Standard: Computer Crime and Privacy Laws

Executive Summary

According to ISAC2 2014, “a computer crime is any illegal action where the data on a computer is accessed without permission. This includes unauthorized access or alteration of data, or unlawful use of computers and services”. Therefore it is important for SJSU to adhere to proper privacy laws and regulations. The overall protection of the data assets must begin with the individual who has access to them. This standard defines the computer crimes and federal and state privacy laws relevant to SJSU. The purpose of this standard is to provide education and awareness to faculty and students on the types of laws (statutory, regulatory, and federal) that the University must follow.

Information Security Standards

Computer Crime and Privacy Laws

Standard #	IS-CCPL	Effective Date	11/10/15	Email	security@sjsu.edu
Version	3.1	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
5/28/2014	Draft sent to Mike
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/19/2021	Reviewed. Cole Gunter
11/30/2022	Reviewed. Cole Gunter

Table of Contents

Introduction and Purpose

This standard defines the computer crimes and federal and state privacy laws relevant to SJSU. The purpose of this standard is to provide education and awareness to faculty and students on the types of laws (statutory, regulatory, and federal) that the University must follow.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

Standard

Identification of applicable legislation

All relevant statutory and regulatory requirements and the university's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.

Laws, Regulations and Contractual Requirements

For every SJSU production information system, all relevant statutory, regulatory, and contractual requirements must be thoroughly researched, explicitly defined, and included in current system documentation.

Periodic Monitoring of Privacy Laws

SJSU must monitor all data privacy laws applicable to the University, for changes that will impact the privacy program and the corresponding written data privacy policies. This monitoring must occur on a quarterly basis.

Privacy Laws and Regulations

Disclosure of Protected Information

Additional laws and regulations specify the disclosure of employee and student information and require the University to take specific actions in the event SJSU suspects protected information may have been disclosed either accidentally or maliciously to unauthorized parties.

Notification and Lines of Communication

Individuals who handle protected information for the University are encouraged to speak with their managers, Information Authorities, or the Information Security Officer to familiarize themselves with relevant laws and regulations.

Reference to Computer Crime and Privacy Laws

For more information on the Computer Crime and Privacy Laws that the University must adhere to, refer to the SJSU "Cheat Sheet: Computer Crime and Privacy Laws" [1].

More Information

[1] San Jose State University: “Cheat Sheet: Computer Crime and Privacy Laws”. <INSERT INTERNAL LINK TO STANDARD>