CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

CSUB Data Access Policy

CSU Bakersfield Policy

Document Number: ITS-90.023
Last Revision Date: 8/31/2021
Responsible Office: Information Technology Services
Effective Date: 9/1/2021
Primary Author: CIO & AVP of Information Technology

General Description

Purpose:

With more of the campus data being stored and managed in the cloud we have to set standards to manage access to that data to protect it from loss or compromise.

Definition:

CSU Policy #8065.00 – The California State University system has a data classification document that outlines data classification and security requirements for systems that manage and maintain that data.

Level 1 Data (Confidential) - The highest level of data classification. This data includes privileged Personal Identifiable Information including banking account numbers, social Security numbers, health insurance records, and other sensitive information. This information requires the highest amount of protection.

Level 2 Data (Internal Use) - The second highest level of data classification. This data includes Personal Identifiable Information including birthdays student information like grades advising records or test scores, employee information like home address or marital status

Level 3 Data (General) - The lowest level of data classification. This data includes information that is typically publicly available like that you would find in a campus directory like email addresses or job titles. This information requires the least amount of protection.

State-Owned Device – A computer, tablet or mobile device owned by the campus and managed by the ITS department.

Personally Owned Device – A personal computer tablet or mobile device not owned by the state or managed by the campus ITS department.

Scope:

This policy applies to all CSUB departments, employees, and auxiliaries. For anyone who is accessing CSUB data from a cloud hosted or server-based application or data store.

Policy/Procedure

Access to any systems rated to manage or maintain any Level 1 or Level 2 data is restricted only to state owned devices. A personally owned device should not be used to access Level 1 or Level 2 Data.

An exception to this policy is granted to lectures who are not provided a state-owned device. They may access Level 2 Data (typically via Canvas) from a personally owned device. Those granted an exception should never download more then 500 records to that local device and are required to remove that locally stored data as soon as the data is no longer required no later then 3 weeks after the end of any term.

Additionally, it is strongly recommended that lectures accessing Level 2 Data from a personally owned device maintain proper security standards for their device including keeping current with OS and application updates / patches, using a good anti-virus application and utilizing strong passwords.

Anyone who's job requirements necessitate to work with Level 1 or Level 2 Data or more then 500 records will require assignment of a State-Owned Device.

Additional Information

The CSU data classification policy can be found here:
https://csyou.calstate.edu/groups/isac/isacstandards/default.aspx
If you have questions, please contact the CSUB Service Center at 661-654-HELP.

Review (Frequency and Process)

This policy should be reviewed and updated if needed on a biannual basics by the Information Security Officer (ISO) and/or the Chief Information Officer (CIO) or a designate and provided to the Vice President Business and Administrative Services for approval and then to Cabinet for final approval.