CALIFORNIA STATE UNIVERSITY BAKERSFIELD

Information Security Policy

CSU Bakersfield Policy

Document Number: ITS-90.012
Last Revision Date: 6/9/2022
Responsible Office: Information Technology Services
Effective Date: 2/20/2019
Primary Author: CIO & AVP of Information Technology

General Description

Purpose:

Define the Information Security Policy for CSU, Bakersfield.

Definition:

The Information Security Policy for CSU, Bakersfield.

Scope:

All employees, vendors, applicants, auxiliary personnel, and persons of interest

Policy/Procedure

California State University Bakersfield recognizes that access to information found on campus information systems is a valuable asset to the academic and business processes of the University. Moreover, reasonable protection of the confidentiality, availability, privacy and integrity of all data including the management of personal information is an integral endeavor towards University excellence.

The California State University Bakersfield Information Security Policy establishes a set of guidelines and expectations to enhance the information security needs of the University. This Policy strives for a balance between the University's desire to promote and enhance the free exchange of ideas and its need for security of critical information and systems. It seeks to promote an environment of recognition for information security and the responsibilities to protect data by all members of the University. This policy recognizes the security concerns from threats outside as well as within the University and serves to protect the University's information resources by setting forth guidelines, responsibilities and procedures to prevent, deter, and respond to compromises of information security.

Statement of Purpose

The purpose of this Information Security Policy is to bridge the gap between the various applicable laws the University must adhere to and the principles of best practices utilized on campus related to managing information security. In doing so, it is important to identify the roles and responsibilities of all University faculty, staff, students, vendors, and consultants when working with electronic information and the information systems containing such information. The objectives of this Policy are to:

- Define the confidentiality, privacy and accessibility of information used in the support of the University's objectives;
- Define the roles and responsibilities of University faculty, staff, students, vendors, and consultants;
- Define the security principles for data, access, and physical security;
- Define the principles and procedures for incident response handling.

Definitions:

Information Security Officer (ISO) - a job title given to a person responsible for the overall management of security for an organization's information technology resources and infrastructure.
Associate Vice President for Information Technology Services) - a job title given to a person responsible for the overall management of information technology in an organization.
Information Systems - term used to generally identify any technology device that stores data for the purpose of giving access to such data remotely.
Computing Systems - a general term given to a computer workstation commonly used by faculty and staff to obtain, manipulate and store data.
Confidential information - information stored digitally or physically requiring restrictions to access and its dissemination, as defined by federal or state law.
Personal information - any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

I. Privacy and Confidentiality

A. A number of federal and state laws apply to the information collected and maintained by the University. Therefore, it is imperative that the University adhere to applicable privacy and confidentiality laws and thoroughly identify and distinguish personally identifiable information as confidential or public. The following federal and state laws are observed and adhered to by

the University for the protection of all data found on University information systems. This is a partial list of privacy laws, both State and Federal, that are pertinent to all members of the California State University, Bakersfield community. It is provided as a resource that might prove useful to faculty, staff, and students and is not intended to be a definitive source for all laws pertaining to privacy or privacy-related issues.

1. **The Family Educational Rights and Privacy Act (FERPA)**

   Enacted in 1974, FERPA (also known as the Buckley Amendment) affords students (or parents if the student is a minor) certain rights with respect to the student's "education records." As defined under FERPA, the term "education records" encompasses a broad range of materials and information such as disciplinary, financial and academic records established during a given student's enrollment and maintained in a variety of University databases and other filing arrangements. In particular, FERPA provides that "education records" and personally identifiable information contained therein may not be released or disclosed (including disclosure by word of mouth) without the written consent of the student (or parents, as the case may be). Violations of FERPA may result not only from the unauthorized disclosure of education records but also from the failure to exercise due care in protecting such records against unauthorized access from outsiders. However, even in the absence of express student (or parental) consent, FERPA permits disclosure of education records to University employees who have a legitimate interest in the student and to outside parties in a variety of circumstances, such as those where public health or safety are at issue.

2. **Health Insurance Portability and Accountability Act (HIPAA)**

   Enacted in 1996, HIPAA sets national privacy standards for the protection of certain types of health information to the extent such information is electronically transmitted by health plans, health care clearinghouses, and health care providers. The University is subject to HIPAA as a provider of student health care through the Student Health Center.

3. **The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA))**

   Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure.

4. **California Information Privacy Act**

The California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. The Act stipulates that if there's a security breach of a database containing personal data, the responsible organization must notify each individual for whom it maintained information. The Act, which went into effect July 1, 2003, was created to help stem the increasing incidence of identity theft.

5. California SB 25

SB 25 extends those Social Security number restrictions to all government agencies, including public colleges and universities. Under SB 25, public entities will have to ensure that Social Security numbers don't get posted or displayed on any printed material, or used on identification cards.

