Incident response teams should make an initial report and then continue to report information to their Chain of Command / Security Specialist (as collected).

All security incident reports provided to the Security Specialist (itsecurity@sfa.edu) in response to TAC 202 requirements will be classified and handled as Confidential per *Chapter 2059.055 Texas Government Code (TGC)* and *Chapter 552.139 Texas Business and Commerce Code (TB&CC)*.

If criminal action is suspected, (e.g., violations of *Chapter 33, Penal Code, Computer Crimes*, or *Chapter 33A, Penal Code, Telecommunications Crimes*), the agency is also responsible for contacting the appropriate law enforcement and investigative authorities.

|  |
| --- |
| **1. Contact Information** |
| Full name: |  |
| Job title: |  |
| Division or office: |  |
| Work phone: |  |
| Mobile phone: |  |
| E-mail address: |  |
| *Additional Contact Information:* |

|  |
| --- |
| **2. Type of Incident** *(Insert X on all that apply)* |
|

|  |  |
| --- | --- |
|  | Account Compromise *(e.g., Lost Password)* |
|  | Denial-of-Service *(Including Distributed)* |
|  | Malicious Code *(e.g., Virus, Worm, Trojan)* |
|  | Misuse of Systems *(e.g., Acceptable Use)* |
|  | Reconnaissance *(e.g., Scanning, Probing)* |

 |

|  |  |
| --- | --- |
|  | Social Engineering *(e.g., Phishing, Scams)* |
|  | Technical Vulnerability *(e.g., 0-day Attacks)* |
|  | Theft/Loss of Equipment or Media |
|  | Unauthorized Access *(e.g., Systems, Devices)* |

 |
| *Description of Incident:* |

|  |
| --- |
| **3. Scope of Incident** *(Insert X on all that apply)* |
|

|  |  |
| --- | --- |
|  | Critical *(e.g., Affects State-Wide Information Resources)* |
|  | High *(e.g., Affects Agency Entire Network or Critical Business or Mission Systems)* |
|  | Medium *(e.g., Affects Agency Network Infrastructure, Servers, or Admin Accounts)* |
|  | Low *(e.g., Affects Agency Workstations or User Accounts Only)* |
|  | Unknown/Other *(Please Describe Below)* |

NOTE: All incidents deemed critical or high require additional notification by phone. |
| Estimated Quantity of Systems Affected: |  |
| Estimated Quantity of Users Affected: |  |
| Third Parties Involved or Affected:*(e.g., Vendors, Contractors, Partners)* |  |
| *Additional Scope Information:* |

|  |
| --- |
| **4. Impact of Incident** *(Insert X on all that apply)* |
|

|  |  |
| --- | --- |
|  | Loss of Access to Services |
|  | Loss of Productivity |
|  | Loss of Reputation |
|  | Loss of Revenue |

 |

|  |  |
| --- | --- |
|  | Propagation to Other Networks |
|  | Unauthorized Disclosure of Information  |
|  | Unauthorized Modification of Information |
|  | Unknown/Other *(Please describe below)* |

 |
| Estimated Total Cost Incurred:*(e.g., Cost to Contain Incident, Restore Systems, Notify Data Owners)* |  |
| *Additional Impact Information:* |

|  |
| --- |
| **5. Sensitivity of Affected Data/Information** *(Insert X on all that apply)* |
|

|  |  |
| --- | --- |
|  | Critical Information |
|  | Non-Critical Information |
|  | Publicly Available Information |
|  | Financial Information |

 |

|  |  |
| --- | --- |
|  | Personally Identifiable Information (PII) |
|  | Intellectual/Copyrighted Information |
|  | Critical Infrastructure/Key Resources |
|  | Unknown/Other *(Please Describe Below)* |

 |
| Data Encrypted?  |  |
| Quantity of Information Affected:*(e.g., File Sizes, Number of Records)* |  |
| *Additional Affected Data Information:* |

|  |
| --- |
| **6. Systems Affected by Incident** *(Provide as much detail as possible)* |
| Attack Sources *(e.g., IP Address, Port)*: |  |
| Attack Destinations *(e.g., IP address, Port)*: |  |
| IP Addresses of Affected Systems: |  |
| Domain Names of Affected Systems: |  |
| Primary Functions of Affected Systems:*(e.g., Web Server, Domain Controller)* |  |
| Operating Systems of Affected Systems:*(e.g., Version, Service Pack, Configuration)* |  |
| Patch Level of Affected Systems:*(e.g., Latest Patches Loaded, Hotfixes)* |  |
| Security Software Loaded on Affected Systems:*(e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)* |  |
| Physical Location of Affected Systems:*(e.g., State, City, Building, Room, Desk)* |  |
| *Additional System Details:* |

|  |
| --- |
| **7. Users Affected by Incident** *(Provide as much detail as possible)* |
| Names and Job Titles of Affected Users: |  |
| System Access Levels or Rights of Affected Users: *(e.g., regular User, Domain Administrator, Root)* |  |
| *Additional User Details:* |

|  |
| --- |
| **8. Timeline of Incident** *(Provide as much detail as possible)* |
| a. Date and Time When Agency First Detected, Discovered, or Was Notified About the Incident: |  |
| b. Date and Time When the Actual Incident Occurred:*(Estimate If Exact Date and Time Unknown)* |  |
| c. Date and Time When The Incident Was Contained or When All Affected Systems or Functions Were Restored:*(Use Latest Date and Time)* |  |
| Elapsed Time Between the Incident and Discovery:*(e.g., Difference Between a. and b. Above)* |  |
| Elapsed Time Between the Discovery and Restoration:*(e.g., Difference Between a. and c. Above)* |  |
| *Detailed Incident Timeline:* |

|  |
| --- |
| **9. Remediation of Incident** *(Provide as much detail as possible)* |
| Actions Taken To Identify Affected Resources: |  |
| Actions Taken to Remediate Incident: |  |
| Actions Planned to Prevent Similar Incidents: |  |
| *Additional Remediation Details:* |