|  |  |
| --- | --- |
| SFSU | **San Francisco State University*****Information Technology Services (ITS)*** |

|  |  |
| --- | --- |
| Incident Response Report**Form version 3** | Date Report Submitted (**PST**) 20yy / mm / dd  |
| Date of Incident (**PST**) 20yy / mm / dd |
| Service Now Ticket # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Principals

|  |  |
| --- | --- |
| Asset User Information |  Device Identification |
| Owner’s Name |  |  Vendor |  |
| Email Address |  |  Make |  |
| Phone Number |  |  Model |  |
| SFSU Employee ID |  |  OS/Firmware  |  |
| Office Location |  |  SFSU Property Tag |  |
| Department |  |  Device 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 could compromise the confidentiality, integrity or availability of SF State information 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)

Triage is intended to assist in evaluating the potential severity of an incident and should be performed *as soon as possible*.

News of the event should be submitted in the form of a **Service Desk** ticket (e.g. https://sfsu.service-now.com/). 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 the campus functional unit that owns the asset in question. 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 Phishing Data Loss**

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

If Level 1 or Level 2 data has been compromised please complete “In-Depth Synopsis” section of this form and attach this form to the Service Desk ticket.

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

* **Please DELETE SECTIONS that you don’t complete**
* Also use text highlighting to help signify your entries.
* Delete portions of this form that aren’t completed or relevant

|  |
| --- |
| 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?  |

|  |
| --- |
| 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 binary files and potentially malicious documents) to the ticket for this incident. Screen shots should attempt to capture as much useful information as possible.

**A Word on Containment**: After collecting evidence from an impacted system please disconnect if from the network and, if possible, scan its primary storage using a different machine. Record the conclusion of this scan in your initial assessment and store the system it in a secure area. This will stop malware from receiving command & control messages, safeguard against further data loss, and protect against tampering with evidence.

 In-Depth Synopsis

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.

|  |
| --- |
| If the user was connected to a network, which one? (Highlight One)* SFSU Wired (Ethernet)
* SFSU Wireless
* SFSU VPN
* Commercial ISP (Comcast, AT&T, etc.)
 |

|  |
| --- |
| Does this incident involve malware? [ ] Yes [ ] NoWhat 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 [ ] NoIf the answer is Yes, please complete **Section D – Unauthorized Access** |

|  |
| --- |
| Was the device used to **access** confidential data involved in this incident (i.e. “Level 1” data)[ ] Yes [ ] NoIf so please respond to the following questions: Has data been lost as the result of **stolen SF State property**? [ ] Yes [ ] NoIf so, was the media storing the accessed confidential data encrypted? [ ] Yes [ ] NoUsing the resources at your disposal is it possible to assess the scope of the breach? Enumerate the SF State data elements at risk, an estimate of the number of records impacted, as well as the systems that hosted the data. Are there indications (i.e. local/remote logs) of unauthorized **modification** of confidential data?[ ] Yes [ ] No |

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

**Submission**

Please attach this completed form to the Service Desk ticket created during the Triage assessment. The instructions that follow 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 in a timely manner.

Please delete unrelated sections to condense this report.

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 device can 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 [ ] NoIf the answer is No, please archive the email along with header information. Please submit this as information in a raw ASCII text file (.txt) and attach it to the service 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 [ ] NoIf 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 site and download history during the time frame of the incident (most browsers have a feature to display recent activity).  |

|  |
| --- |
| Did the user install any browser add-ons or plug-ins shortly before the machine was compromised?[ ] Yes [ ] NoDid the user download any documents (e.g. PDFs) shortly before the machine was compromised?[ ] Yes [ ] NoIf 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 security product 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 detection triggered? (Highlight One)* Periodic Scan
* Runtime Protection (anti-virus monitors activity as it occurs)
 |

|  |
| --- |
| Did the commercial security agent 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 F – Other Incidents

This section is intended to cover less common types of incidents (e.g. Denial of Service, ARP Storms, improper usage, **property theft**) 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 |
| 3.0.0 | 2023-06-20 | Blunden | IR Review | All |