## IR PROCEDURE REFERENCE

### Executive Summary

* “security incident” = any unauthorized access (including company-owned devices, employee-owned registered devices, servers, proprietary and confidential data), unauthorized modifications of data, and unintended downtime traced to malicious activity
* See National Institute of Standards and Technology (NIST)’s Computer Security Incident Handling Guide, Section 3, “Handling an Incident”

### Scope

all employees, devices, infrastructure, and contracted third-party vendors

### Preparation and Planning

* Training, chain of command/management, routine education
* R&Rs for rapid-response
* Implement SIEM, prioritize critical and unpatchable stuff, specialized alerts (IDS portion)
  + Additional countermeasures/defenses as needed
* Backup critical data and services regularly, no complete loss happening here

### Detection and Analysis

* Monitoring tools, automated solutions; IDS/IPS
* Create baseline to minimize false positives, manual review as needed
* Document and preserve as possible in event of incident
* Analyze methodology to guide targeted response (see MITRE ATT&CK), aim for thorough post-mortem

### Containment, Eradication, and Recovery

* Contain threat to mitigate impact, minimize blast radius
* Identify root cause, eradicate from there (out malware, disable bad accs, identify vulns, disable service)
* After adversary eradication, work on restoring normal ops and secure as best as possible (restore from backup, patch, rotate, change perms + firewalls)

### Post-Incident Activity

* Create report - technical details, evidence, impact on business, mitigations for future
* Guideline dev for preventative measures, remediate vulns, addl solutions and operational protocol
* Meet stakeholders + management, guidance
* Address users and external stakeholders, guidance

### 

### Sources

* [*https://frsecure.com/incident-response-policy-template/*](https://frsecure.com/incident-response-policy-template/)
* [*https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17*](https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17)
* [*https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf*](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)
* [*https://www.fbi.gov/file-repository/incident-response-policy.pdf/view*](https://www.fbi.gov/file-repository/incident-response-policy.pdf/view)
* [*https://attack.mitre.org/*](https://attack.mitre.org/)
* [*https://www.sans.org/media/score/504-incident-response-cycle.pdf*](https://www.sans.org/media/score/504-incident-response-cycle.pdf)

Incident Response Form

| **Breach Date and Time:**  MM/DD/20YY, H:M:S(:MS) | |
| --- | --- |
| **Affected IP/Hostname of Breached System(s):**  IP | Hostname | |
| **Source IP of Attacking System(s):**  (REQUIRED.) | |
| **Breach Narrative:**  (Provide information about the breach in detail here, including the type of incident.) | |
| **Impact on Services:**  Please highlight the designated impact below: | |
| None | No effect to the organization’s ability to provide all services to all users |
| Low | Minimal effect; the organization can still provide all critical services to all users but has lost efficiency |
| Medium | Organization has lost the ability to provide a critical service to a subset of system users |
| High | Organization is no longer able to provide some critical services to any users |
| **Impact on Information:**  Please highlight the designated impact below: | |
| None | No information was exfiltrated, changed, deleted, or otherwise compromised |
| Privacy Breach | Sensitive PII of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated |
| Proprietary Breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated |
| Integrity Loss | Sensitive or proprietary information was changed or deleted |
| Please highlight the applicable metrics below: | |
| **Attack Vector:**  Network Adjacent  Local Physical | **Attack Complexity:**    Low High |
| **Privileges Required:**  None Low High | **User Interaction:**  None Required |
| **Scope:**  Unchanged Changed | **Confidentiality:**  None Low High |
| **Integrity:**  None Low High | **Availability:**  None Low High |
| **Remediation/Mitigation Steps:**  (Steps to take in order to patch exploited machines and prevent further vulnerability.) | |
| **Extra Artifacts:**  (Additional artifacts related to the incident should be listed in this section. This can be text, code, or pictures.) | |

This form is modeled after the Forum of Incident Response and Security Teams (FIRST)’s Common Vulnerability Scoring System (CVSS) ([*https://www.first.org/cvss/calculator/3.1*](https://www.first.org/cvss/calculator/3.1)). This template is also copied over from our team members’ past engagements as it was custom-developed to be applicable in all situations.