Symantec PGP End Node Encryption for Windows Computers
UNH Information Security Services (ISS)

Revision 5/19/2014

CONSIDERATIONS FOR THOSE PLANNING ENCRYPTION:

Why Should You Encrypt?
Encrypting information protects it from unauthorized persons viewing it when a computer or another information-storing device is lost or stolen. Encryption is not only a good practice to protect your privacy, but it is required by state and federal laws for certain types of information.

Is Encryption Alone Sufficient?
Encryption is an important component of security. To benefit from encryption, it is important that you also follow other good practices, including:

- Use strong, complex passwords
- Lock your computer screen before stepping away
- Shut down your computer when you will not use it for prolonged periods of time
- Ensure the physical security of your computer to prevent loss or theft
- Maintain current software updates and security configurations for your operating system and application programs
- Maintain university supported malware protection and keep it current
- Scan your computer, removable devices, e-mail and archives, and file shares with Identity Finder and remove any legally protected information from your computer.
- Familiarize yourself with the ISS website at http://it.unh.edu/infosec
- Report a lost or stolen devices immediately to the IT Service desk during customary working hours, or to UNH Police Dispatch outside of working hours

Why Does UNH Use Symantec's PGP Encryption software?
While some operating systems have built-in options to encrypt devices, UNH uses Symantec's PGP encryption software to realize several key benefits:

- Consistency between operating systems and versions of operating systems
- Support for MS Windows and Linux
- Focused support from UNH ISS on a product that serves the largest number of clients
- Self-service option to reset your password yourself if you forget it
- Ability for ISS to assist you with a forgotten password
- Using a product with which others at UNH and the other USNH institutions are familiar
-

What Should You Do Before Encrypting?
Backup any critical documents to a secure file server. Backing up your files protects your information from loss if your computer is lost or stolen, has mechanical problems, or you accidentally delete the information. Doing so also protects the information in the unlikely event that you encounter any complications while encrypting.
If your computer has been previously encrypted with a product other than PGP Encryption, you must decrypt the computer prior to installing and running PGP Encryption. Contact ISS if you need assistance.

Can You Upgrade Your Operating System After Encrypting Your Computer?
If you intend to upgrade your operating system in the near future, it is preferable to do so before encrypting. If your computer is encrypted and you plan to update, Symantec PGP specifies the following process:

1. Decrypt the disk.
2. Back up your keys and keyrings.
3. Uninstall PGP Desktop.
4. Upgrade your operating system.
5. Import your keys and keyrings.
6. Install PGP Desktop
7. Encrypt your disk.

Can You Use Anti-Virus Software On An Encrypted Computer?
You can and should continue to use A/V software on your encrypted computer to protect the computer against malware. If you intend to use an off-line malware scanning tool, such as Windows Defender Offline, to check your computer, you must decrypt the computer before running the scan. Offline scanning is a recommended practice for devices accessing restricted or sensitive information

ENCRYPTING YOUR COMPUTER:

Recommended High Level Approach to Encrypting Your Computer
ISS recommends that the first time you use encryption you schedule a short work session with ISS staff as outlined below:

1. Fill out the request form at https://itsupport.unh.edu/itsec/ and note that you would like assistance with encrypting your computer.
2. ISS will contact you to schedule a brief session – typically 15 to 20 minutes - to install the product, initiate the encryption, and guide you through setting up security questions and encrypting removable devices.
3. Backup all important files. Be sure to use the appropriate location to backup your information. If you maintain legally protected information such as SSNs, Credit Card Numbers, student academic records, and medical information, be sure to speak with ISS about the appropriate locations to which such information may be copied.
4. If you will be encrypting your flash drives, external drives, and other removable devices, back those up as well.

Instructions for Encrypting a PC without Assistance From ISS

1. The encryption installers are only available by request from ISS and are not currently online. To obtain the installers, fill out the request form at https://itsupport.unh.edu/itsec/ and note that you need the installers. Installers are available for:
    a. Windows 32 bit version
    b. Windows 64 bit version
    c. Linux

2. You must use a UNH Ethernet connection, rather than wireless, while the initial encryption is running. Your computer must be plugged into its AC adaptor; encryption will not proceed on battery power.
3. Run the installer. If you are not logged in with administrative rights when you run the installer, you may be prompted for the local administration account on your computer. Depending on how your security settings are configured, you may also be asked whether it is OK to run this program. Since you started it, the answer is 'yes'. Use a UNH Ethernet (wired) connection rather than wireless when running the installer and during the initial encryption process which starts automatically.
4. Reboot your computer when prompted. When your computer reboots, you may be asked to accept the cert from an unrecognized Certificate Authority (CA). While we generally recommend against accepting certs from unrecognized CAs, in this case we are aware of this situation and you can proceed with accepting it as long as you initiated the session following our instructions and it shows to be for "cipher.unh.edu".
5. Work through the encryption enrollment screens that display as the computer boots back up. If you find that the security questions "from your life" do not work for you, you can make up your own security questions. If and when you forget your password or passphrase, you will be able to use these questions/answers to reset your password/passphrase.

The first day you log in on your computer after the installation, you may experience a one-time temporary delay in getting into email and VPN.

What To Do If You Require Assistance Or Are Unable To Remember Your Password

- If you forget your password, you can reset your forgotten password by bypassing the PGP BootGuard screen and answering three out of the five security questions that you setup during the enrollment process. This option can be used at any time, especially outside of customary business hours.
- If you forget both your password and the answers to the security questions, contact ISS for a one-time access via the Whole Disc Recovery Token (WDRT).
- If you require assistance immediately during customary business hours, contact the UNH IT Service Desk at 862-4242, explain your situation, and request a high priority service request to IT Security.

To Decrypt Your PGP Encrypted Computer

Open PGP Desktop by clicking on the PGP icon on your desktop or under 'All Programs' in the PGP folder. Click on 'PGP Disk' and then click on 'Encrypt Whole Disk or Partition'. Click the Decrypt button at the upper right side of the window to start the decryption process which may take several hours to complete. Unlike encryption, decryption will process whether your computer is on battery or AC adaptor power.