Good Computing Practices and Risk Reduction Strategies
Revision 8/21/2012

Executive summary

How you manage and use your computing resources is important. Being aware of threats you face each time you turn on a computer, access the Internet or log into one of your accounts can make the difference between successfully protecting information and having your privacy or information about others compromised. Accidental or malicious release of protected information can result in a full range of undesirable consequences from minor inconvenience to life-long impact, financial damage, reputational damage and liability.

The secure use and operation of university computing environments is guided by university policies and required by state and federal laws. The secure operation and use of these environments and the data stored in these environments is an integral part of our business. Security must be included in the initial design, configuration, operation and decommissioning of these environments. UNH IT Security provides awareness level training and tools that you can use to accomplish this.

Good Practices and Minimum Requirements

1. Know What You Have and Only Keep What You Need

- 1.1. Only collect and retain information for which you have a legitimate business need.
  - 1.1.1. Maintain an inventory of the information that store.
  - 1.1.2. Classify your information according to the USNH Data Classification Policy.
  - 1.1.3. Understand university policies and legally mandated requirements for protect information.
  - 1.1.4. Establish and follow a data retention policy.
    - 1.1.4.1. Identify your legitimate business needs and regulatory requirements to retain or destroy information that you maintain.
    - 1.1.4.2. Document your retention requirements using templates provided in the UNH Faculty and Staff Blackboard organization, under IT Policy and Security.
    - 1.1.4.3. Backup mission critical information to appropriate secure storage and test recovery.
  - 1.1.5. Scan your computer, file shares and removable media with Identity Finder frequently to ensure that it does not contain restricted information such as SSNs, Credit Card Numbers and Passwords.
  - 1.1.6. Ensure that only authorized persons can access the information for which you are responsible.
  - 1.1.7. Submit retired equipment to the SEED program for safe wiping of information and proper processing of the physical material.

2. Store And Process Information In Approved Systems

- 2.1. Use secure storage options in approved systems to store university information. For example, only Banner is approved for storing Social Security Numbers and Academic Records. Credit Card Numbers are not approved for storage in any university systems. Medical information may only be stored in systems built specifically for that purpose according to HIPAA requirements.
- 2.2. Do not copy Restricted information to local and/or portable media such as desktops, laptops, tablet computers, CDs, and removable flash drives.
- 2.3. If legitimate business needs require that protected information be stored on a laptop, first obtain administrative approval and ensure that the laptop is professionally administered and encrypted.
- 2.4. Lock printed and other forms of protected information in secure storage.
  - 2.4.1. Keep an inventory of restricted information that you are storing.
  - 2.4.2. Maintain access records to the stored information. For example, log access to restricted data storage rooms. Consider installing automated mechanisms, such as card access, intrusion alarm, and security camera.
  - 2.4.3. Limit access to the stored records to authorized person. For example, if others have access to your work space or desk during or after work hours, lock up printed material that is not under your direct control.
  - 2.4.4. Use effective containers to protect your work. For example, use quality filing cabinets that have unique locks & keys, rather than cubicle desk drawers that do not have unique keys.
- 2.5. Do not place sensitive and restricted information into off campus systems unless the off-campus system is governed by a strong contract that ensures protection, and the service provider was successfully screened through a formal security review. See USNH Purchasing and UNH IT Security for guidance.
- 2.6. Shred document using a cross cut shredder or an approved and contracted shredding service.

3. Protect Your Computing Equipment And Computing Sessions

- 3.1. Maintain current updates for all operating systems and applications.

3.2. Activate built-in protection mechanisms on the device and in the applications. For example, activate Microsoft Firewall services and password requirement to boot or “wake up” the computer.

3.3. Maintain current malware protection

3.3.1. Check for updates at least daily. Select automatic checking to ensure that it happens.

3.3.2. Configure the protection to detect active threats real-time.

3.3.3. Conduct periodic full and off-line malware scans. See professional assistance if you do not know what this means, or how to do it.

3.3.4. If you run unattended scans after hours, protect your computer with encryption, personal firewalls, strong passwords, locked screen/keyboard, and physical security to prevent theft.

3.3.5. If you detect malware, run an additional malware scans with another reputable tool. If you are not sure, seek professional assistance. Wipe and rebuild the system unless you are sure that all malware was removed.

3.3.6. If you detect malware on a device that is used to access restricted information, report the incident to IT Security immediately.

3.4. Protect your computer from unexpected or unintended installation of unwanted software

3.4.1. Do not conduct your daily work while logged in on your computing device with administrator privileges. For example, remove your AD account from the local administrator group.

3.4.2. Never browse the Internet and never conduct Internet searches while logged in as administrator.

3.4.3. Log out of your administrator account as soon as you have completed administrative tasks.

3.4.4. Ensure you understand what is being installed on your device before you grant permission or provide your administrator password to allow the installation to proceed.

3.5. Protect your passwords.

3.5.1. Never share your password with anyone for any reason.

3.5.2. Change your password periodically at minimum according to university policy.

3.5.3. If possible, use passwords that are longer than the minimum required.

3.5.4. Select services that do not depend solely on passwords for access control.

3.5.5. Do not use the same password to access services that contain restricted university information that you use for less secure environments.

3.5.6. Use strong passwords, at minimum following university policy. UNH IT Security provides training on how to accomplish this.

