San Francisco State University
Information Technology Services (ITS)

# Incident Response Report **Form version 2.8.0**	Date Report Submitted (**PST**)	20yy / mm / dd
	Date of Incident (**PST**)	20yy / mm / dd
	Service Now Ticket #	____________________________

Principals

User/System Admin Identification		Device Identification	
User's Name		Vendor	
Email Address		Make	
Phone Number		Model	
SFSU Employee ID		OS/Firmware	
Office Location		SFSU Property Tag	
Department		Computer Name	
Job Title		IP Address	
User's Availability		MAC Address	
Supervisor's Name		Device Encryption	[ ] Yes [ ] No
Supervisor's Email		Encryption Key	Convey to ITS in person
Supervisor's Phone			Upon request

Usage

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.

Not all incidents need to be reported. Isolated low impact events that do not put protected (Level 1 or Level 2) data at risk generally can be handled without using this form. Such incidents can be addressed internally. Though for the sake of maintaining university-wide statistics it's worthwhile to submit an incident ticket to the Service Desk along with the relevant details and mark the entry as "resolved."

Initial Assessment (Triage)

This section is used to assist in evaluating the potential severity of an incident and should be completed *as soon as possible* after it occurs.

Please convey this preliminary information by opening a **Service Desk** ticket (e.g. https://sfsu.service-now.edu/). When submitting a ticket for a suspected incident the “Urgency” field should be set to “Security/Health/Safety.” The “Assignment Group” field should be set to “ITS Security L2.” The “Short Description” field should begin with the phrase “INFOSEC Incident” followed by the name of the caller and a brief synopsis of the incident. For example:

INFOSEC Incident - Jonas Salk Malicious Email Attachment

A more detailed synopsis should be placed in the “Description” field.

Place responses to both the “Principals” section and the following series of questions in the ticket’s initial description. Someone from ITS will either respond via the help desk system, or contact you directly by phone. Please resist the urge to provide curt, obstructive, response like “Don’t know.”

Once you’ve processed the initial assessment questions and contacted ITS please complete the “In-Depth Synopsis” section of this form and attach the completed Incident Response form to the Service Desk ticket.

Finally, this is a Microsoft Word document and it’s intended to be edited.

- **Please delete sections that you don’t complete**
- Also use text highlighting to help signify your entries.

Who observed the incident? Is this user the same person who initiated the event?

At this point you may need to interview the user to elicit additional details.

What was the user doing at the time of the incident?

What indicators of compromise have been observed?

Depending on the nature of the incident, are there indicators or artifacts which provide additional context about the incident? Emphasize *quality* and *relevance* of data over sheer quantity while maintaining completeness.

For example: screen shots, log files on the breached endpoint, browser history, URLs, timestamps, e-mail messages, DNS cache entries, executable file paths, server-side audit trails, etc.

Attach related artifacts (with the exception of executable files and potentially malicious documents) to the ticket for this incident. Screen shots in particular should attempt to capture as much useful information as possible.

Can the indicators of compromise be replicated? (e.g. pop-up window)

Where did the incident take place?

When did the incident occur? When was it detected?

A Word on Containment: After collecting evidence from an impacted system it's prudent to disconnect the system from the network and scan it with an alternative anti-malware suite. Record the conclusion of this scan in your initial assessment, then power down the system and isolate it in a secure area. These measures will stop malware from receiving command & control messages, safeguard against further data loss, and protect against tampering with evidence.

In-Depth Synopsis

The questions in this section are mandatory. Depending on the nature of the incident additional sections of this form may also need to be completed. Keep in mind that SF State's cyber insurance underwriters allocate approximately a week for incidence response.

Which network was the user connected to when the incident transpired? (Highlight One)

- SFSU Wired (Ethernet)
- SFSU Wireless
- SFSU VPN
- Commercial ISP (Comcast, AT&T, etc.)
- Other Public Network

Please specify the approximate time (**PST**) when the incident was detected:
20___/___/___ Hour: Minute

If the exact date and time (**PST**) are uncertain, specify a narrow range of time:
From: 20___/___/___ Hour: Minute **PST** To: 20___/___/___ Hour: Minute **PST**

Do the time of detection and time of occurrence coincide? [ ] Yes [ ] No

Does this incident involve malware? [ ] Yes [ ] No

What was the malware's likely transmission mechanism? (Highlight One)

- E-mail
- Web Browser
- Shared Storage (i.e. USB drive, SMB Network Share)
- Other (Please specify) ____

If "E-mail" has been selected, complete **Section A - Email Phishing**
If "Web Browser" has been selected, complete **Section B - Browser Compromise**
If "Shared Storage" or "Other" has been selected, complete **Section C – Malware Detected**

Are there indications of unauthorized access to SF State information systems? [ ] Yes [ ] No

If the answer is Yes, please complete **Section D – Unauthorized Access**

Was a device used to access confidential data involved in this incident (i.e. "Level 1" data)
[ ] Yes [ ] No

Are there indications that confidential data was accessed?
[ ] Yes [ ] No

If the answer the latter question is Yes, please complete **Section E – Data Breach**

If there are no signs of malware, unauthorized access, account compromise, or a confidential data breach, please complete **Section F – Other Incidents**

Submission

After notifying your supervisor please attach this completed form to the Service Desk ticket registered during the initial assessment. The instructions given herein are designed to guide users to related sections so that additional information is provided only when it's necessary. Focus on submitting an accurate and detailed initial description to us in a timely manner.

Upon submission the ITS Security Team will contact you with feedback, questions, and/or guidance. Once an incident has been resolved, and the corresponding help desk ticket has been closed, the impacted machine should be rebuilt.

