Information Security Standards					
Email Retention					
Standard #	IS-ER	Effective Date	TBD	Email	security@sjsu.edu
Version	2.0	Contact	Mike Cook	Phone	408-924-1705

Standard: Email Retention

Executive Summary

The Email Retention Standard defines the requirements for retention of SJSU 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.

Revision History

Date	Action
5/27/2014	Draft sent to Mike
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh

Table of Contents

Introduction and Purpose

The Email Retention standard defines the requirements for retention of SJSU 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 SJSU State, Self-Fund, and Auxiliary ("campus") email users with a "sjsu.edu" or "mlml.calstate.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

The retention period for electronic mail in your trash can is controlled by the 3rd party email provider and is subject to change. Messages contained in a trash folder which has been "emptied" are irretrievable.

Storage of Sensitive Information in Email

Storing sensitive attachments in SJSU 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 SJSU "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 SJSJU "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] San Jose State University: "Security Standard for Information Classification and Handling"

[2] San Jose State University: "Cheat Sheet: Information Classification and Handling"

[3] San Jose State University: "HIPAA Summary"

[4] San Jose State University: "Email and Campus Communication Standard"

[5] San Jose State University: "PCI Summary"