3.6. Secure your computing device according to university policy

3.6.1. Enable all reasonable security measures that are available on your device unless you have a legitimate reason not to do so and other layers of protection are available that address the security gap.

3.6.2. Lock the screen on your device before stepping away from it and enable timed lockout following a period of inactivity.

3.6.3. Turn off devices, if possible, when they are not used for prolonged periods of time.

3.6.4. Provide reasonable physical protection for your device.

3.6.4.1. Lock it in a secure location when it is not under your control.

3.6.4.2. Cable the device if it is maintained in an area that others can access.

3.6.4.3. Do not leave it visible in a parked car.

3.6.5. Enable and learn about remote wipe options for portable devices that have such option. For example, the iPad has excellent options for this, but you must activate them in advance, and act immediately if the device is lost or stolen.

3.6.6. Enable available automatic device lock and wipe option following multiple failed password attempts.

3.6.7. Enable password requirement to start, boot, and otherwise “wake up” the device.

3.6.8. Activate or install supported encryption, especially on portable devices and devices that are at risk from physical theft.

3.6.9. Change the default administrator password on your devices to a strong password that only you know.

3.7. Don’t be a Phish.

3.7.1. Be aware of Phishing and Spear Phishing. See http://it.unh.edu/itsecurity.

3.7.2. Do not click on links or open attachments in unexpected e-mail messages.

3.7.3. Do not reply to unexpected messages that ask you for your information, such as your password.

3.7.4. Remember that Phishing attacks can look like completely legitimate e-mail messages. Think about what they are trying to get you to do, not just what they look like.

3.7.5. Contact the UNH IT Service Desk if you are not sure whether an e-mail message is legitimate but you are concerned about experiencing other problems if you do not respond to it.

3.7.6. Phishing is a form of social engineering, be aware of other forms of social engineering attacks, such as fraudulent telephone calls.

4. Use Encryption As A Key Layer Of Protecting Information

4.1. Mobile devices, such as laptops, that must contain restricted information must be encrypted. Contact UNH IT Security to agree on a reasonable plan. This is mandated by privacy laws and common sense.

4.2. Mobile devices that must contain sensitive information should be encrypted.

4.3. Computing devices that are risk of theft should be encrypted. This includes machines in cubicles and public spaces.

4.4. Use UNH's Symantec PGP encryption when possible to ensure consistency and supportability.

4.5. Activate built-in encryption options on devices that cannot use Symantec's PGP encryption.

4.6. Contact IT Security or view the encryption information in the UNH Faculty and Staff Blackboard Organization under IT Policy and Security.

5. Utilize Secure Methods To Access And Search The Internet.

5.1. Never access the Internet while logged in with administrative privileges on your computing device.

5.2. Do not click directly on search results that are displayed in general Internet searches.

5.3. Access search results by typing the high level URL of the location where the search result is found, and drill down to the information you need or repeat the search from a trusted high level link of the organization that has the resources you need.

5.4. Do not allow unexpected installation of software when you access search results on the Internet unless you initiated the installation.

6. Use Secure Methods To Access The Campus Computing Environment Remotely

6.1. Always use a protected, properly configured computing device that is under your control.

6.1.1. Do not use public computing devices to log into university systems. This is especially critical for accessing systems that contain restricted information, such as Banner.

6.1.2. Do not allow others to use the computing device that you use to access university systems. For example, children and other family members using the device to access the Internet put future connections to university systems at risk.

6.1.3. Always log into VPN when accessing university systems remotely.

6.1.4. If possible, use university-issued and maintained devices, such as university owned laptops.

6.1.5. If you must use a personally owned device to access university systems, you are responsible for the security of that device and the device must at minimum have the same level of protection that is practiced for campus systems. Consider having the university Computer Repair Service center check your computer for malware and proper protection at least annually, and follow other minimum recommended practices for secure computing that were developed for the flexible work arrangements initiative.

6.1.6. Do not connect to university systems that contain restricted information from public WiFi hot spots.

6.1.7. Protect the computing devices that you use for remote access from loss and theft while it is in transit or while it is in your home.

7. Seek training

7.1. UNH IT offers free on-line training video. Contact IT Security about obtaining a SANS Securing the Human account.

7.2. Review http://it.unh.edu/itsecurity weekly

7.3. Be familiar with the UNH Faculty and Staff information security and policy portal in Blackboard.

7.4. Invite IT Security to provide your organization customized training sessions

7.5. Seek professional training specific to your discipline.

8. Be Prepared In Case You Experience An Infection Or Breach

8.1. Reach the IT Security Incident Response Plan posted in Blackboard, in the UNH Faculty and Staff Organization, under IT Policy and Security.

8.2. If your malware protection detects an infection or your computing device exhibits suspicious "behavior", disconnect the Ethernet cable and/or turn off wireless services, and conduct additional malware scans.

8.3. Do not assume that malware protection can detect and remove all malware. Any sign of malware is a strong indicator for wiping and rebuilding the system from a clean source. Seek professional advice and assistance.

8.4. Notify IT Security immediately if you have access to restricted university information and experience an infection, compromise or potential compromise.

8.5. Change all your passwords immediately if you experience or suspect a malware infection, inappropriate access to your device(s) or account(s), or have other reasons to believe that someone else could have your password(s).