Computer Incident Reporting Form

|  |  |
| --- | --- |
| **Is this a drill?** | Yes / No |

# General Incident Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** |  | **Incident POC Name** |  |
| **Time** |  | **Incident POC Phone** |  |
| **Time Zone** |  | **Incident POC Email** |  |

# Initial Detection

|  |  |
| --- | --- |
| **Type of Incident** | outage / malware / unauthorized access (outsider) / inappropriate access (insider) / espionage / data breach / other (describe) |
| **Date, time, and time zone of first detection** |  |
| **List names and contact information for all persons involved in detection and initial investigation** |  |
| **How was incident detected?** |  |
| **What do you think happened?** |  |
| **List of systems involved.**  **Include location, system name, IP address, MAC, serial number, corporate ID.** | System 1:  System 2:  System 3: |
| **Where can supporting information be found?** | (location of log files, time-stamps, screenshots, photographs, etc) |
| **Could sensitive information have been accessed? Describe worst and best-case scenarios based on current knowledge.** | Yes / No  PII / PHI / PCI / GDPR / Classified / Unclassified but Sensitive / Trade Secrets / Financial / Other (describe)  Worst case scenario:  Best case scenario: |
| **If yes, notify compliance officer, CISO, or another corporate officer immediately. Who was notified? When?** |  |

# Initial Response

|  |  |
| --- | --- |
| **Were any immediate changes made in response to the incident? (such as disconnecting system or disabling accounts).**  **List time stamps for each change.** |  |
| **Who authorized the changes?** |  |

# Chain of Custody

|  |  |
| --- | --- |
| **Were original systems isolated for forensic review?** |  |
| **Were backups or other system-state copies created? Describe. When were they created?** |  |
| **Location of systems or copies** |  |
| **How are systems or copies protected from alteration?** |  |
| **List name and contact information for person who is responsible for safekeeping of systems or copies** |  |

# Data Breach Incident

|  |  |
| --- | --- |
| **Refer to organization’s data breach procedures or policy. Name of document used:** |  |
| **Each day during incident, add any new findings about worst-case and best-case scenarios for the data breach. Do not delete prior days information.** | # of persons affected  List categories of data compromised (names, socials, credit card numbers, passwords, schematics for X design, etc)  Was data copied outside of the organization?  What sources of data were compromised? |
| **Each day during incident, add any escalations or notifications that were performed.** | FBI contacted on date/time  Notified ### customers of potential data breach on date/time |

# Incident Wrap-up

|  |  |
| --- | --- |
| **Current status of incident?** |  |
| **Final root cause analysis** |  |
| **Date, time, and time-zone that incident started** |  |
| **Date, time, and time-zone that incident ended** |  |
| **Describe actions taken to resolve incident (if applicable). Who performed?** |  |
| **Describe containment and/or preventative actions (if applicable). Who performed?** |  |
| **Follow-up actions needed?**  **List responsible party.** |  |
| **Lessons learned?** |  |