CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Electronic Media & Portable Devices

CSU Bakersfield Policy

Document Number:	ITS-90.009	**Last Revision Date:**	2/22/2021
Responsible Office:	Information Technology Services	**Effective Date:**	11/1/2009
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

Describes the use of electronic media at CSUB for the storage and transport of Level 1 and Level 2 data.

Definition:

Electronic media such as CD's, DVD's, Flash Drives, etc. shall not be used for the storage or transport of Level 1* confidential data, as defined by the CSU Information Security Asset Management Policy, unless the data are encrypted or biometric security is employed at the device level. See more information here.

https://calstate.policystat.com/policy/11773867/latest/#autoid-6vm89

Scope:

This policy applies to all CSUB employees.

Policy/Procedure

Electronic media such as CD's, DVD's, Flash Drives, etc. shall not be used for the storage or transport of Level 1* confidential data, as defined by the CSUB Information Security Policy, unless the data are encrypted or biometric security is employed at the device level. See more information here.

The use of portable devices such as laptops, PDA's, cell phones, etc. shall not be used for the storage or transport of Level 1* data unless the data are encrypted. The University Information Security Officer may, on a case-by-case basis, approve an alternative to encryption of data as a means to protect information assets. Such approval shall be made in writing.

- **Confidential Information (Level I)**

The following are considered Level I confidential information based on the significance of this information for the prevention of identity theft. Furthermore, as per the California Security Breach Information Act (SB 1386), any breach in the following information of any California resident that is unencrypted must be notified accordingly. SB 1386 defines a breach as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information."

-
    - Social Security Number paired with last and first name or first initial
    - Drivers license number or California identification card number paired with last and first name or first initial
    - Account 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.
    - Medical Information
    - Health insurance information
    - A username or email address in combination with a password or security question and answer that would permit access to an online account
    - Information or data collected through the use or operation of an automated license plate recognition system

- **Confidential Information (Level II)**

  The following Level II information should be "guarded" from access to unauthorized persons. This information is considered personal information and is regulated by various federal laws as well as CSU policy. Though this information does not require notification of breach, certain fines may apply if this information is mishandled. The guiding laws and policies for Level I information include FERPA, HIPAA, the Information Practices Act of 1977, California Public Record Act, and CSU policy HR 2003-05. All faculty and staff given access to the following information must complete and sign the CSUB Confidentiality Access and Compliance form. Student assistants given access to the following information must complete and sign the Banner Confidentiality Agreement.

  Students

  Any information in students' educational records that is not listed as non-confidential information.

  Faculty and Staff

    - Ethnicity
    - Gender
    - Home Address
    - Physical Description
    - Home telephone number
    - Medical history
    - Performance evaluations
    - ID card picture

Review (Frequency and Process)

This policy shall be reviewed every two years by the Chief Information Security Officer and provided to the Associate Vice President & CIO for approval.

Related Documents

Related Content:

CSU Information Security Policy and Standards