IS-10 INCIDENT RESPONSE POLICY

**11.1. Incident Response Policy**

<COMPANY NAME> implements an information security incident response process to consistently detect, respond to, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

* Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications.
* Establishment of an information security incident response team;
* Establishment of procedures to respond to media inquiries;
* Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents.
* Workforce training, education, and awareness on information security incidents and required responses; and;
* Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders.

**11.2 Incident Management Policies**

The <COMPANY NAME> incident response process follows the process recommended by [SANS] (https://www.sans.org), an industry leader in security. To keep abreast of vulnerabilities and techniques of attacking networks, the organization subscribes to security alert services such as the SysAdmin, Audit, Network and Security (SANS) Internet Storm Center (ISC) at http://isc.sans.org or the United States Computer Emergency Readiness Team (US-CERT) at <http://www.us-cert.gov/>**.** <COMPANY NAME>'s incident response classifies security-related events into the following categories:

**Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:

* Hardware component failing causing service outages.
* Software error causing service outages.
* General network or system instability.

**Precursors** - A sign that an incident may occur in the future. Examples:

* Monitoring system showing unusual behavior.
* Audit log alerts indicated several failed login attempts.
* Suspicious emails targeting specific <COMPANY NAME> staff members with administrative access to production systems.

**Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:

* IDS alerts for modified system files or unusual system accesses.
* Antivirus alerts for infected files.
* Excessive network traffic directed at unexpected geographic locations.

**Incidents** - A violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:

* Unauthorized disclosure of ePHI.
* Unauthorized change or destruction of ePHI.
* A data breach accomplished by an internal or external entity.
* A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

<COMPANY NAME> employees must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security Officer know about any observed precursors or indications as soon as they are discovered.

**11.2.1 Identification Phase**

1. Immediately upon observation <COMPANY NAME> members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways:
   1. Direct report to management, the Security Officer, Privacy Officer, or other;
   2. Email;
   3. Phone call;
   4. Secure Chat;
   5. Anonymously through workforce member's desired channels.
2. The individual receiving the report facilitates completion of an Incident Response Form and notifies the Security Officer (if not already done).
3. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.
   1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
      1. Non-Technical Event (minor infringement): the Security Officer completes an Incident Response Form (Appendix A) and investigates the incident.
      2. Technical Event: Assign the issue to an IT resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a small office or lack of expertise in the area.
   2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior management.
4. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
5. Once the investigation is completed, progress to Phase V, Follow-up.
6. If the issue is a technical security incident, commence to Phase II: Containment.
7. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
8. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
9. The lead member of the SIRT team facilitates initiation of an Incident Response Form. The intent of this form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
10. The Security Officer, Privacy Officer, or <COMPANY NAME> representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.
11. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to <COMPANY NAME> and potentially external.

**11.2.2 Containment Phase (Technical)**

In this Phase, <COMPANY NAME>'s IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.
2. The SIRT secures the network perimeter.
3. The IT department performs the following:
   1. Securely connect to the affected system over a trusted connection.
   2. Retrieve any volatile data from the affected system.
   3. Determine the relative integrity and the appropriateness of backing the system up.
   4. If appropriate, back up the system.
   5. Change the password(s) to the affected system(s).
   6. Determine whether it is safe to continue operations with the affected system(s).
   7. If it is safe, allow the system to continue to function.
   8. Complete any documentation relative to the security incident on the Incident Response Form
   9. Move to Phase V, Follow-up.
4. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
   1. The individual completing this phase provides written communication to the SIRT.
5. Continuously apprise Senior Management of progress.
6. Continue to notify affected Customers and Partners with relevant updates as needed

**11.2.3 Eradication Phase (Technical)**

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
   1. An increase in network perimeter defenses.
   2. An increase in system monitoring defenses.
   3. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
   1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
4. Complete the Incident Response Form.
5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
6. Apprise Senior Management of the progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase IV, Recovery.

**11.2.4 Recovery Phase (Technical)**

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected. The technical team determines if the affected system(s) have been changed in any way.

* If they have, the technical team restores the system to its proper, intended functioning ("last known good").
* Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
* If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
* If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
* Update the documentation with the detail that was determined during this phase.
* Apprise Senior Management of progress.
* Continue to notify affected Customers and Partners with relevant updates as needed.
* Move to Phase V, Follow-up.

