



California State University East Bay Information Security Policy

Responsible Unit:	Information Technology Services (ITS)
Refer Questions To:	Information Security Officer
Issue Date:	1996
Approved By:	Chief Information Officer
Distributed To:	Cal State East Bay Community

Table Of Contents

1.0	PURPOSE	4
1.1	Commitment to Information Security	4
1.2	Scope	5
2.0	ORGANIZING INFORMATION SECURITY	5
2.1	Accountability for Information Assets	5
3.0	ASSET MANAGEMENT	5
3.1	Ownership of Assets.....	5
3.2	Classification of Assets	5
3.3	Restricted Assets	6
3.3.1	<i>Social Security Numbers (SSNs)</i>	6
3.3.2	<i>Credit Card, Bank Account Information</i>	6
3.3.3	<i>Human Subject Information</i>	6
3.3.4	<i>Personally Identifiable Medical Information</i>	7
3.4	Protecting Information Assets	7
3.4.1	<i>Backing-Up Information Assets</i>	7
3.5	Inventory of Assets.....	7
4.0	HUMAN RESOURCE SECURITY	7
4.1	Prior to Employment	7
4.2	During Employment	8
4.2.1	<i>Information Awareness, Education and Training</i>	8
4.2.2	<i>Segregation of Duties</i>	8
4.2.3	<i>Change of Employment</i>	8
4.3	Termination	8
4.3.1	<i>Return of University Assets</i>	8
4.3.2	<i>Removal of Access Rights</i>	8
5.0	ACCESS CONTROL	9
5.1	Access to Information by University Employees	9
5.2	Access to Information by Students or Non-Employees.....	9
5.3	Access to Information by Business Associates	9
5.4	Network Access Control	9
5.5	Wireless Access Control	10
5.6	Operating System Access Control.....	10
5.7	Directories	10
5.8	Acceptable Use Policy.....	10
5.9	Account Management	10
5.10	Password and Account Restrictions	10
5.11	Logging Out	11
5.12	Telecommuting.....	11
6.0	MANAGING INFORMATION SYSTEM	11
6.1	Identifying Security Requirements.....	11
6.2	Acquiring Software	11
6.3	System Development.....	11
6.4	Testing Information Systems.....	11
6.4.1	<i>Using Test Data</i>	12
6.5	Change Management.....	12
7.0	COMMUNICATION AND OPERATIONS MANAGEMENT	12

7.1	Operational Responsibilities.....	12
7.2	Operations Management.....	12
7.2.1	Configuration Requirements.....	12
7.2.2	Network Requirements.....	12
7.2.3	Logging and Monitoring Requirements.....	12
7.2.4	Documentation Requirements.....	13
7.2.5	Disaster Recovery Plan.....	13
7.3	IT Accessibility.....	13
7.4	Business Associates Delivery Management.....	13
7.5	Change Management.....	13
7.6	Protection against Malicious and Mobile Code.....	13
7.7	Media Handling.....	13
7.7.1	Discarding Information.....	13
7.7.2	Donating or Transferring Equipment.....	14
7.8	Data Exchanges.....	14
7.9	Transmitting Data.....	14
7.9.1	Transmissions via Networks.....	14
7.9.2	Downloading Data.....	14
7.9.3	Physical Media in Transit.....	14
8.0	PHYSICAL AND ENVIRONMENTAL SECURITY.....	14
8.1	Secure Areas.....	15
8.2	Access to the Data Center.....	15
8.3	Equipment Security.....	15
8.3.1	Secure Disposal or Re-Use of Equipment.....	15
8.3.2	Removal of Property.....	15
8.4	Protection against Natural or Accidental Disasters.....	15
8.5	Protection against Theft, Vandalism or Sabotage.....	15
9.0	COMPLIANCE.....	16
10.0	INCIDENT MANAGEMENT.....	16
10.1	Reporting Information Security Events.....	16
10.2	Management of Information Security Incidents.....	16
11.0	RISK MANAGEMENT AND ANALYSIS.....	16
11.1	Risk Management.....	16
11.2	Responsibility for Risk Management.....	17
11.3	Selecting a Risk Treatment Strategy.....	17
11.4	Evaluation and Audit of Risk Reduction Measures.....	17
12.0	BUSINESS CONTINUITY.....	17
13.0	ENFORCEMENT.....	17
14.0	POLICY UPDATE.....	18
15.0	REVISION HISTORY.....	18

1.0 Purpose

The California State University, East Bay (CSUEB) is committed to respecting and protecting the security and privacy of information assets entrusted to the university. The unauthorized collection, processing, modification, deletion, or disclosure of information in university files and data bases can disrupt University operations, compromise the integrity of university programs, violate individual rights to privacy, and constitute a criminal act.