Section A – Email Phishing

How did the email-based compromise occur? (Highlight One)

- Opened a malicious email Attachment
- Clicked on a browser URL contained in the email's message
- A malicious payload contained in the email's message

Has the malicious email been deleted? [ ] Yes [ ] No

If the answer is No, forward the incident response team a copy of the email along with header information. Please submit this as information in a raw ASCII text file (.txt) and attach it to the help desk ticket.

If the email has been deleted, please describe what you recall about its contents.

Please return to the **In-Depth Synopsis** section and answer the remaining questions.

Section B – Browser Compromise

Does the user recall the malicious web site that they visited? [ ] Yes [ ] No

If the answer is yes, list the web site URL below and why the user to visited this web site:

____

____

____

If possible, please include a human-readable copy of the browser's history during the time frame of the incident (most browsers have a feature to display recently visited URLs).

Did the user install any browser add-ons or plug-ins shortly before the machine was compromised?
[ ] Yes [ ] No

Did the user download any documents (e.g. PDFs) shortly before the machine was compromised?
[ ] Yes [ ] No

If the answer is yes to either question, describe the aforementioned items.

Please return to the **In-Depth Synopsis** section and answer the remaining questions.

Section C – Malware Detected

How was the malware detected?

If a commercial anti-virus suite detected the threat agent, what specific details about the malware can be gleaned from the suite's alert report (e.g. name of malware, type of malware, standard behavior and delivery mechanism, file path of infestation on endpoint, etc.)?

How was the anti-virus detection triggered? (Highlight One)

- Periodic Scan
- Runtime Protection (anti-virus monitors activity as it occurs)

Does the time of the detection (PST) likely match the time of infestation? Based on local artifacts what was the user doing at the time of the infestation? Does the user have any details to offer?

Did the anti-virus suite clean or quarantine the malware infestation?

Please return to the **In-Depth Synopsis** section and answer the remaining questions.

Section D – Unauthorized Access

Which SF State systems have been accessed without proper authorization?

What indications are there that an unauthorized access had occurred? Are there *relevant* system log files or other artifacts available on the server-side or the client-side within your unit that might help corroborate this?

Please return to the **In-Depth Synopsis** section and answer the remaining questions.

Section E – Data Breach

Has data been lost as the result of stolen SF State property? [ ] Yes [ ] No

If so, was the media storing the accessed confidential data encrypted? [ ] Yes [ ] No

Are there indications (i.e. local client logs, server logs) of unauthorized modification of confidential data?
[ ] Yes [ ] No

Using local resources at your disposal is it possible to assess the scope of the breach?

Confidential Data (also known as "Level 1" Data)

For each type of data listed in the table below, indicate if the data was accessed and if the data was stored on a server or stored locally. Provide either server meta-data or details about where the data was locally stored. If data was stored on the local device, indicate approximately how many records were present on the device.

Level 1 Data Type	Breached?	Server or Local?	# Records
Passwords/Credentials			
Passwords/Login			

PIN (Personal Identification Numbers)			
Electronic or Digital Signature			
Certificate Private Key			
Social Security Number (SSN)			
Last 4 Digits of SSN with Birthdate & Name			
Full SSN and Name			
Payment and Tax Data			
Credit Card Number and Name			
Bank/Debit Card Data and Access PIN			
Tax payer ID and Name			
Health Related Data			
Health Insurance Information			
An Individual's Medical Records			
Psychological Counseling Records			
Biometric Data			
Legal/Contractual Information			
Attorney/Client Communication			
Legal Investigations			
Third-Party Proprietary Data			
A Sealed Bid			
Contractual Agreement			

Internal Use Data (also known as "Level 2" Data)

For each type of data listed in the table below, indicate if the data was accessed and if the data was stored on a server or stored locally. Provide either server meta-data or details about where the data was locally stored. If data was stored on the local device, indicate approximately how many records were present on the device.

Level 2 Data Type	Breached?	Server or Local?	# Records
Name			
Name with Full Birthdate			
Name with Partial Birthdate			
Employee Data			
Net Salary			
Employment History			
Home Address			
Personal Phone Number			
Personal Email Address			
Payments			

Employee Evaluations			
Background Investigations			
Mother’s Maiden Name			
Race and Ethnicity			
Parent’s or other Family Member Names			
Birthplace (City, State, County)			
Gender			
Marital Status			
Physical Description			
Photograph			

Student Data

Grades			
Courses Taken			
Schedule			
Test Scores			
Advising Record			
Disciplinary Actions			
Non-Directory Student Information			

Miscellaneous

Library Circulation Information			
Trade Secrets, Intellectual Property			
Physical Location of Protected Assets			
Licensed Software			

Please return to the **In-Depth Synopsis** section and answer the remaining questions.

Section F – Other Incidents

This section is intended to cover less common types of incidents (e.g. Denial of Service, improper usage) and violations of the acceptable use policy not handled by previous sections.

What signs of compromise have been witnessed? Please be specific and provide as many *relevant* details as possible:

Please return to the **In-Depth Synopsis** section and read instructions about submitting this document.

Revision History

Version	Revision Date	Revised By	Summary of Changes	Sections Revised
2.5	2016-03-08	Blunden	Redraft of original	All
2.5.8	2016-03-25	Blunden	Post EMT Meeting	All

2.5.9	2016-04-07	Blunden	EMT Comments	Initial Assessment, In-Depth Synopsis
2.6.0	2016-05-06	Blunden	ITS Procedural Review	All
2.7.0	2019-01-10	Blunden	Service-Now rollout	All
2.8.0	2021-01-05	Blunden	Formatting, Usability	All