Standard: Information Security Incident Management

Contents

Revision History

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

Executive Summary

California State University Information Security Policy 8075.00 states security incidents involving loss, damage or misuse of information assets or improper dissemination of protected data, regardless of medium, must be properly reported and investigated to mitigate adverse impacts, protect the university from similar incidents, and comply with existing policies and laws. Information Security Incident Management standard defines the requirements for managing information security incidents for all Stanislaus State computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by Stanislaus State. In addition, it provides strategy such as investigating, developing, reporting, implementation, and successful recovery for the proper channels and team within Stanislaus State to address and manage issues of crisis that affect the organization in a timely manner. The core of incident management is about proactively preparing for, reactively responding to, and lessons learned from an incident.

Introduction and Purpose

This standard defines the requirements for managing Information Security Incidents for all Stanislaus State computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by Stanislaus State.

Scope

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

Standard

Reporting Information Security Events

Campus Information security events should be reported through appropriate management channels as quickly as possible.

Loss or Disclosure of Sensitive Information

If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Officer must be notified immediately.

Disclosure of Information System Vulnerabilities

Specific information about information system vulnerabilities, such as the details of a recent system break-in, must not be distributed to persons who do not have a demonstrable need to know. All discussions, actions, and information surrounding the incident are to be treated as confidential.

Public Releases of Vulnerability Information

Press releases or other public statements issued by Stanislaus State containing information systems vulnerability information must be free of explicit details. Public releases may only be made by the Communications and Public Affairs Department.

System Vulnerability Exploitation and Victim Data

Stanislaus State staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly.

Production System Problems

All significant errors, incomplete processing and improper processing of production applications must be promptly reported to the OIT Help Desk.

Information Security Pranks

Employees must not play practical jokes, engage in pranks, or otherwise humorously make it look like a security incident is taking place, will take place, or has taken place when this is not true.

Offensive Electronic Mail Messages

Employees are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, employees must report the communications to their manager and the Human Resources Department.

Off-Site Systems Damage and Loss

Employees must promptly report to their manager any damage to or loss of Stanislaus State computer hardware, software, or information that has been entrusted to their care. Lost machines must be reported to the Information Security Officer and the appropriate property forms completed. Stolen machines must be reported to University Police in addition to all procedures required for lost computers. A police report must be filed for all stolen computer devices (smartphones, tablets, laptops, computers or other devices capable of storing information).

Incident Reporting

All suspected information security incidents must be reported as quickly as possible through the approved Stanislaus State internal channels.

Violation and Problem Reporting

Stanislaus State employees have a duty to report all information security violations and problems to the Information Security Officer on a timely basis so that prompt remedial action may be taken.

Violation and Problem Reporting Alternatives

Stanislaus State employees must immediately report all suspected information security problems, vulnerabilities, and incidents to either their immediate manager or to the Information Security Officer.

Violation and Problem Reporting Interference

Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited and cause for disciplinary action.

Violation and Problem Reporting Identity

Employees who report to the Information Security Officer a security problem, vulnerability, or an unethical condition within Stanislaus State may, at their sole discretion, have their identity held in strict confidence. This means that the whistleblower's immediate supervisor, other members of the management team, as well as other Stanislaus State employees who are not directly involved in the receipt of the report, will not be given the whistleblower's identity.

Reporting Security Breaches to Third Parties

If an information systems security breach at Stanislaus State causes private or proprietary third party information to be exposed, then these same third parties must be notified immediately so that they can take appropriate action.

Reporting Suspected Security Breaches To Third Parties

If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

Initial Response to Report of Identity Theft

If a customer reports a case of suspected identity theft, Stanislaus State staff must immediately put a hold on all accounts controlled by that individual. A suspected fraud notice must be placed on all accounts involved, and every transaction flowing through these accounts immediately thereafter must be verified with the rightful account holder before they are processed. The involved accounts must be closed as soon as possible, and a notice about the problem must be inserted in all new accounts established for that same customer.

Reporting Unauthorized Activity

Users of Stanislaus State information systems must immediately report to the Information Security Officer any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported to the same manager.

Reporting Questionable Events

All unusual and suspicious information-security-related events must be promptly reported to the Information Security Officer. These events include unusual requests for Stanislaus State information coming from an external party, as well as previously un-encountered system behavior.

Reporting Unexpected Requests for Log-In Information

Other than the regular and expected Stanislaus State log-in screens, users must be suspicious of all pop- up windows, web sites, instant messages, and other requests for a Stanislaus State user ID and password. Users encountering these requests must refrain from providing their Stanislaus State user ID and password, as well as promptly report the circumstances to the OIT Help Desk.