The Board of Trustees (BOT) of the California State University (CSU) is responsible for ensuring the confidentiality, integrity, and availability of information in the custody of the CSU and the privacy rights of the CSU students, faculty and staff. This responsibility is delegated to the campus Presidents in accordance with CSU policies. The CSUEB President has delegated responsibility for the campus information security program to the Chief Information Officer (CIO) and campus Information Security Officer (ISO). The CIO and ISO are responsible for providing leadership on matters related to information security and overseeing the university's efforts to comply with applicable information security statutes, regulations, and CSU policies.

This policy supports the mission of the university by protecting the university's information resources, reputation, legal position, and ability to conduct its operation. The term 'information' is used as a general term and includes data stores, databases, and metadata. The purpose of this policy is to protect the interests of those university constituents who rely on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity. The university considers these security objectives met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability);
- Information is observed by or disclosed to only those who have a right to know (confidentiality);
- Information is complete, accurate and protected against unauthorized modification (integrity);
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).¹

Additionally, the information security policy is intended to:

- Provide direction on developing and implementing protection measures that establish accountability and prudent and acceptable practices regarding the use and safeguarding of campus information assets;
- Protect the privacy of personally identifiable information entrusted to the university;
- Ensure compliance with applicable CSU policies, state and federal laws, and regulations regarding the management and security of information assets; and
- Educate individual users and business associates with respect to their responsibilities associated with the use of university information assets.

The CSUEB information security policy will be reviewed and updated by Information Security Officer as needed.

1.1 Commitment to Information Security

This policy serves as a demonstration of CSUEB commitment to information security and privacy protection. The policy provides as a framework for the development of additional University information

¹ Adapted from ITIL Service Design, p. 141, 2007

security policies, standards, procedures, guidelines and the campus information security program.

1.2 Scope

Information security and risk management are based upon an appropriate division of responsibility among management, technical professionals, and program staff. Every employee and business associate that comes in contact with university data is held accountable for his/her actions. Individuals and business associates, who have been granted access to university resources, are responsible for adhering to the provisions of this policy to ensure that the confidentiality, integrity and availability of CSUEB information are maintained in accordance with applicable CSU policies, federal and state statutes, and regulations, and industry best practices governing information security.

If this policy does not address a specific issue, readers are encouraged to contact the campus Information Security Officer.

2.0 Organizing Information Security

The President and university's executive management team actively support the development and implementation of the campus information security policy and the campus information security program. This support is demonstrated through clear direction, commitment and acknowledgement of information security roles and responsibilities. The university's Information Security Officer (ISO) is responsible for coordinating activities related to information security

2.1 Accountability for Information Assets

All information entrusted to CSUEB is considered an information asset and, as such, every employee or business associate that collects, stores, processes, transfers, administers, maintains, or disposes of an information asset owned or entrusted to the university is responsible and held accountable for its appropriate use.

Misuse of university resources, including computer access or information, may be grounds for denial of access, termination of a contract, student or employee disciplinary action, and/or criminal charges.

3.0 Asset Management

CSUEB information assets are essential public resources that must be given appropriate protection from loss, inappropriate disclosure, and unauthorized modification.

3.1 Stewardship of Assets

University assets must be assigned an "asset steward" who assumes responsibility for ensuring the asset is appropriately classified according to university standards. The asset steward also defines appropriate levels of access (i.e. rights/privileges) to the asset, and periodically reviews asset classifications and access levels.

When an information asset resides on an integrated data base or is used by more than one unit, stewardship of the asset is determined by the manager responsible for the development of the database in which the information resides or the appropriate executive management.

3.2 Classification of Assets

The university's information assets have varying degrees of sensitivity and criticality. Some information assets may require additional levels of protections and special handling. The university shall adopt a data classification standard which provides guidance on classifying data assets according to its value, legal requirements, sensitivity and criticality to the university. The university's Data Classification Standard

shall also include appropriate recommendations for information labeling and handling.

3.3 Restricted Assets

Access to certain categories of information will be restricted, either because the exposure of this information can cause harm or the information is specifically protected under law or contract. Extra care must be taken to protect *restricted assets*. Such assets include Social Security Numbers, Credit Card and Bank Information, Human Subject Information, and Personally Identifiable Medical Information

Excluding his or her own personal data, no member of the CSUEB community may store Social Security Numbers (SSN), Credit Card and Bank data, Human Subject Information, or Personally Identifiable Medical Information for any person on any individual user computer without written permission from their supervisor or manager. This requirement applies to all devices capable of storing electronic information, whether the device is owned or leased by CSUEB or not, whether the data is encrypted or not, and whether the device is portable or stationary. This restriction also applies to CSUEB business associates unless there is a written agreement between the business associate and CSUEB.

