

Information Security Incident Response Form

# Incident Detection & Analysis

|  |  |
| --- | --- |
| Item | Description |
| Incident # |  |
| Date |  |
| Incident Indicators  (employee report, SIEM, IDS or others) |  |
| Determine whether an incident has occurred |  |
| Affected Systems  (which systems are affected) |  |
| Attack Vectors  (how systems were affected) | (External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others) |
| Incident Actors  (whose actions affected system) |  |
| Functional Impact  (how significant is the system impact) | (None, Low, Medium, High) |
| Information Impact | (None, Privacy Breach, Proprietary Breach, Integrity Loss) |
| Recoverability Effort | (Regular, Supplemented, Extended, Not Recoverable) |
| Internal Notification  (list internal notifications that have been made) |  |
| External Notification  (list external notifications that have been made) |  |
| Other information |  |

# Containment, Eradication and Recovery

## Containment

|  |  |
| --- | --- |
| Item | Description |
| Incident Status |  |
| Integrity Assessment |  |
| Containment Measures |  |

## Eradication

|  |  |
| --- | --- |
| Item | Description |
| Incident Status |  |
| Vulnerability Assessment |  |
| Eradication Measures |  |

## Recovery

|  |  |
| --- | --- |
| Item | Description |
| Incident Status |  |
| Recovery Plan |  |
| Recovery Process  Documentation |  |
| Validation |  |

# Post Incident Analysis & Forensic

|  |  |
| --- | --- |
| Item | Description |
| Collected Forensic Data |  |
| Evaluation Process |  |
| Lessons Learned |  |
| Action Items |  |

Incident Handling Checklist

|  |  |  |
| --- | --- | --- |
| **Action** | | **Completed** |
| **Detection and Analysis** | |  |
| 1. | Determine whether an incident has occurred |  |
| 1.1 | Analyze the precursors and indicators |  |
| 1.2 | Look for correlating information |  |
| 1.3 | Perform research (e.g., search engines, knowledge base) |  |
| 1.4 | As soon as the Incident Manager believes an incident has occurred, begin documenting the investigation and gathering evidence |  |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |  |
| 3. | Report the incident to the appropriate internal personnel and external organizations |  |
| **Containment, Eradication, and Recovery** | |  |
| 4. | Acquire, preserve, secure, and document evidence |  |
| 5. | Contain the incident |  |
| 6. | Eradicate the incident |  |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited |  |
| 6.2 | Remove malware, inappropriate materials, and other components |  |
| 6.3 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them |  |
| 7. | Recover from the incident |  |
| 7.1 | Return affected systems to an operationally ready state |  |
| 7.2 | Confirm that the affected systems are functioning normally |  |
| 7.3 | If necessary, implement additional monitoring to look for future related activity |  |
| **Post-Incident Activity** | |  |
| 8. | Create a follow-up report |  |
| 9. | Hold a lessons learned meeting (mandatory for major incidents, optional otherwise) |  |

*Reference: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  | Original version |
|  |  |  |
|  |  |  |