**11.2.5 Follow-up Phase (Technical and Non-Technical)**

The Follow-up Phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
2. Create a "lessons learned" document and attach it to the completed Incident Response Form.
   1. Evaluate the cost and impact of the security incident to <COMPANY NAME> using the documents provided by the SIRT and the technical security resource.
   2. Determine what could be improved.
   3. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.
   4. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.
   5. Close the security incident.

**11.2.6 Periodic Evaluation**

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding <COMPANY NAME>'s expectation for them, relative to security responsibilities. The incident response plan is tested annually.

**11.3 Security Incident Response Team (SIRT)**

Current members of the <COMPANY NAME> SIRT:

* Security Officer
* Privacy Officer

**11.4 Potential Security Log Sources**

* Server and workstation operating system logs
* Application logs (e.g., web server, database server)
* Security tool logs (e.g., anti-virus, change detection, intrusion detection/prevention system)
* Outbound proxy logs and end-user application logs
* Remember to consider other, non-log sources for security events.

**Typical Log Locations**

* Linux OS and core applications: /var/log
* Windows OS and core applications: Windows Event Log (Security, System, Application)
* Network devices: usually logged via Syslog; some use proprietary locations and formats

**What to Look For On Linux**

|  |  |
| --- | --- |
| Successful user login | “Accepted password”, “Accepted publickey”, “session opened” |
| Failed user login | “authentication failure”, “failed password” |
| User log-off | “session closed” |
| User account change or deletion | “password changed”, “new user”, “delete user” |
| Sudo actions | “sudo: … COMMAND=…” “FAILED su” |
| Service failure | “failed” or “failure” |

**What to Look For On Windows**

Most of the events below are in the Security log; many are only logged on the domain controller.

|  |  |
| --- | --- |
| User logon/logoff events | Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc. |
| User account changes | Created 624; enabled 626; changed 642; disabled 629; deleted 630 |
| Password changes | To self: 628; to others: 627 |
| Service started or stopped | 7035, 7036, etc. |
| Object access denied (if auditing enabled) | 560, 567, etc. |

**What to Look For On Network Devices**

* Look at both inbound and outbound activities.
* Examples below show log excerpts from Cisco ASA logs; other devices have similar functionality.

|  |  |
| --- | --- |
| Traffic allowed on firewall | “Built … connection”, “access-list … permitted” |
| Traffic blocked on firewall | “access-list … denied”, “deny inbound”; “Deny … by” |
| Bytes transferred (large files?) | “Teardown TCP connection … duration … bytes …” |
| Bandwidth and protocol usage | “limit … exceeded”, “CPU utilization” |
| Detected attack activity | “attack from” |
| User account changes | “user added”, “user deleted”, “User priv level changed” |
| Administrator access | “AAA user …”, “User … locked out”, “login failed” |

**What to Look For On Web Servers**

* Excessive access attempts to non-existent files
* Code (SQL, HTML) seen as part of the URL
* Access to extensions you have not implemented
* Web service stopped/started/failed messages
* Access to “risky” pages that accept user input
* Look at logs on all servers in the load balancer pool
* Error code 200 on files that are not yours

|  |  |
| --- | --- |
| Failed user authentication | Error code 401, 403 |
| Invalid request | Error code 400 |
| Internal server error | Error code 500 |

**Purpose**

The purpose for this Policy is to define the administration and controls required for the protection of <COMPANY NAME>’s information and information systems from the potential threat of unauthorized physical access, use, abuse, theft, and sabotage independent of its physical location. Additionally, this policy is to ensure that the confidentiality, integrity, and availability of all <COMPANY NAME> data and information systems are protected by having in place appropriate controls for facility and data center access, environmental protection (e.g. temperature/humidity control, fire detection/suppression), and alternate work sites.

