SAN JOSÉ STATE UNIVERSITY

# Standard: Email, Campus Communication & Cloud Services

November 9, 2021

## Executive Summary

The Email, Campus Communication and Cloud Services Standard outlines how SJSU's email and other forms of storage and electronic communication should be used by employees. This standard will help prevent the unauthorized access and loss of or destruction of sensitive campus information that is transmitted through email and other modes of communication while ensuring compliance with all applicable laws and regulations.

# Information Security Standards

## Email, Campus Communication & Cloud Services

| | | | | | |
|---|---|---|---|---|---|
| Standard # | IS-ECC | Effective Date | 5/30/2017 | Email | security@sjsu.edu |
| Version | 5.0 | Contact | Information Security Office | Phone | 408-924-1530 |

### Revision History

| Date | Action |
|---|---|
| **5/27/2014** | Draft sent to Mike |
| **12/1/2014** | Reviewed.  Content suggestions. Added comments. Hien Huynh |
| **3/7/15** | Review.  Content changes.  Prepared for publishing draft. Mike Cook |
| **5/15/2016** | Incorporated changes from campus constituents – Distributed to Campus. Mike Cook |
| **8/26/2016** | Incorporated revisions following discussion with Information Security Office and Academic Senate Chair.  Renamed.  Expanded to include additional Cloud Services.  Mike Cook |
| **9/1/2016** | Incorporated and/or “@mlml.calstate.edu and additional references.  Hien Huynh |
| **11/9/2021** | Review. Janice Lew |

## Table of Contents

# Introduction and Purpose

The Email, Campus Communication and Cloud Services Standard outlines how SJSU's email and other forms of storage and electronic communication should be used by employees. This standard will help prevent the unauthorized access and loss of or destruction of sensitive campus information that is transmitted through email and other modes of communication while ensuring compliance with all applicable laws and regulations.

# Scope

This standard applies to all University employees including employees of SJSU State, Self-Fund, and Auxiliary ("campus"). The information covered in this standard includes, but is not limited to information that is either transmitted or shared via electronic mail, instant messaging, video conferencing, or collaboration technologies.

# Background

The Family Educational Rights and Privacy Act (FERPA) requires that the University maintain control of all access to Personally Identifiable Student Data including Directory information such as student name, grades and contact information. For more information on FERPA, refer to the U.S. Department of Education "Family Educational Rights and Privacy Act (FERPA)" [1]. As such, all locations storing or transmitting sensitive electronic data, must have a legally binding contract in place with the University or its Auxiliaries guaranteeing confidentiality of the information and control over access. Additionally, the CSU Information Security Standards require strict control over protected University data including encryption, anti-malware, NIST Level 2 Password Complexity Requirements and other critical controls.

As such, it is against Federal Law and CSU Policy to utilize personal accounts, including email accounts, hosted by third party providers (i.e. Dropbox, Amazon, Microsoft Azure, Google, Hotmail, Comcast, Yahoo, GoDaddy, etc.) for the transmission or storage of University data which do not have a contract in place with San Jose State University or its Auxiliaries.

# Standard

## Electronic Mail Communication for Employees

### Employees must use University email address

All employees must use their "@sjsu.edu" and/or "@mlml.calstate.edu" email address(es) while conducting University business. University employees include Faculty, Staff, Administrators and Student Assistants of San Jose State University any of its Auxiliaries and Moss Landing Marine Labs. In order to maintain FERPA compliance, Employees shall not initiate communications with students via non-university email addresses nor shall they forward university communications to any personal address.

### Persons without a University email address

Any auxiliary or other person needing a "@sjsu.edu" email address should be entered into the appropriate system as a Person of Interest, by contacting Human Resources for more information.

### Addressing email to students

All employees must use their students' University email address(es) when initiating new email to students containing especially sensitive information such as financial transactions or student records including assignments, grades, and other information pertaining to the student's record.

In the event that a student forward email to a personal account, replies using a personal email account or otherwise authorizes in writing the usage of a personal account, the student has as such waived their FERPA rights and employees may reply using the student's preferred communication method.

## Electronic Mail Communication for Students

### Official University Communications will use SJSU address(es)

All official university communications will be delivered to employees and students at their "@sjsu.edu" and/or "@mlml.calstate.edu" email address(es). Official communications for enrolled students from Administration and the President will go to SJSU email addresses only. It is the students' responsibility to check or forward their email regularly and respond to official communications as necessary.

### Email forwarding

If the student wishes to use another address for campus communication, then they need to sign in and forward it to their other address.

## Electronic Mail Communications Security

### Electronic Mail Privacy

Electronic mail is considered by SJSU to be private information, and must therefore be handled as a private and direct communication between a sender and a recipient. Electronic mail is not to be accessed Administratively other than as specified in ICSUAM 8105.5.3[2]

### Electronic Marketing Material Source

All marketing materials sent through electronic mail must include an accurate return address and must provide clear and explicit instructions permitting recipients to quickly be removed from the distribution list.

### Electronic Marketing FERPA Compliance

All bulk mailing services used to communicate with students must hold a contract with the University and must be FERPA compliant. Departments shall not upload student email addresses to platforms which are not FERPA compliant (i.e. MailChimp).

### Electronic Mail Encryption

All sensitive information including, but not limited to, credit card numbers, passwords, medical information and research and development information must be encrypted when transmitted through electronic mail. Currently this option is not available in the 3rd party email system. All sensitive data must be encrypted prior to uploading as an attachment in email and must not be contained in the message body.

## Cloud Services and Instant Messaging

### Cloud Service Compliance

Employees must not store or transmit protected University data using personal accounts, hosted by third party providers (i.e. Dropbox, Amazon, Microsoft Azure, Google, Hotmail, Comcast, Yahoo, GoDaddy, etc.) which do not have a contract in place with San Jose State University or its Auxiliaries.

### Transmission of sensitive information using IM

IM should not be used for communication of sensitive level 1 or level 2 confidential information, including information contained in files, unless encrypted or explicitly authorized. For more information on data classification, refer to the SJSU "Security Standard for Information Classification and Handling" [3].

Unless explicitly authorized by the Information Security Office, Level 2 data may be transmitted via Instant Message using either SJSU Google Hangouts or SJSU Cisco Jabber.

Level 1 data may only be transmitted via Instant Message using SJSU Cisco Jabber.

## More Information

[1] U.S. Department of Education: "Family Educational Rights and Privacy Act (FERPA)"

[2] California State University: "Responsible Use Policy - ICSUAM8105"

[3] San Jose State University: "Security Standard for Information Classification and Handling"