3.3.1 Social Security Numbers (SSNs)

CSUEB recognizes the special risks associated with the collection, use and disclosure of social security numbers. Accordingly, the requirements of this policy apply to all social security numbers contained in any medium, including paper records.

If the collection or use of social security numbers is permitted, but not required by applicable law, the university shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of educational, business, governmental, and medical purposes. In an effort to reduce the university's use of SSNs, the university will make every effort to assign a unique identifier to each applicant, student, employee, research subject, patient, alumnus, donor, contractor, and other individuals, as applicable, at the earliest possible point of contact between the individual and the university.

All Information Systems acquired or developed after June 30, 2007 must comply with the following:

- The Information System should not use the SSN as a primary key. However, SSNs may be stored in the database, if there is a justifiable reason to do so.
- The Information System must not display social security numbers visually (such as on monitors, printed forms, system outputs) unless required or permitted by law or authorized by the manager;
- Name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the social security number; and
- The manager must maintain a record of approvals whenever they grant authorization to print SSNs on documents (e.g., reports, forms, etc.) or allow SSNs to be stored in databases.

3.3.2 Credit Card, Bank Account Information

The major credit card companies (e.g., American Express, Visa, Master Card, Discover) established the payment card industry security standards council to promote wide adoption of the payment card industry data security standard (PCI DSS or PCI). This standard establishes rules for the protection of payment card (credit and debit cards) information. University departments that accept payment cards must be compliant with the PCI standards. Colleges and departments that are planning to accept credit cards should contact the ISO to discuss plans for contracting for any services, or developing systems that involve the collection of payment card data.

3.3.3 Human Subject Information

All research that includes human subjects must be approved by the university's [Institutional Review](#)

[Board](#) (IRB). Personally identifiable data collected for, used in, or produced by research involving human subjects must be protected from inadvertent or inappropriate disclosure. Proposals for all research projects that involve such data must include an acceptable, effective, and documented procedure for the protection of such data before the project will be approved or granted continuing approval by the IRB.

3.3.4 Personally Identifiable Medical Information

Personally Identifiable Medical Information is highly sensitive and confidential, and should be treated with care. The campus Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer and Information Security Officer must be notified if a department collects, maintains or processes personally identifiable medical information. This requirement does not apply to Student Health Services.

3.4 Protecting Information Assets

Asset owners are responsible for developing and maintaining appropriate countermeasures that will assure the confidentiality, integrity and availability of information assets entrusted to CSUEB.

3.4.1 Backing-Up Information Assets

Data of value (i.e., data that would be missed if lost) which cannot be easily recreated must be backed up on a regular basis. An exception to this standard may be granted if the cost of backing up exceeds the cost of restoration from a total loss. Backup copies shall be made regularly and maintained in a different physical location to protect against physical catastrophes such as floods and fires.

The Information Technology Division shall maintain working backups of all files and data bases in its custody in the data center and secondary backups located at a remote site. Asset stewards and technical administrators must establish similar controls for information assets under their direct control. Where backup is not automatic, users who create critical files are required to backup the information in conformance with the schedule developed by the appropriate asset steward.

CSUEB obtains services from the Chancellor's Office (CO) of the California State University. It is the responsibility of the CIO to verify that the CO's backup and restoration services meet the needs of the CSUEB.

Backups and records retention shall comply with the CSU's Records Retention schedule(s).

3.5 Inventory of Assets

The university will conduct periodic inventories of confidential, sensitive or critical information assets.

4.0 Human Resource Security

The success of the campus Information Security Program is largely dependent upon the individuals who are granted access to the university's information assets. These individuals represent the university's most effective means of protecting the confidentiality, integrity and availability of university's information assets. This section describes the university's information security practices related to personnel management.

4.1 Prior to Employment

During the hiring process, manager should consider information security requirements in the selection of candidates or the hiring of business associates. Prior to hiring a new employee, the manager should carefully screen and check the backgrounds of those will have access to critical assets or confidential/sensitive information. Appropriate background verification checks ("screening") should be carried out by hiring managers under the guidance of an appropriate administrative office (e.g., Human Resources, Academic Affairs, University Police Department, Student Health Services, or the Procurement

Office).

