Title: Information Technology - Security Risk Management Program - Policy

I. Policy Statement
   a. An IT Security Risk Management program will be developed, implemented and managed by the MUHS Risk Assessment Committee. The Risk Assessment Committee (RAC) will be comprised of:
      i. the MUHC Chief Information Officer (CIO)
      ii. the MUHC Chief Medical Information Officer (CMIO)
      iii. the SOM Sr. Assoc. Dean for IT
      iv. the MUHS Chief Compliance Officer (CCO)
      v. the MUHS Chief Privacy Officer (CPO)
      vi. the MUHS Information Security Officer (ISO)
      vii. Additional MUHC, School of Medicine (SOM), School of Nursing (SON), School of Health Professions (SHP) administration and/or compliance officers as appropriate
      viii. The Program will provide mechanisms and processes.

II. Definitions
   a. Not applicable.

III. Process/Content
   a. Establishing and maintaining an inventory of IT systems and applications that create, modify, store or transmit data of the health system regardless of whether those IT systems and applications are managed by UMHS or are provided by a 3rd party. (responsibility of the Tiger Institute)
   b. Reviewing IT systems and applications to identify vulnerabilities and their potential impact on the availability, integrity and privacy of UMHS IT resources and data. (responsibility of the Tiger Institute and MU Information Security Team)
   c. Ensuring that identified risks are eliminated or mitigated as directed by the RAC. (responsibility of the Tiger Institute and MU Information Security Team)
Title: Information Technology - Security Risk Management Program - Policy

d. Maintain all documentation related to the risk management program and provide reports as needed. (responsibility of the MU Information Security Team)

IV. Attachments
   a. Not applicable

V. References, Regulatory References, Related Documents, or Links
   a. Joint Commission Hospital Manual, Information Management 02.01.03