**Name of Organization**

**Incident Notification Form**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Reporting Form is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals with a need to know. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

(Name of Organization) Incident Reporting Form is a standard procedure form used to document relevant security incident information during the reporting of confirmed or suspected breach or misuse of Name of Organization’s technology and resources.

All personnel are responsible for:

* Contacting the Incident Commander and assisting the Cybersecurity Incident Response Team (CIRT) in assessing the significance of a security incident within their organization
* Submitting this report to the Incident Commander based on the business impact on affected informational resources and the current and potential technical effect of the incident. This includes the loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks. The Incident Reporting Form is used to document relevant security incident information.

Depending on the priority of the incident, it may not always be feasible to gather all information prior to reporting to the Incident Commander. In such cases, incident response teams should make an initial report and then continue to report information to the Incident Commander as it is collected.

All security incident reports provided to the Incident Commander in response to organizational requirements will be classified and handled as Confidential. If criminal action is suspected, the Incident Commander is responsible for contacting the appropriate law enforcement and investigative authorities. Based on criticality and scope of the incident, the Incident Commander may need to report and establish communication with other agencies and follow National Incident Management System (NIMS) guidelines related to emergency response, communication, and coordination.

This report is broken up into 10 sections. Each section is important to the reporting process and should be accurately completed in its entirety.

| **1. Contact Information** | |
| --- | --- |
| Full name: |  |
| Job title: |  |
| Company: |  |
| Department: |  |
| Work phone: |  |
| Mobile phone: |  |
| E-mail address: |  |
| Fax number: |  |
| *Additional contact information:* | |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Type of Incident** *(Check all that apply)* | | | |
|  | Account compromise *(e.g., lost password)* |  | Social engineering *(e.g., phishing, scams)* |
|  | Denial-of-Service *(including distributed)* |  | Technical vulnerability *(e.g., 0-day attacks)* |
|  | Malicious code *(e.g., virus, worm, Trojan)* |  | Theft/loss of equipment or media |
|  | Misuse of systems *(e.g., acceptable use)* |  | Unauthorized access *(e.g., systems, devices)* |
|  | Reconnaissance *(e.g., scanning, probing)* |  | Unknown/Other *(Please describe below)* |
| *Description of incident:* | | | |

| **3. Scope of Incident** *(Check one)* | | |
| --- | --- | --- |
|  | Critical *(e.g., affects company-wide information resources and or customers)* | |
|  | Serious *(e.g., affects Company’s entire network or critical business or mission systems)*  NOTE: All incidents deemed critical or high require additional notification by phone. | |
|  | Important *(e.g., affects Company’s network infrastructure, servers, or admin accounts)* | |
|  | Informational *(e.g., affects Company’s workstations or user accounts only)* | |
|  | Unknown/Other *(Please describe below)* | |
| 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** *(Check all that apply)* | | | |
| --- | --- | --- | --- |
|  | Loss of access to services |  | Propagation to other networks |
|  | Loss of productivity |  | Unauthorized disclosure of data/information |
|  | Loss of reputation |  | Unauthorized modification of data/information |
|  | Loss of revenue |  | 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** *(Check all that apply)* | | | |
| --- | --- | --- | --- |
|  | Confidential/sensitive data/info |  | Personally identifiable information (PII) |
|  | Non-sensitive data/info |  | Intellectual property/copyrighted data/info |
|  | Publicly available data/info |  | Critical infrastructure/key resources |
|  | Financial data/info |  | Unknown/other *(Please describe below)* |
| Data encrypted? Yes \_\_\_\_ No \_\_\_\_ | | | |
| Quantity of data/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 department or individual 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: | |

| **10. Miscellaneous** *(Provide any other relevant information)* |
| --- |
| Additional information: |

PLEASE NOTE: All Security Incident Reporting Forms and accompanying documentation must be transmitted to the Incident Response Commander in a secure manner. Please encrypt all documents prior to transmission or use secure messaging.

Please submit completed form to:

Incident Commander [Name@organization.com](mailto:Name@organization.com) or +1 xxx xxx-xxxx or via Ticket system