4.2 During Employment

The manager is responsible for the following activities:

- Ensuring their employees possess the knowledge and skills necessary to effectively and responsibly use university resources in the performance of their job duties;
- Effectively segregating duties to reduce the likelihood of fraud and abuse;
- Ensuring employees receive appropriate security awareness training;
- Notifying the campus service desk when an employees transfers to another campus department or terminates their employment with the university.

4.2.1 Information Awareness, Education and Training

New employees are encouraged to participate in the university's new employee orientation program.

Employees of the Student Health Services department are required to participate in HIPAA training, offered to all medical service workers, to gain access medical information covered under HIPAA.

All university employees whose duties require access to sensitive information must complete the university's security awareness training within 15 days of gaining access to information assets entrusted to the university. This training is designed to minimize possible security risks by educating employees on appropriate information security practices. The campus information security office is responsible for providing general information security awareness training. Upon completion of information security awareness training, all employees are required to read and sign the university's Acceptable Use policy. This document will be retained on file in the Information Security Office or in the Human Resources personnel file.

4.2.2 Segregation of Duties

The manager is required to follow CSU policies, California State regulations, or best practices to ensure that staff duties are appropriately segregated to minimize the risk of fraud or abuse.

4.2.3 Change of Employment

A change in employment status occurs when an employee transfers to a new department, goes on temporary leave, or his/her duties significantly change in their home department. Changes in employment status shall trigger a review of access rights granted to the user. The manager (or designee) is required to notify the university service desk whenever there is a change in an employee's employment status. The service desk staff will follow campus procedures for managing changes in employment status.

4.3 Termination

The manager is required to notify the university service desk when an employee separates from the university. The service desk staff will follow campus procedures for separating employees from the university.

4.3.1 Return of University Assets

The manager is responsible for collecting university assets (e.g., keys, computers, etc.) from employees who are separating from the university. Additionally, the manager is responsible for ensuring that university assets provided to business associates are returned to the university or discarded under the conditions of the contract.

4.3.2 Removal of Access Rights

The campus operations team and local security administrators are required to de-active an employee's access to university applications within 3 days of being notified an employee has separated from the university. The campus Information Security Office is responsible for conducting an annual review of account holders to ensure that terminated user accounts have been appropriately de-activated.

5.0 Access Control

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Procedures to manage access to university assets, including confidential/sensitive data and critical applications, must be documented.

The information security office is responsible for processing requests to access operational systems and periodically reviewing access accounts and privileges. The campus operations team, network and server administrators, and local security administrators share responsibility for creating user accounts and credentials.

5.1 Access to Information by University Employees

The asset steward is responsible for classifying the information asset and defining its security requirements to control access to and ensure the integrity of the asset. Employees may only access critical assets or confidential/sensitive data, if access is required to perform their duties. However, assets stewards must approve such access before access is granted. If the data steward denies access to the desired protected information, access will not be granted, except upon the appeal to and approval by the asset steward's Vice President.

5.2 Access to Information by Students or Non-Employees

In no event will students or other non-employees be granted access to critical systems or sensitive/confidential university information. Passwords and accounts for student assistants or other special employees (e.g., interns, volunteers, etc.) require special monitoring by the sponsoring agent. User accounts for student assistant and special employees will provide limited access to university assets. Requests for exceptions to this requirement should be submitted to the asset steward and approved by the ISO.

5.3 Access to Information by Business Associates

The university recognizes that business associates serve an important function in the support of services, hardware and software. Contracts with business associates must require them to comply with all applicable university policies, standards, business practices, and address all Federal and State laws to which CSUEB must adhere to ensure that the university remains in compliance with such policy or law.

The manager is responsible for managing business associates access to sensitive, confidential or critical university assets. Prior to entering into a new contract with a business associate or renewing an existing contract, the manager should request a review of the business associate's information security strategy for protecting CSUEB information assets if the business associate will be granted access to critical systems or confidential/sensitive information. This review should be conducted by an appropriate university official (ISO, CIO, Risk Manager, etc.)

5.4 Network Access Control

Access to the campus network shall be managed to ensure that network services are not compromised. The university will install appropriate interfaces between the campus network and the internet or networks owned by other organizations. Appropriate authentication mechanisms will be used to manage access to areas or devices on the network that store critical applications or confidential/sensitive

materials. Users shall access network resources or services that they have been specifically granted authority to use. Appropriate authentication methods will be deployed to control access by remote users. Inactive sessions may be shut down after a defined period of inactivity.

5.5 Wireless Access Control

Users are required to comply with the Acceptable Use Policy. The university maintains processes to enforce safe wireless access (e.g., up to date virus definitions, etc.).