Reporting Design Problems

All potentially serious problems associated with information systems being designed or developed, that are not being adequately addressed by planned or existing projects, must be promptly reported to Information Security Officer.

Contacting Law Enforcement

Employees must contact University Police immediately if an unlawful activity has taken place or any involved party feels physically threatened in any way.

Computer Crime Investigation

Whenever evidence clearly shows that Stanislaus State has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Missing Access Devices

Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to University Police and Facilities Services immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen—or are suspected of being lost or stolen--must be reported to the Information Security Officer immediately.

Reporting Unintended Sensitive Information Disclosures

Unintended disclosures of sensitive Stanislaus State information are serious matters, and they must all be immediately reported to both the Campus Compliance Officer and the Information Security Officer. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

Reporting security weaknesses

Category Description: All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services to the Information Security Officer.

Centralized Problem Reporting

All known vulnerabilities -- in addition to all suspected or known violations -- must be communicated in an expeditious and confidential manner to the Information Security Officer. Unauthorized disclosures of Stanislaus State information must additionally be reported to the involved information owners. Reporting security violations, problems, or vulnerabilities to any party outside Stanislaus State (except external auditors) without the prior written approval of the Campus Compliance Officer is strictly prohibited.

Reporting System Vulnerabilities

Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the OIT Help Desk. Users are prohibited from utilizing Stanislaus State systems to forward such information to other users, whether the other users are internal or external to Stanislaus State.

Security Weaknesses and Vulnerability Discussion

Employees who discover a weakness or vulnerability in the information security measures used by Stanislaus State must not discuss these matters with anyone other than Information Security Officer, or trained investigators designated by the Information Security Officer.

Vulnerability Disclosure

If a serious information system vulnerability is discovered by Stanislaus State employees, and the vulnerability can be directly traced to a weakness in a certain vendor's hardware and/or software, then that vendor must promptly and confidentially be notified of the problem. Stanislaus State employees must give the vendor a reasonable period of time to fix the problem before they publicly release any information about that same problem.

Reporting a Suspected Virus or Malware

Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, if employees report a computer virus infestation to the Information Security Officer immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action will be taken. The only exception to this early reporting amnesty will be those circumstances where a worker knowingly caused a computer virus to be introduced into Stanislaus State systems. However, if a report of a known infestation is not promptly made, and if an investigation reveals that certain employees were aware of the infestation, these employees will be subject to disciplinary action including termination.

Reporting of Software Malfunctions

All apparent software malfunctions must be immediately reported to line management or the information system service provider.

Management of Incident Response and Improvements

The Information Security Officer will implement, manage, and improve a Computer Security Incident Response Team (CSIRT) as detailed in the Security Action Plan, for handling information security events. Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.

Responsibilities for Information Security Incident Response (IR)

The Information Security Officer will develop and manage an Incident Response team as detailed in the university security action plan, and any other stakeholders the team identifies as relevant to the case. The Incident Response Team shall handle any security abuse incidents.

Designated Contact Person for All Disasters and Security Events

Unless expressly recognized as an authorized spokesperson for Stanislaus State, no worker may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

Computer Incident Response Plans

For computer and communications systems, management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical systems in the event of an interruption or degradation of service.

Computer Incident Response Team

OIT must organize and maintain an internal Information Security Management Team that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins.

Suspected System Intrusions

Whenever a system is suspected of compromise, the involved computer must be immediately taken offline, and predetermined procedures followed to ensure that the system is free of compromise before bringing it back online on the network(s).

Information Security Alert System

The Information Security Officer management must establish, maintain, and periodically test a communications system permitting employees to promptly notify appropriate staff about suspected information security problems.

Unauthorized Access Problems

Whenever unauthorized system access is suspected or known to be occurring, Stanislaus State personnel must take immediate action to terminate the access or request assistance from the OIT Help Desk.

Messages to Attackers

A cease and desist message must be sent to the source of all attacks mounted against Stanislaus State computers or networks whenever the source or intermediate relay points can be identified.

Information Security Problem Resolution

All information security problems must be handled with the involvement and cooperation of in- house information security staff, the OIT Information Security Management Team, or others who have been authorized by the Stanislaus State Information Security Officer.

Incident Management Responsibilities

The individuals responsible for handling information systems security incidents must be clearly defined by the Information Security Officer. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents. Currently these individuals include the Chief Information Officer and Information Security Officer.

Privacy Breach Response Team

Stanislaus State must establish and staff a special team with the responsibility of planning for, analyzing and responding to data breaches that may involve sensitive customer data.

