Standard: Email Retention

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-ERS		strevena@csustan.edu	0.9	Stan Trevena	209.667.3137

Executive Summary

The Email Retention Standard defines the requirements for retention of Stanislaus State email, including the deletion and archiving of electronic mail. This standard is intended to help campus employees and students determine what information sent or received via email should be retained and for how long. This standard of due care will help prevent the unauthorized loss of or destruction of sensitive campus information, as well as ensure that the university is compliant with any litigation or eDiscovery requirements.

Introduction and Purpose

The Email Retention standard defines the requirements for retention of Stanislaus State email, including the deletion and archiving of electronic mail. This standard is intended to help campus employees and students determine what information sent or received via email should be retained and for how long. This standard of due care will help prevent the unauthorized loss of or destruction of sensitive campus information, as well as ensure that the university is compliant with any litigation or eDiscovery requirements.

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 stored or shared via electronic mail or instant messaging technologies.

Standard

All information stored in electronic mail format shall follow record retention schedules as established by the California State University Chancellor's Office. http://www.calstate.edu/recordsretention/ Email account owners are responsible for monitoring their email for any applicable material and taking the appropriate action to adequately follow the published retention schedules. Email is a communication mechanism and is not to be relied upon for the long-term archival or storage of sensitive university data.

Deletion and Archiving of Email

Retention Period for Deletion of Email

Campus users should regularly empty their email deleted items folder, as email that is left in this folder can exceed retention periods without the user's knowledge. Messages contained in a deleted items folder which has been "emptied" are irretrievable.

Storage of Sensitive Information in Email

Storing sensitive attachments in Stanislaus State campus email permanently is prohibited. For more information on the types of information that can be transmitted or stored and their respective classification, refer to the "Information Classification and Handling Standard" [1] and "Cheat Sheet: Information Classification and Handling" [2].

Level 1 Health Insurance Portability and Accountability Act (HIPAA) Information Prohibited

Users are prohibited from transmitting, storing or archiving sensitive HIPAA emails and attachments in any email system. For more information on HIPAA requirements, refer to the Stanislaus State "HIPAA Summary" [3].

Level 1 Payment Card Industry (PCI) Information Prohibited

Users are prohibited from transmitting or storing sensitive PCI data including credit card numbers in any email system. For more information on PCI requirements, refer to the Stanislaus State "PCI Summary" [5].

Storing Sensitive Attachments Received Through Email

Users must not use the email system to permanently store or archive any attachments including sensitive Level 1 or Level 2 information. Instead, users should save the sensitive attachments to their hard drive and apply the required encryption application, where applicable, within one month of receiving the sensitive information. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files on their hard drive.

Storing Sensitive Attachments Received Through Instant Messaging

Users must not use Instant Messaging applications to permanently store sensitive Level 1 or Level 2 information. These attachments should be regularly moved to the hard drive and apply the required encryption application.

Email and Campus Communication

For more information on the usage of email and other forms of campus communication, refer to the "Email and Campus Communication Standard" [4].

More Information

[1] Stanislaus State: "Security Standard for Information Classification and Handling"

[2] Stanislaus State: "Cheat Sheet: Information Classification and Handling"

[3] Stanislaus State: "HIPAA Summary"

[4] Stanislaus State: "Email and Campus Communication Standard"

[5] Stanislaus State: "PCI Summary"