5.6 Operating System Access Control

The process for logging into operating systems shall be designed to minimize the opportunity for unauthorized access. All users shall be assigned a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user. In exceptional circumstances, where there is a clear benefit to the university, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Generic IDs for use by an individual shall only be allowed either where actions carried out by the ID do not need to be traced (e.g., read only access), or where there are other controls in place (e.g., password for a generic ID only issued to one staff at a time and logging such instance). Exceptions to this requirement may be granted with approval from the asset owner and the ISO.

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

5.7 Directories

Any directory application that provides access to information collected by CSUEB about individuals must adhere to all applicable privacy laws. Such laws may allow individuals to establish privacy preferences. For example, Family Educational Rights and Privacy Act (FERPA) blocks allow a student to limit the disclosure of their directory information.

5.8 Acceptable Use Policy

All users are required to follow the university's Acceptable Use Policy which defines acceptable and unacceptable computing uses and practices at the university. University employees who have access to confidential information are required to properly protect and not distribute the data in a way that compromises its confidentiality. Such employees will be required to sign the university's Access Compliance form.

5.9 Account Management

Asset stewards must establish and document criteria for issuing, reviewing, and revoking accounts used for access to critical applications or systems containing confidential/sensitive data. An Access Management Process must incorporate procedures for the following:

- Create unique identifiable accounts for all users. This includes accounts created for use by outside vendors and operational systems (system-to-system interface);
- Review accounts at least annually;
- Cancel or modify accounts or access as required when there has been a change in job duties, or to termination of employment or enrollment.

5.10 Password and Account Restrictions

All CSUEB constituents should follow recommended guidelines for strong passwords (e.g., passwords which cannot be easily guessed). Individuals with access to sensitive information are required to follow

strong passwords standards. Account holders must not share account passwords, even with supervisors or network administrators.

5.11 Logging Out

Users must log off from applications, computers, and networked device when finished. Users, who hold accounts that grant access to critical applications or confidential/sensitive data, must not leave their workstations or storage devices (e.g., PDA, flash drives, CD/DVDs, portable hard drives) unattended. If computers are located in a public or shared area, users must complete their session and log off completely before leaving their computer.

5.12 Telecommuting

Managers may authorize telecommuting activities under the provisions of the CSUEB Telecommuting Policy only if they are satisfied that appropriate security arrangements and controls are in place. Security protection measures for remote sites should be in place against theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to the university's application systems.

6.0 Managing Information System

This section describes the university's information security practices related to information systems acquisition, development and maintenance. Information systems include operating systems, business applications, off-the-shelf products and in-house developed applications. If this policy does not address a specific issue, consult with the campus CIO, ISO, or Procurement Office.

6.1 Identifying Security Requirements

Managers must ensure that the protection of the university's information assets is considered during the development phase or purchase of a new computer application. The operational requirements of new systems and changes to the operational requirements of existing systems should be discussed and documented in the early stages of a project. These requirements must consider the administrative, technical and physical controls needed to protect the confidentiality, integrity and availability of the information system. Contracts with software vendors should address the identified security requirements. Managers are required to review information security requirements and contract language with the campus CIO and/or ISO.

6.2 Acquiring Software

All software installed on CSUEB owned or leased devices (e.g., computers, PDA, portable hard drives, etc.) must be acquired from a reputable source that will accept responsibility for its integrity. Software must be used in accordance with the applicable software license.

6.3 System Development

Appropriate operational environments (e.g., development, test, and production) should be separated to reduce the risks of unauthorized access or changes to operational systems. Exceptions to this requirement must be documented and approved by an IT manager.

6.4 Testing Information Systems

Acceptance criteria for new information systems or system upgrades should be established. Suitable tests of the system(s) should be carried out prior to acceptance. A formal plan for testing and accepting new information systems or changes to an existing sensitive information system containing confidential and/or sensitive data must be documented. Exceptions to this requirement must be documented and approved by an IT manager.

6.4.1 Using Test Data

Test data should be selected with care. Non-production systems that contain data derived from production systems must be protected using the same security controls applied to the production systems. Requests for exceptions to this requirement should be submitted to the data steward.

6.5 Change Management

The use of formal change control procedures minimizes the risk to the confidentiality, integrity, or availability of the information systems. Major changes to university systems that are considered critical assets or contain confidential and/or sensitive data must follow a formal change management process. Managers are responsible for ensuring that a formal change control process is used to effectively manage a system change.

