Security Awareness and Training Policy

- Date of Issue April 2015
- Date of Review
- Purpose
The Awareness and Training Policy will define the standards for security training that all employees receive to ensure that the entire organization supports a safe computing environment. It is the belief of Mount Sinai Health System that a secure computing environment is the responsibility of all users, not just a single department. To facilitate this Mount Sinai Health System supports training for all users annually to refresh as well as update previous training on the basics of security awareness and emerging threats.

- Scope;
This policy will apply to all of Mount Sinai Health System and its associated entities.

- Roles and responsibilities;
  - Management will:
    - Oversee implementation of this policy.
    - Ensure that exceptions to this policy are documented with Information Technology Security.
    - Provide training, in conjunction with Information Technology Security, to their constituents.
  - Information Technology Security will:
    - Maintain this policy in accordance with NIST guidelines to benefit the Mount Sinai Health System.
    - Review the policy, its articles and procedures annually or as is deemed necessary.
    - Support training activities having to do with this policy.
  - Application Owners will:
    - Establish classifications (PHI/PII) of data stored, processed or moved through systems.
    - Ensure that data handling controls are implemented and followed.
  - Authorized Users will:
    - Only access authorized systems and data.
    - Only assume privileges for which they are authorized.
    - Protect the systems, or information contained on systems, at the level in which it has been classified.
    - Share access to the system, or information contained within, with only authorized personnel.
    - Report any suspected, or actual, un-authorized access to their management team.
- Reference

MSH HIPAA ACS-SMP.5
CHP Security Policy HS-005 / HS-005.1

- Policy

Mount Sinai Health System requires all information system users in an administrative role to complete security awareness training annually in order to maintain their access to Mount Sinai Health System information systems. These training requirements must be completed before performing assigned duties and when required by regulatory changes. These trainings must be repeated annually to ensure compliance.

When employees take part in the Mount Sinai Health System's New Beginnings seminar at the start of their employment they attend training with personnel from the security group and the fire safety group. This training will outline the hospital's utilization and operation of environment controls. If/when employee changes area within the campus training should be with a focus on the specifics of the new area they will work in. Refresher training for each area will be run by the resident departments in a local area annually.

In the event that a user has been identified as being in possession of a system compromised by malware, training may be assigned to impart a greater understanding of specific threats to mitigate future instances of malware incidents.

All training sessions that are attended as a result of this policy will be recorded by either the New Beginnings orientation team or by the employee’s direct supervisors. Initial training conducted through New Beginnings is recorded as attendance in the seminar. All role based or access based training will be recorded by the direct supervisor and kept on record for no less than two calendar years.

At least annually the Security Awareness and Training policy will be reviewed and updated by management to ensure its continued effectiveness. Otherwise, in the event that significant regulatory change occurs, the policy will be reviewed and updated as needed to ensure compliance.