Travel Guidelines for Safe Computing – Personal Checklist

This document contains precautionary measures that travelers should follow to help safeguard sensitive data when travelling to any destination, foreign or domestic. Review this list before traveling, and refer to the related sections in the accompanying document for detailed explanations. This document is intended as a guide to best practices, and does not constitute actual legal advice. For legal questions about these guidelines, please contact an appropriate legal professional.

Before you travel:

If a loaner laptop is available through your department, consider traveling with a sanitized, virus free, fully updated loaner laptop with minimal software, and take only what you need for your work while leaving your primary computer at home.

Remove unneeded sensitive data from computers, laptops, and personal electronic devices such as cell phones, iPods, and hand held organizers.

Confirm that your laptop computer has working antivirus and anti-spyware software, and that they are up to date. Run the latest updates for your operating system (Windows XP, Windows Vista, Mac OS, etc), any third party browsers you use (Firefox, Chrome, Opera), and patch all 3rd party application software.

Make backups of important data that will travel with you, and leave the backups behind at a secure location. This applies to your laptop computer, iPods, USB storage, and cell phones which contain information you want to protect.

Password protect all your devices, including your cell phone, and use strong passwords.

Please contact the office of Export Controls at MSU for important information regarding restrictions on the use of encryption software and other security technologies outside of the US. Use encryption on files which may contain sensitive data. This applies to your portable computer, as well as removable USB drives, iPods, hand held organizer, or other portable device where files can be stored.

Disable remote connectivity features you aren't using. Turn off Bluetooth, file and print sharing, and any other wireless functions which could be used to surreptitiously access your device.

While you travel:

Avoid the use of kiosk computers, or computer workstations in public places or commercial businesses (kiosks, Internet cafes, etc.) Never use them to login to or access systems which contain sensitive or personal data.

Always use the MSU VPN service, or other Virtual Private Network service to encrypt your communications traffic when you connect to MSU from any network., whether you are using a wired or wireless network. Avoid using networks which require you to download software onto your computer for access.

Remember that you have no reasonable expectation of privacy when using your computer in a public place. Use a privacy screen or other device to obscure your display to prevent anyone nearby from observing your work.

Always decline any request from someone you don't know to use your laptop, hand held computer, or cell phone. If you are required to surrender your devices for any reason, always check them for viruses and malware before using them for any work. Avoid allowing others to connect USB or portable devices to your laptop, and don't connect your devices to an unknown computer.

Maintain physical possession of your computer and personal electronic devices, and activate any anti-tampering or automatic disabling features available. Do not leave devices unattended in hotel rooms or hotel safes. Avoid allowing others to connect USB or portable devices to your laptop.

When you return:

Assume the worst: that your computer hard drive may need to be erased and rebuilt, so back up and remove the data you need from the computer before inspecting it. Check your computer and personal electronic devices for spyware, malware, and viruses before reconnecting to the campus or departmental networks. Don't use USB drives or software you received as gifts or promotional items until they have been examined by your IT group for viruses.