CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Instant Messaging Policy

CSU Bakersfield Policy

Document Number: ITS-90.013
Last Revision Date:
Responsible Office: Information Technology Services
Effective Date: 11/1/2009
Primary Author: CIO & AVP of Information Technology

General Description

Purpose:

This policy describes the classification of information that should not be transmitted through Instant Messaging software.

Scope:

This applies to all employees of the university.

Policy/Procedure

Reference: CSU System-Wide Information Security Policy, 11.4 - Information System Logs
Instant Messaging and other types of communication technologies shall not be used for communicating messages that would constitute official business records of the University, nor shall these types of technologies be used for transmitting Level 1* confidential data, as defined by the University Information Security Policy.

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

Related Documents

Related Content:

CSUB IM Policy