Security Assessment and Authorization Policy

- Purpose
The Security Assessment and Authorization Policy will define the practice of assessing assets owned or operated by The Mount Sinai Health System. Because no two systems are alike, this policy and procedure package can never be a step by step guide. However, the goal is to establish a standard for documentation and record keeping that, overtime, will form a complete view of the organization. The versatility of this set of documents will also allow for the evolution of our process despite emerging threats and while maintaining conformity in documentation and therefore clarity of results.

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

- Roles and responsibilities;
  o Management will:
    o Oversee implementation of this policy.
    o Ensure that exceptions to this policy are documented with the Information Technology Security Department.
    o Provide training, in conjunction with the Information Technology Security Department, to their constituents.
  o The Information Technology Security Department will:
    o Maintain this policy in accordance with NIST recommendations.
    o Review the policy, its articles and procedures annually or as is deemed necessary.
    o Support training activities having to do with this policy.
  o Application Owners will:
    o Establish classifications (PHI/PII) of data stored, processed or moved through systems.
    o Ensure that data handling controls are implemented and followed.
  o Authorized Users will:
    o Only access systems and data to which they are authorized.
    o Only assume privileges for which they are authorized.
- Policy

At least annually The Mount Sinai Health System assesses the security controls for Health System controlled information systems to determine if the security controls are implemented correctly, operating as intended, and producing the desired outcome throughout the environment. At the end of all standard security assessments, IT Security Risk produces a report that documents the results and delivers that report to all impacted management personnel. The report will include, at the minimum:
- Found vulnerabilities
- Recommendations for changes to the configuration of information systems and/or their constituent components.
- A determination of the impact of recommended configuration changes to the information systems and environment of operation.
- A Proposed Plan of action and Milestones for the remediation for found vulnerabilities.

The Mount Sinai Health System identifies connections to vendor's information systems and monitors the connections for appropriate access as defined in the service contract of the vendor. The Mount Sinai Health System also monitors the information system connections on an ongoing basis to verify enforcement of security requirements and the nature of the information communicated.

The Mount Sinai Health System has established a continuous monitoring strategy and program that covers all locations and departments. Quarterly scans are conducted on business critical applications to ensure patching and remediation of vulnerabilities. In addition, The Mount Sinai Health System has annual 3rd party audits completed on financial applications. This is to ensure continuing compliance with all regulatory guidelines as well as randomized internal audits on all applications not included as critical.

The Mount Sinai Health System defines the acceptable normal forms of security testing to be included in security control assessments as in-depth/continuous monitoring, manual checks, network scans, penetration testing, personnel interviews, and social engineering. Any combination of these strategies considered necessary to evaluate internal systems or processes will be conducted on an annual basis and may be changed as needed to reflect the emerging threat model against general health organizations. To effectively test all aspects of our organization, tests may not be announced to all
employees if prior knowledge is determined to be a contributing factor in personnel performance. Records of all security control assessments will be maintained by IT Security Risk.

Once annually Mount Sinai Health System IT Security Risk Team reports the Security State of the information environment to organizational officials in conjunction with the 4th quarter IT Scorecard. The report is delivered to all Information Technology Associate Directors and above through to the CIO. The report will include details of the continuous monitoring program for The Mount Sinai Health System that includes:
- Reports from suspected and actual incidents occurring since the preceding Security State report;
- Major changes to the configurations of the information systems and their constituent components;
- A determination of the security impact of configuration changes to the information systems and environment of operation; and
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

The Mount Sinai Health System also employs independent assessors and assessment teams to monitor the security controls in place for the organization on an ongoing basis. We have many independent auditing activities throughout the year including audits of our financial systems, independent vulnerability assessments, and reviews by the Joint Commission.

At least annually the Security Assessment and Authorization 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.