6. California Code of Regulations, Title V, Sections 42396 - 42396.5

Title V of the California Code of Regulations, specifically sections 42396 - 42396.5 addresses privacy and principles of personal information management applicable to the California State University.

7. Information Practices Act of 1977 (IPA)

Found in the California Civil Code (Sections 1798.14-1798.23), the IPA requires state agencies to record only personal information that is relevant and necessary to accomplish the purpose of the agency. Additionally, the agency should collect personal information directly from the individual who is the subject of the information rather than from any other source.

8. California Public Records Act

The California Public Records Act addresses exclusions to the disclosure of public information of personally identifying information that may be a violation of personal privacy.

9. Social Media Privacy: Postsecondary Education

SB 1349 is Effective January 1 2013.

B. California State University Bakersfield (CSUB) identifies various types of personal information to be confidential in nature. Confidential data at CSUB is categorized into two levels. Level I data contains information of extreme sensitivity that triggers legal obligations to the University to disclose any compromise of information contained in this category. Level II data contains

information that the University considers confidential as per federal and state regulations as well as University protocol.

1. Confidential Information (Level I)
2. Confidential Information (Level II)
3. Non-Confidential Information

II. Roles and Responsibilities

University President

The role of the University President regarding information technology is to ensure University compliance with this policy in accordance with all existing local, state and federal laws pertaining to the security of University information systems and protection of the confidentiality, availability, privacy and integrity of all data on such systems. Furthermore, the University President is the sole authority to authorize the release of confidential information for the purpose of responding to court-ordered subpoenas.
If anyone on campus wishes to introduce a new server that contains confidential or personal information, that person should take his/her request to the appropriate Cabinet officer. If the Cabinet Officer approves, he/she will schedule a meeting with the Information Security Officer and the Associate Vice President for Information Technology Services to discuss the need for a server and how information contained on the server will be safeguarded. The President will make the final decision about whether to approve the server. The President may assign additional roles and responsibilities appropriate to the campus.

Information Security Officer (ISO)

The role of the Information Security Officer is to establish policy and procedures to protect the integrity of confidential and personal information. The ISO also has responsibility for investigating any potential breaches of this information.

Associate Vice President for Information Technology Services (AVP ITS)

The role of the AVP ITS is to lead the University's activities regarding information technology. The AVP ITS will lead IT staff in carrying out the University's technology support for information security ensuring the security of all University information systems and protection of the confidentiality, availability,

privacy and integrity of all data on such systems.

Administrative Officials (VPs, Deans, Directors, and other supervisory personnel)

The responsibilities of administrative officials include those of all campus users in addition to the following responsibilities:

- Identify and define subordinates access privileges needed to perform their job
- Recommend access to information systems for subordinates
- Ensure subordinates have completed any and all confidentiality compliance forms
- Ensure subordinates have received appropriate training regarding computer security and handling of confidential information

Information Technology Services Personnel

All Information Technology Personnel are expected to comply with all responsibilities of campus users in addition to the following responsibilities:

- User passwords cannot be reset without confirming user identity
- Passwords of users must not be requested at any time
- Report security breaches immediately to the ISO
- Vendor, auditor or consultant access to any information system required to perform the scope of work initiated by the University must be approved by supervisory personnel prior to access
- Access to or possession of any information system or data stored on such systems enforced by a court-ordered search warrant must be approved in writing by the University President or his/her designee
- Access to or possession of any information system or data stored on such systems by law enforcement will not be granted without a search warrant

All Campus Users

All campus members, including vendors, are expected to comply with all federal, state and local laws pertaining to the protection of confidential information as well as campus policies meant to protect the security of information systems on campus. The responsibility of each and every campus user includes, but is not limited to:

- Use secure passwords to access any campus computer used to access the campus network
- Keep computer monitor and desktop area clear of any hand written passwords
- Secure computer from unauthorized access when unattended
- Shred all discarded hard copies of confidential information

- Securely destroy all instances of files, digital or paper, containing identifying personal information (e.g. SSN, driver's license number, etc)
- Sign an access compliance form on the first day of employment or by start of first work day
- Use different passwords for campus accounts than your personal accounts

III. Security Principles

A. Physical Security

The principle of physical security is to restrict physical access to all computing systems, backup media, printed copies of confidential data, and network electronics and other network-related gear on campus.

