Security Incident Form

|  |  |
| --- | --- |
|  | |
| INCIDENT IDENTIFICATION INFORMATION | |
| Date and Time of Notification: | |
| Incident Detector’s Information: | |
| Name: Date and Time Detected: | |
| Title: Location: | |
| Phone/Contact Info: | **System or Application:** |
| INCIDENT SUMMARY | |
| Type of Incident Detected:  ☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Access ☐ Unplanned ☐ Downtime | **☐ Unauthorized Use**  **☐ Other** |
| Description of Incident: | |
| Names and Contact Information of Others Involved: | |
| Other information: | |
| ACTIONS | |
| Identification Measures (Incident Verified, Assessed, Options Evaluated): | |
| Containment Measures: | |
| Evidence Collected (Systems Logs, etc.): | |
| Eradication Measures: | |
| Recovery Measures: | |
| Other Mitigation Actions: | |
| EVALUATION | |
| How Well Did Work Force Members Respond? | |
| Were the Documented Procedures Followed? Were They Adequate? | |
| What Information Was Needed Sooner? | |
| Were Any Steps or Actions Taken That Might Have Inhibited the Recovery? | |
| What Could Work Force Members Do Differently the Next Time an Incident Occurs? | |
| What Corrective Actions Can Prevent Similar Incidents in the Future? | |
| What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents? | |
| Other Conclusions or Recommendations: | |
| FOLLOW-UP | |
| Reviewed By: ☐ Security Officer ☐IT Department/Team ☐ Privacy Officer ☐ Other | |
| Recommended Actions Carried Out: | |
| Initial Report Completed By: | |
| Follow-Up Completed By: | |

This form has been developed as a working tool for assessment and improvement activities after an incident in an organization.   
It is intended for internal use only.