Privacy Breach Notification Contents

Stanislaus State must provide a detailed explanation of any breach of private customer data as part of the standard notification process. The notification content must be reviewed and approved by both the Legal Department and the Information Security Officer.

Privacy Breach Record of Notification

Stanislaus State must keep a record of each customer notification attempt, including the name of the individual, date, time and notification method.

Privacy Breach Media Notice for HIPAA Violations

If the number of individuals affected by a HIPAA privacy breach incident is over 500 individuals within a given state or jurisdiction, then notice of the breach must be disclosed to prominent media.

Privacy Breach Notice for Level 1 Violations

Level 1 data violations must be reported by the Information Security Officer to the system-wide Chief Information Security Officer and to the Chief Information Officer. The Chief Information Officer shall notify the Vice President of Business and Finance. The Vice President of Business and Finance must notify the campus President.

Privacy Event Notification Analysis

Each security event identified as a possible privacy breach must be further analyzed to determine the notification requirements for the breach. Breaches that trigger the notification requirements must be logged and reporting immediately to the OIT Information Security Management Team.

Privacy Breach Notice - Web Site Posting

Stanislaus State must post notice of any privacy breach on the public web site, including details of the breach approved for public disclosure as required by law for confidential Level 1 security breaches.

Learning From Information Security Incidents

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Violation and Problem Analysis

An annual analysis of reported information security problems and violations must be prepared by the Information Security Officer and presented to the University President.

Collection of Evidence

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Computer Crime or Abuse Evidence

To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The relevant information must then be securely stored off-line until official custody is given to another authorized person or the chief legal counsel determines that Stanislaus State will no longer need the information. The information to be immediately collected includes the current system configuration as well as backup copies of all potentially involved files.

Sources of Digital Evidence

For every production computer system, the Information Security Officer must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subject a standardized capture, retention, and destruction process comparable to that used for vital records.

Disclosure of Information to Law Enforcement or Third Parties

By making use of Stanislaus State systems, users consent to allow all information they store on Stanislaus State systems to be divulged to law enforcement at the discretion of Stanislaus State management. Information is also subject to discovery as specified by the Public Records Act.

Performance Monitoring Information

Management must not use computers to automatically collect information about the performance of employees unless the involved employees have collectively agreed that such information realistically reflects their job-related performance.

Internal Investigations Information Confidentiality

Until investigations are complete and disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Law Enforcement Inquiries

Even if the requesting party alleges to be a member of the law enforcement community, Stanislaus State employees must not reveal any internal Stanislaus State information through any communications mechanism unless they have established the authenticity of the individual's identity and the legitimacy of the inquiry. Any release of protected information shall be authorized by the Campus Compliance Officer.

Legal Proceeding Participation

Any Stanislaus State worker called by a subpoena or in any other manner called to appear or testify before a judicial board or government agency on the behalf of the University must notify the Campus Compliance Officer.

Providing Information in Legal Proceedings

Employees are prohibited from providing any Stanislaus State records, or any copies thereof, to third parties outside of Stanislaus State or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the Campus Compliance Officer has first been obtained. Likewise,

employees are prohibited from testifying to facts coming to their knowledge while performing in their official Stanislaus State capacities, unless the prior permission of the Campus Compliance Office has first been obtained.

Investigation Status Reports

The status of information security investigations must be communicated to management only by the lead investigator or the management representative of the investigation team.

Computer Crime Investigation Information

All evidence, ideas, and hypotheses about computer crimes experienced by Stanislaus State, including possible attack methods and perpetrator intentions, must be communicated to the Campus Compliance Officer and treated as restricted and legally privileged information.

Forensic Analysis Process

Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

Information Security Investigations

All Stanislaus State internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Officer.

Internal Investigations and Official Inquiries

All Stanislaus State employees must testify or otherwise respond to questions associated with internal investigations when directed to do so by the Campus Compliance Officer. Under certain circumstances, this testimony or response must be provided while under oath.

Intrusion Investigations Details

Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of intruders, files which describe an investigation now underway must not be stored on potentially compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

Single Person Responsible for Electronic Evidence Production

Stanislaus State will appoint a single individual responsible for coordinating the discovery and presentation of electronic evidence that may be required to support litigation or to fulfill the obligations of the Public Records Act.

Special Data Classification for Possible Electronic Evidence

Stanislaus State data that may be considered electronic evidence must have a specific data classification. An electronic evidence handling policy, published jointly by the Information Security Officer and the legal department, will outline the controls required to protect this special class of data.