7.0 Communication and Operations Management

7.1 Operational Responsibilities

Computers that lack the most basic levels of security protection are vulnerable to attacks which can result in disclosure of confidential or sensitive data and widespread disruption to the CSUEB network and connected computers. Computing and network devices must be properly configured and maintained in order to ensure the protection of information on those resources. Individuals responsible for managing information systems, or areas where information is processed, must ensure that operating and change management procedures are documented, maintained and made available to all users who need them.

7.2 Operations Management

Individuals who are responsible for managing the campus technology infrastructure must ensure the environment is secure, patches are up to date and devices (e.g., telecommunication equipment, workstations, servers, etc.) are operated in a way to minimize the chance of a security breach.

Users must take steps to protect their desktop, laptop, PDAs and other devices (e.g., flash drives, portable hard drives, etc.) from compromise. They should select devices, operating systems or software that can be secured, and if necessary, modify default installation accounts and passwords to reduce vulnerabilities to a minimum.

7.2.1 Configuration Requirements

Server and network administrators must ensure that servers are properly protected to ensure that malicious traffic does not reach the applications on the server. Servers should be sufficiently hardened based on risk analysis and should be maintained according to campus policy, standards or procedures.

7.2.2 Network Requirements

Networks should be managed and controlled in order to protect against threats and vulnerabilities. Network managers shall implement controls and monitoring processes to ensure appropriate countermeasures are in place to minimize risk.

7.2.3 Logging and Monitoring Requirements

Appropriate logging and monitoring should be applied to enable the recording of security related events. Operational systems containing confidential or sensitive data shall be monitored and information security events logged to ensure problems are identified. System monitoring shall be used to check the effectiveness of controls adopted and to verify conformity to university policies. Logs should be protected against tampering and unauthorized access.

7.2.4 Documentation Requirements

To protect data integrity and avoid careless mistakes, system documentation should be maintained for all applications or assets containing sensitive or confidential information. System documentation should include, but not be limited to, configuration specifications, system requirements, description of installed software, inventory of assets stored on system, and implementation and maintenance procedures.

7.2.5 Disaster Recovery Plan

The security and availability of confidential information must be assured in case of a declared disaster. The university must develop and maintain a disaster recovery plan.

7.3 IT Accessibility

Information Technology resources and services provided via CSUEB-hosted Web sites to the CSUEB community or to the public must adhere to established technology accessibility guidelines and law, including Section 504 of the Rehabilitation Act of 1973 and the American Disabilities Act (ADA) of 1990.

7.4 Business Associates Delivery Management

Managers are responsible for checking the implementation of contractual agreements, monitoring compliance with agreements, and managing changes to services or products provided by agreement between the university and its business associates. The services, reports and records provided by business associates should be regularly monitored and reviewed. Changes to the provisions of services provided by the business associate should be reviewed to ensure the agreement complies with current university's information security policies and all state and federal laws governing the information security and privacy protection.

7.5 Change Management

Changes to technical operational processes must follow a change control process if the process affects a critical asset or an asset containing confidential/sensitive information.

7.6 Protection against Malicious and Mobile Code

The university's network infrastructure and other information resources must be continuously protected from known vulnerabilities and threats posed by computer viruses, worms, and other types of hostile computer programs. All CSUEB owned or leased devices that connect to the campus network must run recommended current virus protection software and adhere to any other protective measures as required by applicable policies and procedures.

Technical staff may monitor systems and/or network operations for signs of malicious code affecting the university's infrastructure and report finding to the appropriate manager.

7.7 Media Handling

The data steward must establish appropriate procedures to protect documents, computer media (e.g. tapes, disks), data and system documentation from unauthorized disclosure, modification, removal or destruction.

7.7.1 Discarding Information

Destruction and disposal of information and devices containing critical systems or confidential/sensitive information must be handled in a manner as to ensure confidential/sensitive data cannot be retrieved and recovered by unauthorized persons. Whenever authorized users print confidential/sensitive information, they are responsible for properly disposing of the printed information, once it is no longer required.

Confidential/sensitive information assets shall be retained in a secure environment before being released to authorized individuals for appropriate disposal. Users must follow the guidelines issued by the Receiving department for recycling or disposal of confidential information which the users no longer require.

7.7.2 Donating or Transferring Equipment

When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that critical systems or confidential/sensitive data is rendered unreadable. Users must follow the guidelines issued by the Receiving department for donating or transferring equipment that is no longer needed.

7.8 Data Exchanges

Formal exchange policies, procedures and controls must be in place to ensure that the confidentiality, integrity and availability of information are protected during a transfer between computing systems or database applications. Exchanges of information between campus departments or operational systems should be based on a formal exchange agreement or policy, and should be compliant with all relevant university policies and applicable regulations governing the protection of information assets. Transfer of data files from one data center to another should include mutual validation of the identity of the transmitting and receiving computers prior to allowing the transfer to occur.