**Scope**

This policy applies to all <COMPANY NAME> locations including any alternate processing centers used for disaster recovery. Additionally, all users of Company information systems are responsible for complying with and understanding this policy. This includes (but is not limited to) employees, consultants, contractors, vendors, business partners and temporary staff.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 11.a - Reporting Information Security Events
* 11.c - Responsibilities and Procedures

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(5)(i) - Security Awareness and Training
* 164.308(a)(6) - Security Incident Procedures

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |

## SECURITY INCIDENT REPORT

**1.0 Reported By**

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1 Last Name: |  | 1.2 First Name: |  |
| 1.3 Position: |  | | |
| 1.4 Name of organization or  company: |  | | |
| 1.5 Telephone No: |  | | |
| 1.6 E-mail: |  | | |

**2.0 Organization Details**

|  |  |
| --- | --- |
| 2.1 Name of organization: |  |
| 2.2 Type of organization: |  |
| 2.3 Street Address: |  |
| 2.4 At this time, is it known that other organizations are affected by this incident? (If so, list names, addresses, telephone number, email addresses and contact  persons): |  |

**3.0 Incident Details including Injury and Impact Level**

|  |  |  |  |
| --- | --- | --- | --- |
| 3.1 Date: |  | 3.2 Time: |  |
| 3.3 Location of affected site: |  | | |
| 3.4 Brief summary of the incident (what has happened, where did it happen, when did it happen): |  | | |
| 3.5 Description of the project/program and information involved, and, if  applicable, the name of the  specific program: |  | | |
| 3.6 Classification level of the information involved |  | | |
| 3.7 System compromise (detail): |  | | |
| 3.8 Data compromise (detail): |  | | |
| 3.9 Originator and /or Official Classification Authority of  the information involved? (List name, address, telephone no., email and contact person). |  | | |
| 3.10 Is Foreign Government Information involved? Originating country or  International organization? |  | | |
| 3.11 Did the incident occur on an accredited system authorized to process and store the information in question? |  | | |
| 3.12 Estimated injury  level/sector: |  | | |
| 3.13 Estimated impact level: (any compromise or  disruption to service?) |  | | |
| 3.14 Incident duration: |  | | |
| 3.15 Estimated number of systems affected: |  | | |
| 3.16 Percentage of organization systems  affected: |  | | |
| 3.17 Action taken: |  | | |
| 3.18 Supporting documents attached (describe if any) |  | | |
| 3.19 Multiple occurrence or first time this type of incident  occurs within this location? |  | | |
| 3.20 Incident Status (resolved or unresolved) |  | | |
| 3.21 Has the matter been reported to other authorities? If so, list names, addresses, telephone no., email and contact person. |  | | |

|  |  |
| --- | --- |
|  |  |

**4.0 Status of Mitigation Actions**

|  |  |
| --- | --- |
| 4.1 Mitigation details to date: (List any actions that have been taken to mitigate  incident and by whom) |  |
| 4.2 Results of mitigation: |  |
| 4.3 Additional assistance required? |  |

**5.0 Computer Network Defense Incident Type (if applicable)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5.1 Malicious code: (Worm, virus, trojan,  backdoor, rootkit, etc.) |  | | | |
| 5.2 Known vulnerability exploit:  (List the Common Vulnerabilities and Exposures (CVE) number for known vulnerability) |  | | | |
| 5.3 Disruption of service: |  | | | |
| 5.4 Access violation: (Unauthorized access attempt, successful unauthorized access, password cracking, Etc.) |  | | | |
| 5.5 Accident or error: (Equipment failure, operator error, user error, natural or  accidental causes) |  | | | |
| 5.6 If the incident resulted from user error or malfeasance, identify reasons (training, disregard for policy,  other) and responsible parties |  | | | |
| 5.7 Additional details: |  | | | |
| 5.8. Apparent Origin of Incident or Attack | Source IP and port: |  | Protocol: |  |
| URL: |  | Malware: |  |
| Additional details: |  | | |

**6.0 Systems Affected**

|  |  |
| --- | --- |
| 6.1 Network zone affected: (Internet, administration,  internal, etc.) |  |
| 6.2 Type of system affected: (File server, Web server, mail server, database, workstation  (mobile or desktop), etc.) |  |
| 6.3 Operating system (specify  version): |  |
| 6.4 Protocols or services: |  |
| 6.5 Application (specify version): |  |

**7.0 Post Incident Activities**

|  |  |
| --- | --- |
| 7.1 Has information contained in this report been provided to the authorities?  When? |  |
| 7.2 Complete a root cause analysis to determine the reason for the incident and steps to prevent re-occurrence. |  |