IT Security Training: System Access from Off-Campus

1.) The USNH System Access Policy requires that access to university systems and information from off-campus, such as from home, meets the same level of secure access that is provided in the USNH-managed environment. Section 5.7.1.7 of the UNH System Access Policy Compliance Standards document contains a helpful explanation of what this policy means at UNH. The document has additional important information, such as the requirement to securely wipe drives before transferring a computer to another person, etc., and can be found at http://it.unh.edu/media/IT%20Security/USNHSystemAccessPolicyComplianceStandards04292009.pdf

2.) It is best that no other person uses a computer which is used at home for work purposes, but if the situation requires that other persons use the machine, they should be issued a separate computer account and informed about the practices used to protect that computer. Institutional password sharing is prohibited by university policy. Too many security incidents involve former friends, acquaintances and even family members who were trusted in the past but due to a turn of events are no longer on friendly terms....do not share passwords and accounts.

3.) A machine in a private home is at risk from theft and should be encrypted. IT Security strongly recommends encrypting any machine that is portable or used off-campus. In addition, any campus machine that has restricted or sensitive data should be encrypted, but it is best to keep such information on a secure server, whether working on campus or from off-campus. An encrypted machine that is stolen is less likely to result in a compromise of the information that is stored on the computer. An encrypted computer must be logged-off and shut down to prevent a thief from viewing the encrypted content. While the machine is running and is logged-in, a thief can read the content. A strong password that is not used for any other purpose, and that is documented in a secure manner is recommended for encrypted machines as a forgotten/lost password will lock out the user permanently. IT Security recommends and offers assistance in enabling TrueCrypt encryption. The TrueCrypt pamphlet is located at http://it.unh.edu/media/IT%20Security/TrueCryptPamphlet022302009.pdf.

4.) The Protected Computing Best Practices document contains many pertinent good practices for off-campus computing, as well as general good computing practices no matter where computing is done. The document can be found at http://it.unh.edu/media/IT%20Security/ProtectedComputingBestPractices.pdf

5.) Any computer’s security/protection is outdated quickly, and must be updated frequently. At a minimum, automatic updates should be enabled for the operating system, Adobe software, virus protection, and other applications that either protect the machine or are known to put the machine at risk if outdated. It is important to verify often - goal is once per week - whether the updates are working and are current.

6.) Securing a computer physically to prevent theft is important. Theft of computers is one of the most common events that results in an information compromise. Locking the machine in a secure place, cabling it, or keeping it out of sight is better than leaving it exposed during a burglary.

7.) UNH has a program for checking computers for vulnerabilities. This service does not reach a computer that is kept off-campus. The machine should therefore have additional protection installed. A popular tool is http://www.malwarebytes.org/ which should be run often – at least weekly - to check for key loggers, and other hidden malware.

8.) Be aware of unexpected behavior and pop-ups, as unsuspecting “friendly” users of the machine may go to a malicious web site and unknowingly infect the machine. You may not know for
months that your machine has a key logger and is harvesting and reporting out your passwords, for example.

9.) The UNH CSC offers disk wiping services for a fee.

10.) IT Security is available to do additional training if specific skills are needed, such as installing Malwarebytes, checking for updates, etc.

11.) Any connections from home to the UNH campus should be done through a VPN session. If you are just doing e-mail, public VPN is sufficient. VPN encrypts your communication from your computer to the campus.

12.) Home computers should be protected by a firewall. While software firewalls can be installed and/or activated directly on computers, this recommendation refers to placing a hardware firewall between the ISP modem and the computer. The firewall often comes with multiple ports and can protect multiple computers as well as a wireless router. While not perfect, it eliminates many of the common threats to your home network. The Windows 7, Vista and XP Service Pack 2/3 operating systems have firewalls built in that are turned on by default to block threats from the Internet, and should also be left on for protection.

13.) A university owned machine is appropriate for processing through the Safe Electronic Equipment Disposal (SEED) program. Full program information can be found at http://it.unh.edu/index.cfm?id=43A69C62-CAE8-B08D-8F3CE7C896E32791

14.) Screen shots of problems will help troubleshoot them. (For example, a screen shot of an annoying or potentially threatening pop-up.)

15.) Information for protecting yourself on the Internet is located at http://it.unh.edu/index.cfm?id=B82A908F-B7A6-A094-7FC8793BC96EDD2B.

16.) When accessing university resources from home (ex. University e-mail, Banner applications, etc.), university policies apply. Below is a summary of the most directly pertinent ones for today’s session.

USNH Data Classification Policy
Foundation for protecting data http://it.unh.edu/media/IT%20Security/Data_Classificaton_Policy_11202008.pdf

USNH Policies http://www.usnh.edu/olpm/USY/VI.Prop/F.htm

Section 4. Policy on Use of Technological Resources
Section 5. Information Technology Security Policy

UNH Policies http://www.usnh.edu/olpm/UNH/VI.Prop/

Section 4: Privacy and Security
Section 5: Acceptable Use

IT Security is available for additional training, if needed or requested. Contact IT Security at https://remedy.unh.edu/itsec/inquiry.shtml