Travel Guidelines for Safe Computing – Detail Document Outline

TABLE OF CONTENTS:

Travel Guidelines for Safe Computing – Detailed Information Draft

Below are precautionary measures that travelers should follow to help safeguard sensitive data when traveling to any destination. This document provides additional information regarding the items in the Travel Guidelines for Safe Computing – User Checklist. While many of the steps listed here can be performed by a computer savvy individual, please contact your technology support department if you need assistance with any of the guidelines found in this document. If you do not have an in-house technology support service, contact MSU Academic Technology Services Help Desk for assistance with any of these issues.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:

Why take the risk with your primary computer when traveling if a loaner laptop is available? Some departments may have one or more laptops available to loan you when traveling. A properly prepared loaner laptop can provide you with all of the applications you need for your work, and only the data you need while traveling. If the loaner is damaged physically, or by viruses, your primary computer is still in top working order, back at your office. A sanitized laptop should have all updates applied, and contain only installed software you will need for your work. Windows Disk Cleanup should be run to remove any temporary files from the system, and all browser caches should be cleared. Taking only what you need for your work, while leaving your primary computer at home, can be the best first step to safeguarding your computers and data.

Everyone working today has may options for storing critical data. Computers and laptops are an obvious place to store data, but it is easy to forget that cell phones, smartphones, iPods, handheld organizers, and USB storage drives can all hold data considered sensitive, as well as data critical for your work. All of these devices could be misplaced, lost, damaged, stolen, or confiscated during the course of travel. While most people don't even think twice about loading up a USB drive with work related data, it is important to consider them as a potential target for data theft. Always remove unneeded sensitive data from computers, laptops, and personal electronic devices such as cell phones, iPods, and handheld organizers.

New viruses, spyware, malware, worms, trojans, and now network bots are invented and distributed on the Internet every day. Even the simple act of viewing a web page can cause some types of malicious programs to download onto your computer. Confirm that your laptop computer has working antivirus and anti-spyware software, and that they are up to date. In order to combat the continuous threat that malicious software represents, it is vital to keep not just antivirus, but software up to date on your computers. You should always run the latest updates for your operating system (Windows XP, Windows Vista, Mac OS, etc), and confirm that they have installed correctly. Check for manual or automatic update features on all Internet browsers you use (Firefox, Chrome, Opera) and apply the latest updates. Finally, every application software installed on your system may have vulnerabilities which could be addressed by patches or updates from the manufacturer. Check the programs you plan to use during your travels, and if they have an update option, run it to install the latest updates. Continue to regularly check for updates while you travel, and install critical updates while you are on the road. Keep your software up to date while you travel, and scan regularly for malicious software as you move from one network to another.

Finally, obtain a Virtual Private Network (VPN) software client for your computer. A VPN client allows you to create an encrypted network connection from your computer back to your network at the university. Your department may have their own VPN system and client software, so ask your technology contact for more information. If a departmental VPN is unavailable, contact MSU Academic Technology Services for additional information about the MSU network VPN, available to encrypt connections between a remote location and the campus network. See the link in the appendix for more information on the MSU VPN service. Once it is installed, test it from home or another location before you leave on your trip. Make certain you can create a VPN connection to the resources you need on the campus network before you

are forced to do it from your travel destination. In addition, make certain all VPN configuration information is correct and verified before you leave.

Computer professionals cannot stress this point enough: create backups of critical data. Don't take the only copy of a file or a document with you without making absolutely sure you have a backup copy left behind. Make backups of important data that will travel with you, and leave the backups behind at a secure location. This applies to EVERY device where you store data. After you backup your laptop, don't forget to backup the data on your iPod, cell phones, smart phones, hand held organizers, and USB storage devices. For some, losing all the contacts and memos on your cell phone could be just as critical as losing a laptop hard drive full of critical data.

Passwords are an easy way to provide additional protection. Password protect all your devices, including your cell phones and handheld devices, if you store any data on them you want to protect. You should always use strong passwords, and avoid writing them down anywhere. Strong passwords should always include a mix of upper and lower case letters, numbers, and special characters. Strong passwords should not include words, or contain any common information about you that could be obtained publicly (don't use your name, family members names, address or phone information, etc.)

Contact the office of Export Controls at MSU for important information regarding the Federal 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, handheld organizer, or other portable device where files can be stored. If you are planning travel outside the United States, there may be specific restrictions on the types of encryption you can take into some countries. If you plan on using encryption or other security technology on any of your devices, contact Export Controls for the most current guidelines and recommendations.

It is a fairly common practice for manufacturers to turn on every available feature on devices they sell. This applies to laptop computes as well as cell phones, smart phones, and other hand held organizers. Examine your devices closely for features that provide remote connectivity that you aren't using, like Bluetooth, or InfraRed (IR) ports. Disable all 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 without your knowledge as you travel. If you are unsure what features are enabled, contact a technology professional, or in the case of wireless devices, contact your cell service provider for assistance.

While you travel:

Having followed all the recommendations in the first section of the document, you are now prepared to travel. There are additional security concerns you need to be aware of while traveling.

