APPENDIX A
Minimum Security Standards for Computer Systems

1. **Purpose:** Adherence to minimum security standards for computer systems is critical to the protection of institutional information assets as well as the operational integrity of the university's information technology infrastructure. The standards outlined by this section cover the configuration and maintenance requirements for systems on the Mississippi State University (MSU) network.

2. **Scope:** Certain security configurations and standards are required for all systems that connect to the Mississippi State University data network. Additional operation and configuration standards are required where data is classified using the MSU data classification program.

3. **Authority:** The Policy and Procedure for Use of Computing and Network Resources at Mississippi State University (OP 01.12), requires users or administrators of computers systems to maintain the security of computing resources.

4. **Standards:** Software obsolescence is a critical problem for computer system security. All network attached systems should have a supported operating system installed which is current with all security patches. Obsolete or unsupported systems must not be used for communication beyond the local network.

   The following table outlines the minimum security standards for computer systems based upon the category of data stored on the system, as defined in the Data Classifications and Individual Responsibilities section of the Information Security Program. Category I data is protected specifically by law or by Mississippi State University policy. Category II data is not otherwise protected by statute, regulation, or policy, but could do harm to the university and its reputation if inappropriately released. Category III data is public information.

#	Configuration	Cat I	Cat II & III
1	All critical security patches should be applied. Updates set to download automatically for Microsoft OS and Mac OS	Required	Required
2	Anti-virus software must be installed and enabled with live update where practicable	Required	Required
3	Network Firewall protection for servers	Required	Required
4	Workstation access protected by login and password (excluding public access systems such as kiosks)	Required	Required
5	Workstation inactivity triggers password protected screen saver (excluding public access systems such as kiosks)	Required (20 min max)	Required (60 min max)
6	Host-based Firewall protection	Recommended	Recommended
7	Anti-spyware protection	Recommended	Recommended
8	Laptop and "flash drive" Whole Disk Encryption	Required	Recommended
9	Legacy protocols such as Telnet, FTP, pop, imap which do not encrypt passwords should be replaced with secure alternatives such as SSH, SFTP, pops, imaps (dedicated network devices such as printers excluded) Standard http auth should be replaced with https SSL protection	Required	Recommended
10	Services, applications and user accounts not in use should be disabled or uninstalled	Required	Recommended
11	Systems must be physically secure or encrypted with restricted access	Required	Recommended
12	Data backup must take place on a regular basis, with secure storage of media	Required	Recommended
13	System integrity checks performed on a regular basis, including backup media verification	Required	Recommended
14	System logging enabled and reviewed	Required	Recommended
15	Proactive vulnerability scans	Required	Recommended
16	SSL certificates should be from a recognized authority.	Required	Recommended
17	Enterprise passwords must be protected by encryption during use and encrypted at rest.	Required	Required

5. **Summary:** Use of Mississippi State University's computer and network resources is not a matter of right, but rather all use of Mississippi State University's computer and network resources must be consistent with the mission of the university in support of public education, research, and public service. Minimum standards for system configuration and maintenance allow for the protection of university data, the protection of other systems connected to the university network, and help prevent the improper use of campus resources.