|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Incident Response Report**  **NOTE: UNDER NO CIRCUMSTANCE SHOULD personal INFORMATION OF InDividuals IMPACTED IN the Incident be documented in the Security Incident Report to protect the individual’s Privacy and rights.** | | | | | |
| **Incident Tracking Identifier:**  IR-MM-DD-YY-### | | | | **Footprints Ticket #:** | |
| **Date/Time Incident Started:** MM-DD-YY HH:mm  **Date/Time Incident Ended:**  MM-DD-YY HH:mm | | | | **Date/Time Incident Reported:** MM-DD-YY HH:mm  **Date/Time Incident Resolved:** MM-DD-YY HH:mm | |
| **Identification** (Step 1):  **Reporting Source** (check one):  Employee  Customer  Internal Administration (e.g. Mgt, HR, Legal, IT)  Outside Counsel  Law Enforcement  Media  Other: Please specify  **Incident Description:**  Description of the incident as provided by the reporting source. Include who reported the incident, who initially responded to the incident, what happened, when did the incident occur, where did the incident occur, how did the event occur? | | | | | |
| **Incident Classification** (Step 2): | | | | | |
| **Category** (check all that apply)  Theft/Loss  Unauthorized Access  Service Disruption  Policy Violation  Personal Safety  Privacy  System/Data Compromise | | **Asset Type** (check all that apply):  Hardware  Piracy (Software)  Electronic  Physical  Electronic  Physical  Employee  Customer  Patient Safety  Employee PII  Customer PII  PCI  PHI  Public  R&D  Customer Confidential Company IP  Company Records | | | |
| **Triage** (Step 3):  Check all departments and business units that apply:  IT  Facilities  HR  Mobility  Enterprise  Healthcare  Legal  CSO | | | | | |
| **Impact Analysis and Escalation** (Step 4):  **Business and Assets Impacted:** <10  10-50  50-100  100-500 500-1000 1000+  Specify assets impacted by the incident:  Physical HW(s): Specify ANY hardware impacted by incident  Facility(s): Specify ANY facilities impacted by incident  User(s): Specify ANY general User Groups impacted by incident  Services: Specify ANY Services impacted by incident  Application/Product(s): Specify ANY Applications and/or Products impacted by incident  Customer(s): Specify any customer groups impacted by incident  Data: Specify ANY Data or information impacted by incident  Other: Specify AnY other assets or business impacted by incident  **Risk Severity Level**: Select Rating From Rating Chart (0-5):  **Escalation (Incident Management Team):**  IT Service Desk: SPECIFY INDIVIDUAL NAME(S)  Dept./BU Incident Coordinator: SPECIFY INDIVIDUAL NAME(S)  Dept./BU Sr. Manager: SPECIFY INDIVIDUAL NAME(S)  Dept./VP: SPECIFY INDIVIDUAL NAME(S)  Dept./SVP: SPECIFY INDIVIDUAL NAME(S)  Legal & CSO: SPECIFY INDIVIDUAL NAME(S) | | | | | |
| **Incident Investigation and Forensics Analyses** (Step 5):  **Mitigation/Containment Steps:**   * In chronological order, list steps taken to mitigate or contain the incident. Provide date & time (MM-DD-YY HH:MM) of each step along with the individual name(s) who performed the step. e.g.   04-01-12 02:20 – John Doe observed application not responding. CPU at 100%.  04-01-12 02:30 – John Doe restarted application. CPU still running at 100%.  04-01-12 02:45 – John Doe rebooted server. CPU and application returned to normal.  **Investigation:**  In chronological order, list steps taken to determine the following (Provide date & time (MM-DD-YY HH:MM) of each step along with the individual name(s) who performed the step):   * Assets impacted * Severity of the incident * Who has the incident management contacted * Root cause * Post-mortem activities   **Root Cause:** Describe in detail the root cause for the incident. | | | | | |
| **Post-Mortem** (Step 6): | | | | | |
| List all post-mortem activity with assigned owner and expected due date. Include the following:   * Additional actions needed to remediate the incident * Internal communications with employees * External communications with customers, media, regulators, law enforcement, external counsel * Meetings for action plans, communications, lessons learned | | | | | |
| **Report Revisions** | | | | | |
| **Date** | **Modifier Name** | | **Role** | | **Notes** |
| MM/DD/YY |  | | Author (required) | | Initial Report Creation |
| MM/DD/YY |  | | Contributor | |  |
| MM/DD/YY |  | | Approver (required) | | Approval of report |