San Francisco State University
Information Technology Services (ITS)

Incident Management – Roles and Responsibilities

Description

An information security *incident* is an event that violates SF State information security policy in such a way that it has the potential to seriously compromise the confidentiality, integrity or availability of SF State information technology assets.

Incident management is a structured approach to handling information security events in a manner that both limits their negative impact and helps to prevent them from arising in the future.

This document outlines the specific responsibilities of the San Francisco State University community related to incident management, with an emphasis on the responsibilities of functional campus areas.

Roles

End Users
This sections defines the responsibilities of individuals reporting a security incident.

Functional Campus Area
This section defines the responsibilities of the frontline responders designated as the Point of Contact.

Management
This section defines the responsibilities of administrators who supervise IT Support.

End Users

The incident response cycle begins when a suspicious event is observed. In this sense end users are a valuable source of data. Security incidents are considered high priority and take precedence over normal university operations. Individuals in functional campus areas must either contact their local IT service desk or (in their absence) communicate with the central ITS service desk directly to begin the process of handling the incident immediately. Depending on the nature of an incident (e.g. theft) the end user may also need to contact law enforcement and file a report.

End users are expected to provide as much detail as possible about the incidents that they observe, as well as to preserve related evidence, and to make themselves available to offer assistance as the incident response progresses. End users must offer reliable contact information to their initial Point of Contact (POC) in the event that they are away from campus when phoned.

Functional Campus Areas

Functional campus areas consist of those university employees who normally deploy, manage, and maintain the information systems which are suspected of being compromised. The initial POC is a member of the corresponding functional campus area.

Containment
When a potential information security incident has been identified, the first thing the POC should do is to ensure that a compromised system has been taken off the network and is quarantined in a physically secure area. This will discourage property loss, prevent malware from receiving command and control messages, safeguard against additional data exfiltration, and protect against tampering with evidence.

Initial Assessment
Once containment has been achieved the POC should contact the ITS Security Team. The primary documents involved in an incident response are:

- The incident response Report Form
- A corresponding service desk ticket

Not all incidents require a completed incident response Report Form. Isolated low impact events that do not put protected (Level 1 or Level 2) data at risk generally can be handled without using the Form. Such incidents can be addressed internally. Though for the sake of maintaining university-wide statistics the POC needs to submit an incident ticket with the relevant details and mark the entry as "resolved."

If protected data may have been put at risk, functional campus areas are expected to perform an "Initial Assessment" immediately. This means interviewing the end user about the incident as well as collecting and securing additional relevant evidence as needed. The goal of this phase is to:

- Screen out false positives
- Prepare to notify the appropriate authorities in case of a genuine breach
- Establish a foundation for escalation if needed

Preliminary information should be conveyed by opening a service desk ticket (e.g. https://sfsu.service-now.com/). The Subject field should begin with the phrase "INFOSEC Incident" followed by the name of the user and a brief synopsis of the incident.

Response Time
Keep in mind that the underwriter for SF State's cyber insurance policy requires that incidents be formally disclosed within a relatively short time frame. But while speed is important it's also crucial that the POC provides a chronological narrative that's as complete as possible. A handful of carefully posed, context sensitive, queries can easily replace several days of otherwise unnecessary digging.

Hence, the POC should strive to answer pertinent information with respect to who, what, when, where, why, and how. The POC is in a unique position to do so because (as a unit-level liaison) they typically have immediate access to compromised assets and tighter links with departmental personnel.

Additional Details
After containing the impacted system, the POC should complete the "In-Depth Synopsis" section of the Report Form and attach the completed Incident Response form to the service desk ticket. The POC should make themselves available answer any additional queries that may arise and to assist as needed over the course of the incident response.

Management

Per the Integrated CSU Administrative Manual (ICSUAM) Sections 8015.S000 and 8075.00 campus management is responsible for ensuring that the information assets under their control are managed in compliance with CSU and SF State information security policies.

As stated earlier, security incidents are considered high priority and take precedence over normal SF State business operations. Managers who supervise functional campus areas must be prepared to manage work priorities applying judgment to the scope, impact, and urgency in accordance with direction provided by the SF State Information Security Officer.

In the event of a data breach involving Level 1 or Level 2 data, functional campus areas must also be prepared to coordinate with the SF State Information Security Officer with regard to the process of communication.

Finally, management must ensure that lessons learned from an information security incident are understood by the staff under their supervision as well as to assist the SF State Information Security Officer to address vulnerabilities identified as the result of an incident.

Revision History

Version	Revision Date	Revised By	Summary of Changes	Sections Revised
2.0	2016-08-31	Blunden	Original version	All
3.0	2018-05-22	Blunden, Tolson	Accommodate systems team feedback	All
4.0	2019-01-10	Blunden	Review of IR Process	-
5.0	2019-09-05	Blunden	Footprints decommissioned	All