10. Incident Response Policy

Ceresti implements an information security incident response process to consistently detect, respond, 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

Note: These policies were adapted from work by the HIPAA Collaborative of Wisconsin Security Networking Group. Refer to the linked document for additional copyright information.

10.1 Applicable Standards

10.1.1 Applicable Standards from the HITRUST Common Security Framework

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

10.1.2 Applicable Standards from the HIPAA Security Rule

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

10.2 Incident Management Policies

The Ceresti incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process

which can be found in this document.

Ceresti'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 Ceresti 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.

Ceresti 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.

10.2.1 Identification Phase

1. Immediately upon observation Ceresti 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. Online incident response form located here;

5. Private channel on Slack.
6. Anonymously through employees desired channels.

2. The individual receiving the report facilitates completion of an Incident Identification 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 a SIR Form 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.
    2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior management.
        1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
        2. Once the investigation is completed, progress to Phase V, Follow-up.
        3. If the issue is a technical security incident, commence to Phase II: Containment.
        4. 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.
        5. 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.
        6. The lead member of the SIRT team facilitates initiation of a SIR Form or an Incident Survey Form. The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
4. The Security Officer, Privacy Officer, or Ceresti representative appointed notifies any affected Customers. If no Customers are affected, notification is at the discretion of the Security and Privacy Officer.
5. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to Ceresti and potentially external.

10.2.2 Containment Phase (Technical)

In this Phase, Ceresti'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 affect system(s).
    7. If it is safe, allow the system to continue to function;
        1. Complete any documentation relative to the security incident on the SIR Form.
        2. Move to Phase V, Follow-up.
    8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
    9. The individual completing this phase provides written communication to the SIRT.
4. Continuously apprise Senior Management of progress.
5. Continue to notify affected Customers with relevant updates as needed

10.2.3 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 Eradication 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.

10.2.4 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.

1. The technical team determines if the affected system(s) have been changed in any way.
    1. If they have, the technical team restores the system to its proper, intended functioning ("last known good").
    2. 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).
    3. 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.
    4. 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.
    5. Update the documentation with the detail that was determined during this phase.
    6. Apprise Senior Management of progress.
    7. Continue to notify affected Customers and Partners with relevant updates as needed.
    8. Move to Phase V, Follow-up.

10.2.5 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 SIR Form.
    1. Evaluate the cost and impact of the security incident to Ceresti 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.

10.2.6 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 Ceresti's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

10.3 Security Incident Response Team (SIRT)

Current members of the Ceresti SIRT:

- Security Officer
- Privacy Officer