1. All information systems containing confidential information shall be physically secured in a central computing center on campus such that access is limited to personnel authorized by the AVP ITS.
2. All data and telecommunication electronic devices used for the transmission of any data that may or may not be confidential in nature (e.g. routers, switches, wireless access points, etc.) shall be physically secured within a locked room or cabinet so that physical access to the device's power cord(s), network cable(s), buttons and/or switches is limited to personnel authorized by the AVP ITS.
3. Any media containing a full or partial backup of any information system containing confidential information such as tape backups may not be removed from its secure environment except for regularly scheduled pickup and delivery of tapes to the University's contracted off-site storage facility.
4. All public computers shall be physically secured so that the computer or its network resources (e.g. network jack) can not be used for unauthorized purposes.
5. Any printed hard copy of confidential data is discouraged and should be properly disposed of through a cross-cut shredder.

B. Access Security

The principle of access security is to limit access to data on all computing systems with the proper use of secure passwords. This should apply to all workstations, servers and other network devices to prevent unauthorized physical or remote access to any computing system on campus.

1. An authentication process that minimally includes manual input of a userid and password must be initiated prior to accessing any computer workstation on campus. All passwords must meet the University's guidelines for secure passwords.
2. Shared credentials for more than one person are strictly prohibited

3. Remote access to workstations for the use of shared access to information on the workstation (e.g. GoToMyPC, peer-to-peer networking, web server, ftp server, etc.) is prohibited.
4. Remote access to information systems for administrative use must be secured with a minimum of one set of authentication credentials and/or limited access to known computer hosts. Access to information systems for administrative use from a non-University network shall be secured through an encrypted session (e.g. VPN tunnel, etc.).

C. Data Security

The principle of data security is to preserve the integrity, privacy and confidentiality of information during the transmission from one computing system to another through the use of secure transmissions.

1. All transmission of confidential data from one computing system to another must utilize a secured transmission with a minimum of 128-bit encryption. Confidential data transmitted via email must be sent with a securely encrypted attachment.
2. Computing systems that duplicate in their entirety, or in part, data found on information systems containing confidential information whether or not information stored is considered to be confidential and provides access to more than one person, must be identified and registered as a shadow system with the ISO.
3. All access to information systems containing confidential information is prohibited from computing systems located on a non-University network without utilizing a secured transmission with a minimum of 128-bit encryption.

IV. Incident Response

A. An incident response plan is a formal set of procedures that allows the University to effectively and efficiently respond to an incident involving the identification of an information security compromise.
B. The University shall maintain a Computer Security Incident Response Team (CSIRT) in accordance with industry standards that will be the initial responders to a reported information security incident on campus.
C. Furthermore, the University shall develop a formal set of procedures for responding to information security incidences that model a 6 step process of handling incident responses. This 6 step model includes incident identification; incident reporting; containment of the incident; eradication of the incident; restoration of the system; and a follow up review process.
D. Any information security incident that results in the possibility of a breach of confidential information (Level I or Level II) shall be reported immediately to the ISO verbally and following, an email. The ISO shall report to the President's Cabinet for review to determine further action including but not limited to disciplinary action, policy analysis, and or public disclosure of

information compromised. (In accordance with the appropriate provisions of the applicable Education Code section and CBA, if any)

E. Any access to confidential information by local, state or federal law enforcement shall be preceded by the following:
    1. Subpoena delivered to the Vice President of Business Administrative Services or designee.
    2. Written acknowledgement by the University President or designee to disclose confidential information citing time of access; whom access is to be given to; how the access is to be obtained; what information and/or materials will be released to law enforcement.

V. Policy Review

This Policy shall be reviewed and updated annually or as necessary by the Information Security and Data Management committee under the direction of the campus ISO. Substantial changes to this policy will be communicated to the campus community through an email notification at the time of the change.

VI. Policy Awareness

A. This Policy shall establish a campus Information Security webpage to institute a central repository of information security notices, policies and best practices.
B. This Policy shall be distributed annually during any activities related to National Cyber Security Awareness Month in October to all campus faculty and staff via email and should direct them to the campus Information Security website for more information. New faculty and staff shall receive a copy of this Policy as part of Human Resource's new employee orientation material.
C. This Policy shall be distributed to any vendor performing work as a consultant or installer of any information technology related hardware or software that may operate on the campus network and/or access any computer system that resides on the campus network.

VII. Contacts

Questions about this policy or other campus Information Technology policies may be directed to the campus Information Security Officer.
Technical questions about information security may be directed to the campus Information Security webpage.
Information Security incidents may be reported to the campus Computer Security Information Response Team (CSIRT) via email Information Security.

Related Documents

Related Content:

CSUB ISO Page
Campus Acceptable Use Policy
ResNet Acceptable Use Policy
Confidentiality of Email Policy
Email Blocking Policy and Procedures
Information Practices Act (IPA)
Title V, California Code of Regulations (Sections 42396 - 42396.5)
HR 2003-05 Requirements for Protecting Confidential Employee Data
Privacy and Personal Information Management Student Records Administration - Executive Order No. 382
RunnerCard Policies
CSU Information Security Policy and Standards