CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Standard for Recalling Communications
CSUSB Information Technology Services

Last Revised: **03/12/2020**

Final

REVISION CONTROL

Document Title: CSUSB Standard for Recalling Communications

Author: James Macdonell & Laura Carrizales

Date	By	Action	Pages
8/29/2019	Macdonell & Carrizales	Created Standard	All
10/10/2019	Au	Revised based on sub-committee suggestions	All
02/17/2020	Au	Revised based on sub-committee suggestions	All
03/09/2020	Carrizales & Au	Revised based on ITGEC suggestions	All
3/12/2020	Au	Reviewed and approved by ISET Subcommittee	New Additions

Review/Approval History

Date	By	Action	Pages
3/12/2020	ISET Subcommittee	Approved Standard	All

Table of Contents

1.0 Introduction

In general, once a communication is sent, it cannot be recalled. A recipient will have the ability to read, print, screenshot or otherwise reproduce the information moments after it was sent. It is impossible to "unring the bell." The CSUSB Acceptable Use Policy states that “any individual using CSU, San Bernardino's computer communications systems is responsible for the material s/he sends or displays via the campus computing/communications resources” and “the University reserves the right, without notice, to limit or restrict any individual's use of any computing and communications facility or resource, and to inspect, copy, remove or otherwise alter only the data, file, or system resource which may undermine security, integrity or the effective operation”[1]

In limited situations, CSUSB has the technical capability to remove or destroy communications within the CSUSB email systems. This is intended to be used to minimize the impact of a security incident such as phishing, a virus or unauthorized disclosure of sensitive information.

It is not intended for situations where a sender makes typographical errors, makes spelling mistakes, sends a draft prematurely, or regrets other embarrassments in their communication. This is not something that should be considered as a remedy for miscommunications. This capability is also not intended to be used in a way that could reasonably be considered censorship.

2.0 Scope

When a communication poses a significant and ongoing security or financial threat to the university CSUSB will consider recalling the message if it is reasonably and technically feasible to do so.

Action Taken:

Situations where CSUSB will consider attempting to remove or destroy a communication:

Verified imposter: A verified unauthorized communication made to appear to come from a campus authority.
Example: An impersonated manager asking employees to buy gift cards.

Verified phishing attempt: A verified unauthorized communication that poses security risks to the campus.
Example: A malicious email that contains a link to an unauthorized website intended to harvest passwords or other credentials.

Malicious software: Software that causes harm to computers and networks, such as viruses, trojans, viruses, spyware, etc.
Example: An email attachment that contains a verified virus or a verified malicious link that could infect a large number of computers or compromise the campus network.

[1] https://www.csusb.edu/policies/acceptable-use-policy-electronic-communications

Personal Identifiable Information (PII): A communication that contains sensitive information, particularly level 1 information that was sent to an unauthorized party.
Example: An office that sent a spreadsheet containing employee SSN to a group that is not already authorized to view or receive such information.

Fraud: A situation in which an individual makes an endorsement that appears to represent the university.
Example: Someone claiming to be a representative of CalPERS, but is actually a 3rd party not endorsed by the State of California.

Highly Sensitive: A communication that contains highly sensitive information that is sent to a broad unauthorized audience. *Example: An email that contains a list of passwords to systems was sent to a group that was not authorized to receive such information.*

3.0 Out of Scope

CSUSB will not attempt to remove or destroy a communication in situations where the communication does not pose an ongoing security or financial threat to the university.

Situations where CSUSB will not attempt to remove or destroy a communication:

These may include messages that violate the Acceptable Use Policy, CSU/CSUSB Policy, Federal and State Laws: For example: Bullying, defamation, slander, litigation holds, advertising personal business, etc. provided the communication does not pose an ongoing security or financial threat.

Examples may include:

- **Poorly formatted communication**
  Example: A message that was sent with a missing attachment or distorted images.
- **Poorly edited communication**
  Example; misspellings, grammatical mistakes, or copy/paste errors, incomplete messages sent prematurely.
- **Technical or human errors in communication**
  Example: Message states verbatim "Dear {FirstName}", missing attachment, message was sent from incorrect account.
- **Sent to wrong listserve**
  Example: A message intended to be sent to FORUM and was sent to CAMPUS.
- **Political endorsements**
  Example: An email stating to vote for or against a ballot measure or candidate.
- **Items contributing to a hostile work environment**
  Example: A cartoon that is biased against gender or race.

Recommended, alternative strategies for handling miscommunication:

Reply with a follow up communication containing the corrections. For example, “The date is actually Monday instead of Tuesday”.

For a supervisor or department to send an apology communication explaining intent or the corrective actions that are taking place to prevent a miscommunication from happening in the future.

Revoke or modify permissions to “send as”, “send on behalf of” or “send to” certain destinations that support such restrictions.