7.9 Transmitting Data

7.9.1 Transmissions via Networks

Whenever critical or confidential information is transmitted via the network, appropriate security is required. It is the responsibility of Managers to establish appropriate controls to protect the transmission of confidential/sensitive information via the network. The possibility of unauthorized intrusion can be reduced through the appropriate use of encryption, authentication techniques, gateways and the installation of firewalls and the routine examination of their logs.

7.9.2 Downloading Data

If a file containing confidential/sensitive data is downloaded to a local or mobile device (e.g., desktop, laptop, PDA, etc.) from a university operational system, the requirements for information confidentiality and integrity that have been established for the data file in the source system must be adhered to while it is stored on the local or mobile device.

7.9.3 Physical Media in Transit

Media containing critical systems or confidential/sensitive data shall be protected against unauthorized access, misuse or corruption while in transit. Employees are strongly encouraged to use cryptographic tools as a protection measure.

8.0 Physical and Environmental Security

Appropriate controls must be employed to protect physical access to university resources in proportion to the criticality or importance of their function and the confidentiality of any impacted Information Resources affected. These controls must be commensurate with the identified level of acceptable risk assigned to the resource. The university must adopt appropriate safeguards to manage access to the physical asset. Safeguards should address the management of credentials which permit physical access to areas; management of user access privileges when there is a change in employment status; and monitoring of visitors and business associates who require physical access to campus areas where critical assets or

confidential/sensitive information may be located.

8.1 Secure Areas

Confidential or sensitive information should be housed in secure areas that are protected from unauthorized physical access or damage. Managers are responsible for ensuring that secure areas are protected by appropriate entry controls. The university's Facilities Management department, Environmental Health and Safety office, and University Policy Department should work with managers to develop and implement physical safeguards to protect secure areas against damage from man-made, environmental, or natural disasters.

8.2 Access to the Data Center

The Data Center must be locked at all times. Only those university employees whose responsibilities require that they have access to the data center should have credentials to enter. Such employees are required to protect their credentials from loss or unauthorized use. The CIO or ISO authorizes and periodically reviews the list of employees who are permitted access to the data center. Credentials which grant access to the data center should be changed at regular intervals, whenever an employee, who has been given access to the credentials, terminates, or whenever a question exists regarding the security of the existing credentials.

Access to the data center is permitted to other university personnel, business associates or escorted visitors when such entrance is authorized by CIO or ISO. The person supervising the data center must identify any individual not known and refuse entrance to anyone not authorized unless permission is granted by the CIO or ISO

Staff, faculty, and students are encouraged to question the presence of outsiders in any university work areas and to report any unusual occurrences to the University Police Department.

8.3 Equipment Security

Users must not leave workstations, fax machines and other devices that contain confidential/sensitive data unattended.

8.3.1 Secure Disposal or Re-Use of Equipment

University employees may refer to the Receiving department for direction on appropriate methods for equipment and media disposal. Employees may also contact the Information Security Officer for further guidance.

8.3.2 Removal of Property

Media containing critical assets or confidential/sensitive data shall not be taken off campus without prior authorization from asset steward or manager. University employees are required to follow the campus' policy for guidance on removing or transferring university property.

8.4 Protection against Natural or Accidental Disasters

University buildings were designed to meet all building standards in effect at the time of construction. The main data center should use a combination of countermeasures (e.g., fire prevention, detection, suppression and warning systems) to provide protection against natural, environmental, or accidental disasters. In selecting the location for the placement of servers, managers must take into account the availability of appropriate physical protection.

8.5 Protection against Theft, Vandalism or Sabotage

The primary protection against intentional risks such as theft, intrusion, or vandalism is vigilant observation by the CSUEB community and adherence to policies related to the securing of equipment and locking of rooms when not occupied and firm control of access by means of account and passwords and access limits. Employees must notify the University Police department when they discover an incident of theft, vandalism or sabotage.

9.0 COMPLIANCE

Appropriate campus officials are expected to develop and implement procedures and standards to ensure the university complies with legislative, regulatory and contractual agreements. Campus records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and CSU requirements. Managers are responsible for ensuring that all security procedures within their area of responsibility are carried out to achieve compliance with campus information security policies and standards.

10.0 Incident Management

Information security events should be reported through appropriate management channels as quickly as possible. All employees and business associates who have been given access to information assets entrusted to CSUEB or utilize university services must report observed or suspected security weaknesses in systems or services to their manager.

