Cyber Essentials Policy Exhibit 1

Exhibit Summary

The HMS Cyber Essentials policy and program features best-of-breed software applications to establish a baseline security posture for all systems that connect to a non-public HMS network. At a high level, these applications fall into the following categories:

- Systems management software
- Anti-virus software
- Backup software
- Next-generation endpoint protection software

These application categories represent a full suite of protections against the most common forms of attacks that are focused on individuals and end point systems.

Systems management software is the best way for HMS IT to keep systems up to date with software patches and to enforce University and school requirements around passwords, locking screen savers, encryption, and more.

Anti-virus software is essential for keeping systems free of known viruses and malware.

Backup software helps to protect against all forms of data loss, from accidental deletion of files or data, to ransomware attacks which make data unavailable.

Next-generation endpoint protection software takes its place among more traditional protections such as anti-virus by filling a void in protection. While anti-virus is very good at protecting against known viruses and other malware, it fails against attacks that use unknown malware or, as we see with more sophisticated attacks, use known good tools to gain unauthorized access to sensitive systems. By using machine-learning and behavioral analysis, next-generation end point protection tools are extremely effective at alerting us to intrusions and other forms of attack that would go undetected using more traditional means of protection.

Additionally, HMS IT has standardized a naming convention that will help to identify where an endpoint is located and who owns the system. Full details of the naming convention may be found on the naming convention collaboration page.

Exhibit Detail

Harvard Medical School Information Technology has standardized on the following specific software applications as part of the Cyber Essentials Suite of tools designed to keep end points safe:

- Casper and LANDesk: Systems management software applications for OS X and Windows, respectively
- CrashPlan Pro: Backup software
- ESET: Anti-Virus/Anti-Malware software
- CrowdStrike: Next-generation end point protection software
• Naming Convention: To ease the process of finding systems and tying them to individuals, labs, or departments, HMS IT is also requiring that systems be named in such a way as to make them consistent and identifiable based on factors such as, location, device type, department, asset ID, and workgroup. Full details of the naming convention may be found on the naming convention collaboration page.

Review Period
Annual

Related Resources/ Referral Links
• HMS IT Cyber Essentials Policy

Revision History
December 6, 2016: Version 1

Key Words/Tags
IT, Security, Cyber Essentials, End Point, CrowdStrike, CrashPlan, ESET, Anti-virus, Anti-malware, backup, recovery, Systems Management Software, Casper, LANDesk, Portal, Self Service