System Information and Integrity Policy

- Purpose
The Mount Sinai Health System recognizes system updates and remediation as needing to be approved by the corporate change management process. This document describes many centrally managed processes that add to the Information Technology infrastructure.

- Scope;
This policy will apply to all of 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 Information Technology Security.
    o Provide training, in conjunction with Information Technology Security, to their constituents.
  o Information Technology Security will:
    o Maintain this policy in accordance with NIST guidelines to benefit the Mount Sinai Health System.
    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 authorized systems and data.
    o Only assume privileges for which they are authorized.
    o Protect the systems, or information contained on systems, at the level in which it has been classified.
    o Share access to the system, or information contained within, with only authorized personnel.
    o Report any suspected, or actual, un-authorized access to their management team.

- Policy
Through the use of teams of operating system experts, the Mount Sinai Health System centrally manages the system updates and remediation process by requiring all changes affecting the systems to be approved by application owners and the relevant support teams. The Mount Sinai Health System
Department of Information Technology

does not install updates automatically. All updates go through the change management and quality assurance processes.

The Mount Sinai Health System defines the frequency of scans to detect deficiencies for remediation in the Security Assessment and Authorization policy.

The Mount Sinai Health System utilizes perimeter/boundary security mechanisms. In addition to these mechanisms, additional security technologies are installed within the infrastructure.

The Mount Sinai Health System updates malicious code protection signatures as defined in the System and Information Integrity Guidelines.

The Mount Sinai Health System centrally manages security mechanisms where feasible as described in the System and Information Integrity Guidelines.

The Mount Sinai Health System monitors communications for unauthorized activities as described in the System and Information Integrity Guidelines.

Mount Sinai Health System incident responders endeavor to take the least disruptive measures possible to correct incidents in support of continuity and operations aligning with business objectives.

The Mount Sinai Health System receives security updates and advisories from external organizations. From these pieces of information, if necessary, internal alerts may be issued to staff.

The Mount Sinai Health System implements protection against spam both entering and exiting our network. Spam protection mechanisms are centrally managed by the Mount Sinai Health System Information Technology Department.

The Mount Sinai Health System discourages saving work items to local disk. Employees are encouraged to save working items to their home drive so that it can be backed up automatically.

Through the use of data loss prevention mechanisms and back ups The Mount Sinai Health System handles and retains information in accordance with applicable federal laws, regulations, and operational requirements.

At least annually the System and Information Integrity 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.