program (http://daf.csulb.edu/forms/bhr/safetyrisk/CISProgram.doc)