Employees Policy

MolecularMatch is committed to ensuring all workforce members actively address security and compliance in their roles. As such, training is imperative to ensure an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

Applicable Standards from the HITRUST Common Security Framework

- 02.e - Information Security Awareness, Education, and Training
- 06.e - Prevention of Misuse of Information Assets
- 07.c - Acceptable Use of Assets
- 08.j - Controls Against Malicious Code
- 01.y - Teleworking

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) - Security Awareness and Training

Employment Policies

1. **Workforce Training**
    1. Records are kept for all training by the Security Officer, Privacy Officer, or designated Compliance or Training manager.
    2. Training is conducted either in person, in a webinar, or by a training manual.
    3. All new workforce members within 60 days of employment receive training on:
        - Security policies and procedures, including operations security.
        - HIPAA including HIPAA reporting requirements, the ability to anonymously report security incidents, and the levels of compliance and obligations for the company, its Customers, and its Partners.
        - Responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices, and social media usage.
        - Remote (teleworking) workforce training including the risk, the controls implemented, their responsibilities, and sanctions associated with violation

of policies.

2. **Related Policies**
    1. All workforce members are granted access to formal organizational policies, including the sanction policy for violations.
    2. Employees are directed to the *System Access Policy* for information and forms to either gain access to internal systems or to modify existing access.
    3. Employees are directed to the *System Access Policy* section titled *Employee Workstation Use* to be educated and confirm they are using their workstations and other provided equipement appropriately.
    4. Employees are directed to the *Approved Tools Policy* to verify that they are educated and in compliance with approved tools.
3. **Connecting to Production Environments**
    1. No mobile devices are allowed to connect to any production environment.
    2. All access to production systems is accmplished through remote secure connections. Workforce members are trained to use VPN (when available), but to otherwise use as a minimum SSH and SFTP access.
4. **Employee Travel**
    1. Employees traveling to high risk areas, including all international travel, for business reasons are to speak with the Security Officer prior to travel and upon completion of travel.

Note: Upon completion of training, workforce members complete this form.