Incident Response Policy

MolecularMatch 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 following-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.

Applicable Standards from the HITRUST Common Security Framework

- 02.f - Disciplinary Process
- 06.f - Prevention of Misuse of Information Assets
- 11.a - Reporting Information Security Events
- 11.c - Responsibilities and Procedures
- 11.a - Reporting Information Security Events

Applicable Standards from the HIPAA Security Rule

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

Incident Management Policies

The incident response process follows the process recommended by SANS, an industry leader in security (www.sans.org). Process flows are a direct representation of the SANS process.

I. Identification Phase

1. Immediately upon observation workforce members report suspected and known Precursors, Events, Indications, and Incidents in one of the following ways:
    1. Direct report to the Security Officer or Privacy Officer;
    2. Email to the Security Officer or Privacy Officer (can be anonymous);
    3. Phone call to the Security Officer or Privacy Officer (can be anonymous);
    4. The individual receiving the report facilitates completion of an *Incident Reporting Form (see below)* and notifies the Security Officer (if not already done).
    5. The Security Officer determines if the issue is a Precursor, Incident, Event, or Incident.
    6. 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 *Incident Reporting Form (see below)* 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 expertise is lacking in the area.
    7. 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 **V. Follow-up Phase**.
        3. If the issue is a technical security incident, commence to **II. Containment Phase**.
        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 documents 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 *Incident Reporting Form (see below)*. The intent of the Incident Reporting Form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
    8. The Security Officer, Privacy Officer, or appointed representative notifies any affected Customers and Partners. If no one was affected, notification is at the discretion of the Security and Privacy Officer.
    9. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary internal resources and consider any necessary

external assistance.

Note: Use the Incident Reporting Form;

II. Containment Phase (Technical)

In this Phase, our internal IT department attempts to contain the security incident via the security response technical team. It is extremely important to take detailed notes during the security incident response process. This will provide required evidence about the security incident that can be used 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 security response technical team 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 on the affected 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 Incident Reporting Form.
        2. Move to **V. Follow-up Phase**.
    8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to **III. Eradication Phase**.
    9. The individual completing this phase provides written communication to the SIRT.
4. Continuously update Senior Management of progress.
5. Continue to notify affected Customers and Partners with relevant updates as they occur.

III. 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 *Incdient Reporting Form and indicate eradication(see below)*.
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 **IV. Recovery Phase**.

Note: Use the online Incident Reporting Form;

IV. 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 security response 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). Monitor for proper behavior and note any anomalous 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. Monitor for proper behavior and note any anomalous behavior.
    5. Update the documentation with the detail that was determined during this phase.
    6. Notify Senior Management of progress.
    7. Continue to notify affected Customers and Partners with relevant updates as applicable.
    8. Move to **V. Follow-up Phase**.

V. 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 up to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resources) 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, 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.

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 our expectations for them, relative to security responsibilities. The incident response plan is tested annually.

Security Incident Response Team (SIRT)

Individuals needed and responsible to respond to a security incident make up a Security Incident Response Team (SIRT). Members may include the following:

- Security Officer
- Privacy Officer
- Senior Management
- VP of Engineering
- Security Experts