Avoid the use of kiosk computers, computer workstations in public places like libraries or municipal buildings, and computers in commercial businesses (kiosks, internet cafes, public libraries,etc.) Never use them to login to or access systems which contain sensitive data, or University systems containing sensitive or protected information. Avoid using them to access sites where you store personal information that could be used for identity theft (such as bank sites, credit card web pages, etc.) These computers may not be well maintained, and may provide fertile ground for viruses, spyware, and other malicious software. Some companies monitor all activity, including the keystrokes you type, on kiosk and internet cafe computers. In some countries, this is not only a common practice, it is government policy. If you do choose to use a public computer, it is safest to assume that you have no expectation of privacy for anything you do on that computer.

Always use the MSU Virtual Private Network service, your departmental Virtual Private Network service, or a trusted third party service to encrypt your communications traffic when connecting your computer from an untrusted network to the MSU networks. Whether you are using a wired or wireless network, this

is the only way you can assure a reasonably secure connection. Some hotels, restaurants, and coffee shops offer “free” wireless networks, but require you to download software on your computer before you can use their network. Avoid using any network service that requires you to download and install software onto your computer to gain access. These software packages nearly always include some form of “adware”, software which monitors your browsing and directs advertising to you to pay for the network service. Avoid using these networks, and never download untrusted software onto your computer to gain network access.

Remember that you have no reasonable expectation of privacy when using your computer in a public place. It is not difficult for another person in a cafe to sit a few tables behind you, and view what you are doing on your computer. Always use a privacy screen or other device to obscure your display to prevent anyone nearby from observing your work. Several manufacturers make polarized screens that fit over your laptop display, and obscure your screen from casual view unless you are sitting directly in front of the computer.

Just as airport security requires you to maintain possession of your carry-on bags at all time, your computer and electronic devices should also remain in your possession. 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. Use password protection on your devices to prevent someone picking up and using your computer and electronic devices. Even if your computer is nearby, turn on password protection for your screensaver, and lock your screen if you leave your computer idle in a secure location. Always decline any request from someone you don’t know to use your laptop, handheld computer, or cell phone. In a similar manner, avoid using the devices of others, and practice Safe Computing: don't allow others to connect devices to your computer or electronic devices for any reason. Viruses and malware can easily travel from USB devices to infect a computer.

There may be times when you have no choice, such as if airport security or customs agents ask you to surrender your devices for security reasons. If you are required to surrender any of your devices, always assume that they are compromised if they are returned to you. Always check them for viruses and malware before continue using them for any work. Immediately backup any critical data on the device once it is returned, and scan your backup device for any malicious software or virus infections.

When you return:

Now that you've returned, and you believe you've taken every reasonable precaution while traveling, you're not done yet. Assume the worst: that you still may have picked up some malicious bug that could potentially pose a threat to your departmental network and computers. The best way to resolve any potential for infection is to assume that your computer hard drive may need to be erased and rebuilt.

First, back up all the critical data you need to save from your trip, including all files you created or modified while traveling. Once you've confirmed you have everything you need from the computer, if you borrowed a loaner laptop for your travel, return it to your IT department and let them deal with any cleanup of the system or software.

If you didn't travel with a loaner that can be easily erased and rebuilt, you should immediately scan for viruses, malware, and spyware before you reconnect your computer to the MSU networks.

Travel can often result in obtaining new equipment, whether you received a gift from a co-worker, or a promotional item from a vendor. It is quite common for vendors and others to simply give away a USB drive containing conference proceedings, promotional information, white papers, or sample software. These promotional items provide another path for viruses and malicious software to find their way onto

your computer. Before accessing any files or software on any promotional item you receive, fully scan that device for malicious software.

In addition to promotional items, travel can provide opportunities to purchase computer software and hardware at discount rates. Let the buyer beware, inexpensive software may not be legitimate, and can contain malware and/or viruses. Check any hardware or software you purchase for viruses and malicious software when used.

If you discover new software installed on your computer that you did not install, contact your IT department for assistance immediately. In addition, if your machine response seems significantly slower than usual, or software that was operating normally begins malfunctioning or reporting odd errors, it may be the result of interference or damaged caused by a virus infection. Again, if this occurs after you return, contact your IT department for assistance in troubleshooting your computer for a potential malicious software issue.

APPENDIX: Additional Resources

Vendors providing free firewall, antivirus, antispyware, and malicious software scanners:

Comodo firewall and antivirus
http://www.personalfirewall.comodo.com/

AVG personal antivirus
http://free.avg.com/

ZoneAlarm free firewall
http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm

Additional links to MSU resources

MSU Academic Technology Services Help Center
http://help.msu.edu

MSU ATS techbase article on the MSU VPN service
http://techbase.msu.edu/article.asp?id=8068&service=techbase

MSU ATS techbase article on changing your MSU NetID password, which contains some recommendations about how to create a secure password:
http://techbase.msu.edu/article.asp?id=142&service=techbase

MSU Office of Export Controls and Trade Sanctions Compliance
http://www.exportcontrols.msu.edu/

MSU Office of International Students and Scholars
http://www.oiss.msu.edu/

MSU University Travel Office
http://www.ctlr.msu.edu/COTravel/