10.1 Reporting Information Security Events

Any member of the campus community who has evidence that university information assets have been accessed without proper authorization or detects suspicious activity that could potentially expose, compromise or destroy information assets entrusted to CSUEB must report these incidents to his /her immediate supervisor or manager. The manager must report the incident to the CIO or ISO. No one should take it upon himself or herself to investigate or remediate the matter without proper authorization from the campus ISO and/or CIO (or designee).

Members of the campus community who observe information security violations may also report them anonymously by directly contacting the Information Security Officer.

10.2 Management of Information Security Incidents

Reported CSUEB information security incidents will be managed using CSUEB's Incident Management Procedures to ensure that a consistent and effective approach is applied to the management of information security incidents involving the unauthorized disclosure or unencrypted personal data collected, processed, stored, transmitted or disposed of by university staff, its auxiliary units and business associated. The incident management procedure describes a series of steps that guide the campus in its response to information security events and helps ensure that timely corrective action is taken. The campus ISO is responsible for coordinating the campus response to an information security incident.

11.0 Risk Management and Analysis

11.1 Risk Management

Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis and the initiation and monitoring of appropriate practices in response to that analysis through the university's Risk Management Program. Risk management for information technology is an essential aspect of the total CSUEB Risk Management Program.

11.2 Responsibility for Risk Management

The Vice President of Administration and Finance/Chief Finance Officer is responsible for the university's Risk Management program. The CIO is responsible for information technology risk management coordination. Managers are responsible for risk analysis and management in conjunction with the files and data bases under their direct jurisdiction.

11.3 Selecting a Risk Treatment Strategy

It is the responsibility of the managers responsible for risk management to select risk treatment strategies that are appropriate, based upon the nature of the threat, the consequences of the loss, and the costs of the possible counter measures.

Once a prevention plan is agreed upon and approved, it is the responsibility of all affected managers to implement the plan in the shortest time possible, consistent with the risk assessment and to assure that appropriate communication to affected users takes place, necessary training is conducted, and employees uniformly apply the new measures according to the plan.

11.4 Evaluation and Audit of Risk Reduction Measures

The Information Security Officer is responsible for developing plans to test existing security safeguards and performing audits of all security policies and procedures to ensure confidence in those policies and procedures. The CIO, managers and others are responsible for active participation in the assessment, and may perform additional monitoring of implemented risk reduction measures on an on-going basis. When appropriate, previously implemented safeguards may be discarded, modified, or replaced in order to maintain the identified acceptable risk environment.

12.0 Business Continuity

The university must develop and maintain a business continuity plan (BCP) that ensures the continuity of essential functions or operations following or during the recovery phase of a catastrophic event. The campus BCP shall include, but not be limited to, the following procedures:

- **Business Impact Analysis:** A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result in the event of a disruption of programs or operations.
- **Risk Assessment:** A process of identifying the risks to the university, assessing critical functions necessary for the university to continue business operations; defining controls in place to reduce the university's exposure and evaluating costs for such controls.

Each campus unit that provides essential functions must develop a business continuity plan or provide input to the business continuity plan of a governing business unit. Each campus business continuity plan must be approved/signed-off by the head of the campus unit and forwarded to the campus Business Continuity Planning group. All campus business continuity plans must be tested on a regular basis as needed. Plans should be updated whenever changes occur in operating procedures, processes or key personnel.

13.0 Enforcement

It is the responsibility of all faculty, staff and students to report any suspected or confirmed violations of this policy to the Information Security Officer. Members of the campus community who observe information security violations may report them anonymously by contacting the Information Security Officer.

Employees who fail to adhere to this policy may be subject to penalties and disciplinary action, both within and outside the university. Violations will be handled through applicable university disciplinary procedures.

A violation of this policy by business associates, interns or volunteers may result in penalties and disciplinary action, both within and outside the university. Violations will be handled through applicable university disciplinary procedures and may include terminating the work engagement.

Students who violate this policy may be referred to student judicial affairs. Students may be subject to a review under CSU Executive Order No. 970, Student Conduct Procedures.

The university may temporarily suspend, block or restrict access to resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

14.0 Policy Update

Technological advances and changes in business requirements will necessitate periodic revisions to university policies and standards. In cooperation with other members of the university community, the Information Security Officer shall periodically reassess this policy to determine if revisions are needed to accommodate changes in information security or weaknesses in the policy. Deficiencies within this policy should be immediately communicated to the campus Information Security Officer.

15.0 Revision History

Issue/Revision Date	Approving Committee/Official
Original issue date: 1996	AVP Information Technology
Revised: 03/06/2009	CIO