APPENDIX B
End User Best Practices

1. **Critical Security Patches:** Operating system patches should be loaded automatically. Microsoft Windows provides "Automatic Update" to automatically download and install patches on a schedule. Best practice would be to do this daily to insure that all critical updates and service packs are installed in a timely manner. Apple Macintosh users under OSX are provided with "Software Update" where OSX checks for operating system updates may be scheduled. Software such as media players, browser plug-ins, office applications and others are often overlooked but can have significant security issues and must be patched regularly.

2. **Viruses:** As required by MSU Policy 01.12, personal computers must be protected by anti-virus software and virus definitions must be kept current. Best practice is to enable the automatic update service for daily updates. Anti-virus software that has expired is of little value and must be replaced. ITS provides, at no charge, Sophos Anti-Virus which is available at http://www.its.msstate.edu, under the software downloads sections.

3. **Firewalls:** The MSU campus network is protected from external threats by a system of firewalls. However, attacks can originate from computers within the MSU campus network (e.g., a roommate's infected PC). Best practice recommends use of a host firewall product to guard against this level of threat. Modern operating systems such as Windows and OSX provide reasonable firewall services.

4. **File Sharing:** Peer to Peer (P2P) file sharing software can provide a method of entrance for many types of infected and prohibited software and an exposure risk to University data. Users should be aware of the university acceptable use policy MSU Policy 01.12 and read http://filesharing.msstate.edu for additional information before usage of any P2P software on university owned equipment.

5. **Spyware:** Spyware is another category of malicious software that must be guarded against. ITS recommends the free Spybot – Search and Destroy product available at http://www.its.msstate.edu, under the software downloads section. Other free products such as Microsoft Windows Defender or commercial products such as Malwarebytes are also available.

6. **Passwords:** Per MSU Policy 01.12, passwords should be obscure, hard to guess, changed regularly, and never shared. Avoid using words found in the dictionary and obvious passwords like the name of a pet or family member. Strong passwords contain a mixture of upper and lower case letters, numbers, and special characters. A good, memorable password might be formed from

the letters of a phrase along with some special characters. For example, "My dog Spot is a great dog" could yield the password MdSiaGd! **WARNING:** As noted above, the sharing of passwords is a violation of university policy and could result in disciplinary action being taken.

7. **Awareness:** Users should be aware of sensitive data that may exist on their computers. Tools such as Cornell "Spider" can help find some sensitive data that might be stored inadvertently. This free software is available at http://www.its.msstate.edu, under the software download section.

8. **Email:** Users must be aware that email typically transmits information in "clear" text and should never be used to send unencrypted sensitive data. Always be careful of links and never respond to requests for personal information. http://www.infosecurity.msstate.edu/faqs/

9. **Web Space:** Sensitive data must never be stored in a publicly accessible Web space. Even if no direct link to the information exists, search engines and Web "crawlers" can discover such information and enable direct access to it from anywhere on the Internet.

10. **File Storage:** ITS provides general purpose network storage for units that it supports. The J:\Everyone folder is shared by the entire unit, and everyone in the unit can access documents stored in that folder. You should be aware of this and understand that ITS can also provide restricted access, shared folders on the J: drive. Other units may also provide network file storage, and users in those units should understand who has access to the files stored thereon.

11. **Cloud Services: As the popularity of cloud-based services** such as Dropbox.com, Google, Box.net, Amazon, and iCloud grows, users should exercise caution when storing or transmitting information with any cloud service. Consider legal, regulatory, and University policy requirements in areas such as:

    - FERPA and HIPPA
    - Grant restrictions
    - Human Subject restrictions
    - Intellectual Property restrictions
    - Export restrictions
    - Data Classification of information.

12. **Paper Shredding:** Always shred documents containing sensitive information when disposing of them, and use a cross-cut or high security paper shredder instead of the more common strip-cut shredder. Use of a cross-cut or high security shredder makes it virtually impossible to reconstitute a document from its shredded remains.

13. **Purchases:** Employees should consult with their local information technology support staff about security considerations when evaluating new IT goods and services.

14. **Software:** Be careful what you install on your work machine. Many users say "Yes", to all options when installing software and end up with additional "toolbars", multiple anti-virus packages or other extraneous software that will often conflict with existing software.

15. **Backup:** Users should store critical files on network folders where regular backup is provided by their unit's information technology support staff. Users should protect their mobile devices from theft and make sure that data stored on these devices is being backed up regularly.

16. **Encryption:** Sensitive data should never be transmitted across the network without encryption. SSL is a method used to protect data passed between a web browser and web server and is identified via the "lock" symbol on your browser. Web pages that collect or display sensitive data and everywhere you login via the web should be protected via encryption. SSH is a secure replacement for protocols such as TELNET and FTP. It uses strong encryption to protect the data transfer between a client computer and a server.

17. **Disk/File Encryption:** Sensitive data should not be carried on a portable electronic device such as a jump drive or laptop that could easily be lost or stolen. However, in situations where this is a requirement, the sensitive data must be encrypted. On mobile systems such as laptops the best practice is to encrypt the entire hard drive via whole-disk encryption software. **WARNING: Installation of whole-disk encryption software should only be done after consultation with your IT support person. As a precaution, it is recommended that you make a copy of your hard drive before installation. Losing the decryption key will lose all data.** Unit supervisors are responsible for maintaining all decryption keys in secure locations in the event of an emergency. Further information about campus-supported disk encryption products can be found on the ITS webpage at http://www.its.msstate.edu/software/dept/.

18. **VPN Remote Access:** A Virtual Private Network (VPN) provides a secure encrypted network connection over the Internet between a workstation and a private network. ITS provides VPN services to faculty and staff to enable access to restricted services. Best practice restricts certain services to campus address ranges. Examples include remote desktop control or remote management (SSH) access.