Vulnerability Scanning Policy

MolecularMatch is proactive about information security and understands that vulnerabilities need to be monitored on an ongoing basis. This policy, and associated procedures for vulnerabilty scanning detection, has been subcontracted to a third-party, Platform as a Service, HIPAA compliant vendor (PaaS Subcontractor). We have verified that their policies and procedures meet or exceed our standards and those of HIPAA and the HITRUST Common Security Framework. The PaaS Subcontractor currently utilizes OSSEC and Nessus Scanner.

Proof of such due diligence is kept by the Security Officer.

Applicable Standards from the HITRUST Common Security Framework

- 10.m - Control of Technical Vulnerabilities

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) - Evaluation

Vulnerability Scanning Policy

Combined OSSEC and Nessus Scanner enable detection, identification, and remediation of vulnerabilities on our systems as well as logging and file integrity checking. Intrusion detection is covered in the **Intrusion Detection Policy** and file integrity is covered in the **Data Integrity Policy**.

We are responsible for:

- Reviewing generated reports from OSSEC and Nessus on a monthly basis by the Security Officer.
- Retaining all vulnerability scanning reports for 6 years by the Secrity Officer.
- Investigating into discovered vulnerabilities by the Security Officer.
- Coordinating with the PaaS Subcontractor to respond to any discovered vulnerabilities.
- In the case of new vulnerabilities, the following steps are taken:
    - All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.

  - Vulnerabilities that are repeatable manually are documented and reviewed by the Security Officer, VP of Engineering, and Privacy Officer to see if they are part of the current risk assessment performed.
    - Those that are a part of the current risk assessment are checked for mitigations.
    - Those that are not part of the current risk assessment trigger a new risk assessment, and this process is outlined in detail in the **Risk Management Policy**.

PaaS Vendor is responsible for:

- Management of Nessus and OSSEC.
- Monitoring with Nessus all all internal IP addresses (servers, VMs, etc) on the network.
- Scanning on a weekly basis and after every production deployment.
- Reviewing Nessus reports and findings, as well as any further investigation into discovered vulnerabilities.
- Retaining all vulnerability scanning reports for 6 years.
- Regularly performing penetration testing as part of the vulnerability management policy.
  - External penetration testing is performed bi-annually by a third party.
  - Internal penetration testing is performed quarterly.
  - Gaps and vulnerabilities identified during penetration testing are reviewed, with plans for correction and/or mitigation, by the PaaS Subcontractor's Security Officer.
  - Penetration tests results are retained for 6 years.

Note: Vulnerability and penetration test findings and mitigations are documented using this form.