Standard: Email and Campus Communication

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-ECCS		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

Executive Summary

The Email and Campus Communication standard defines the requirements for how Stanislaus State's email and other forms of electronic communication should be used for employees and students. This standard of due care will help prevent the unauthorized loss of or destruction of sensitive campus information that is transmitted through email and other modes of communication. Workers must restrict their electronic communications to business matters.

Introduction and Purpose

The Email and Campus Communication standard defines the requirements for how Stanislaus State email and other forms of electronic communication should be used for employees and students. This standard of due care will help prevent the unauthorized loss of or destruction of sensitive campus information that is transmitted through email and other modes of communication.

Scope

This standard applies to all Stanislaus State, Self-Funded, and Auxiliary ("campus") email users with a "@csustan.edu" email address. 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.

Standard

Compliance to Email Standards

Email Retention Standard

Specific requirements for the storage and deletion of email is specified in the Email Retention Standard. For more information, refer to the Stanislaus State "Email Retention Standard" [1].

Electronic Mail Communication for Employees

Employees Must Use University Email Address

Any university employee must use their "@csustan.edu" email address while conducting university business. University employees include faculty, staff, and administration. In order to maintain FERPA compliance, faculty shall not communicate with students via non university email addresses nor shall they auto-forward university communications to a personal email address.

People without University Email Address

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

Refusal to Service Non Stanislaus State Addresses

Office of Information Technology (OIT) may refuse to service customers using non "@csustan.edu" email addresses.

Faculty and Staff Sending Email to Students

All faculty and staff must use the student's "@csustan.edu" email address when sending email to students, especially sensitive information such as financial transactions or student records including assignments, grades, and other information pertaining to the student's record.

Electronic Mail Communication for Students

Official University Communications will use Stanislaus State Address

All official university communications will be delivered to employees and students at their "@csustan.edu" email address. Official communications from administration and the president will go to Stanislaus State email addresses only. It is the recipient's responsibility to check 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.

Responsibility for Lost and Deleted Emails

Users are responsible for any lost and deleted emails, including their email retention settings. Users are responsible for deleting old messages that are no longer needed. It is important to understand that when the user's mailbox is full, it might automatically delete previous messages in order to accept new ones. Office of Information Technology (OIT) does not have the ability to restore messages that have been deleted.

Retention of Important University Documents

Email should not be the sole mechanism for retaining important university documents. Users are encouraged to extract any important attachments from their email onto network drives on a regular basis for safe keeping.

Electronic Mail Communications Security

Information involved in electronic messaging should be appropriately protected.

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.

Inappropriate Electronic Mail Messages

Workers must not create and send, or even forward, any externally-provided electronic mail messages that may be considered to be harassing in nature, or that may contribute to the perception of a hostile work environment.

Electronic Mail Privacy

Electronic mail is considered by Stanislaus State to be private information, and must therefore be handled as a private and direct communication between a sender and a recipient with a limited expectation of privacy.

Electronic Mail Encryption

All sensitive information including, but not limited to, credit card numbers, passwords, 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.

Electronic Mail Message Monitoring Approval

Email administrators must only access another user's account in strict compliance with ICSUAM-8105.

Electronic Mail Modification

Workers must not modify, forge, or remove any information appearing anywhere in an electronic mail message including the body of the message or the header.

Centralized Control over Electronic Mail Systems

Centralized control over both inbound and outbound electronic mail will be provided by the Office of Information Technology. All Stanislaus State electronic mail must flow through systems established, operated, and maintained by that same department. All on-campus systems which send email externally must do so through an SMTP relay server controlled by OIT.

Bulk Electronic Mail

Workers must not use Stanislaus State computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients.

All Campus, All Students, All Staff Emails

Emails to complete campus constituent groups shall be sent only with OIT approval.

Sending Unsolicited Electronic Mail

Users must not send uninvited or unsolicited electronic mail (also known as spam) to a large number of recipients.

Distributing Stanislaus State Information via Blogs

Workers must not publish or otherwise communicate any Stanislaus State internal information on the Internet, or in any other public forum, unless this public disclosure has first been approved by University Advancement. Such publishing includes, but is not limited to, weblogs (blogs), Internet discussion groups, social networks, and personal web pages. Further guidance about what information may be publicly released can be found in the Information Classification Policy.

Electronic Mail Attachments

Workers must not open electronic mail attachments unless they were expected from a known and trusted sender, and these attachments have been scanned by an approved anti-virus software package.

Unexpected Electronic Mail Attachments

Users who receive an unexpected attachment to an electronic mail message that does not have a credible business-related explanation must not open the attachment until they obtain a believable explanation from the sender.

Responding to Spam Messages

To keep spam to a minimum, users must refrain from responding in any way to spam and must not purchase anything advertised in spam.

Instant Messaging (IM)

Transmission of Sensitive Information using IM

IM should not be used for communication of sensitive level 1 or level 2 confidential information, including confidential information contained in files. For more information on data classification, refer to the Stanislaus State “Security Standard for Information Classification and Handling” [2].

Capture and Transmission of Sensitive Information

Campus users shall not use a camera to capture, save, transmit or otherwise share level 1 or level 2 data.

Telepresence Video Conferencing

Approved Telepresence Video Conferencing Application

Campus users and students must use the official approved Telepresence vendor and applications for campus communication.

Web Conferencing

Approved Web Conferencing Application

Campus users and students must use the official approved web conferencing solution application for campus communication.

More Information

[1] Stanislaus State: “Email Retention”

[2] Stanislaus State: “Security Standard for Information Classification and Handling”