Disaster Recover Policy

The MolecularMatch Contingency Plan establishes procedures to recover following a disruption resulting from a disaster.

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - *Notification/Activation phase* to detect and assess damage and to activate the plan;
    - *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
    - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out essential activities during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to our systems.
4. Assign responsibilities to designated Operating Division (OPDIV) personnel and provide guidance for recovering all systems during prolonged periods of interruption to normal operations.
5. Ensure coordination with other internal staff who will participate in the contingency planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

This Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This Contingency Plan is promulgated under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

This Contingency Plan complies with the OPDIV IT Contingency Planning Policy as follows:

> *The organization shall develop a contingency planning capability to meet the needs*

of critical supporting operations in the event of a disruption extending beyond 48 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987;
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000;
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998;
- PDD 63, Critical Infrastructure Protection, May 1998;
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, and internal malicious activities.

There are two defined categories of systems from a disaster recovery perspective:

1. **Critical Systems**. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored as soon as possible.
2. **Non-critical Systems**. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent *Critical Systems* from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(i) - Contingency Plan

Line of Succession

OPDIV sets forth an order of succession to ensure that decision-making authority for this Contingency Plan is uninterrupted. The Chief Technology Officer (CTO), Security Officer (SO), and VP of Engineering are responsible for ensuring the safety of personnel and the execution of procedures documented within this Contingency Plan. If any of these three are unable to function as the overall authority or they choose to delegate this responsibility to a successor, the Chief Executive Officer (CEO) or Chief Operating Officer (COO) shall function as that authority. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

1. **Nick Tackes**, CTO/SO: 949-573-5288, ntackes@molecularmatch.com
2. **Ryan Smith**, VP Engineering, ???-???-????, rsmith@molecularmatch.com
3. **Kevin Coker**, CEO: 501-319-4156, kcoker@molecularmatch.com
4. **Collin Brack**, COO: 409-939-3941, cbrack@molecularmatch.com

Responsibilities

The following team have been developed and trained to respond to a contingency event affecting the IT system.

1. The **Technical Team** is responsible for recovery of the hosted environment and coordinating with the hosted platform as a service (PaaS) provider currently being used to host the web and data servers. It is also responsible for testing redeployments and assessing damage to the environment. Members of the team include personnel who are also responsible for the daily operations and maintenance of our systems. The team leader is the Chief Technology Officer.

Testing and Maintenance

The CTO and VP of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency

Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Tabletop Testing

Tabletop Testing is conducted in accordance with the CMS Contingency Planning Tabletop Test Procedures. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the Contingency Plan in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis; and
- Crisis communications and call tree verification.

Technical Testing

The primary objective of the technical test is to ensure the communication processes, data storage, and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch voice and data telecommunications to alternate processing site.

1. Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to vital systems. Based on the assessment of the Event, sometimes according to the Incident Response Policy, the Contingency Plan may be activated by either the CTO or VP of Engineering.

Contact information for key personnel is listed above. The notification sequence is listed below:

- The first responder is to notify the CTO. All known information must be relayed to the CTO.
- The VP of Engineering is to contact the rest of the Technical Team and inform them of the event. The CTO is to instruct all Team Leaders to begin assessment procedures.
- The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to assess as best possible to gather the most information to come to the best conclusion about how best to proceed.

    - **Damage Assessment Procedures:**
        1. The CTO and VP of Engineering are to logically assess damage,
        2. Gain insight into whether the infrastructure is salvageable, and
        3. Begin to formulate a plan for recovery.
- The Contingency Plan is to be activated if one or more of the following criteria are met:
    - A key system will be unavailable for more than 48 hours.
    - Hosting facility is damaged and will be unavailable for more than 24 hours.
    - Other criteria, as appropriate and as defined by the CTO.
- If the plan is to be activated:
    1. The CTO is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
    2. Upon notification from the CTO, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond or relocate if necessary.
    3. The CTO is to notify the hosting partners that a contingency event has been declared and to send the necessary materials (as determined by damage assessment) to the alternate site.
    4. The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
- Notifications are allowed to be sent by phone, email, or text message.

2. Recovery Phase

This section provides procedures for recovering the application at an alternate site, while other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the critical systems at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild critical systems to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected.
2. Assess damage to the environment.
3. Begin replication of new environment using automated and tested scrips.
4. Test new environment using pre-written tests.
5. Test logging, security, and alerting functionality.
6. Verify systems are appropriately patched and up to date.
7. Deploy environment to production.
8. Update DNS to new environment.

3. Reconstitution Phase

This section discusses activities necessary for restoring operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate to the main site.

1. **Main Site Restoration** (original or new site)
    - Begin replication of new environment using automated and tested scrips.
    - Test new environment using pre-written tests.
    - Test logging, security, and alerting functionality.
    - Deploy environment to production.
    - Verify systems are appropriately patched and up to date.
    - Update DNS to new environment.
2. **Plan Deactivation**
    - If the environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the Media Disposal Policy.