U.S. Department of Labor

EMPLOYMENT STANDARDS ADMINISTRATION

OFFICE OF MANAGEMENT ADMINISTRATION & PLANNING (OMAP)

DIVISION OF INFORMATION TECHNOLOGY MANAGEMENT AND SERVICES (DITMS)

Pointsec

Frequently Asked Questions

Document Version: **V.1.0**

Document Date: **September 20, 2007**

Version & Change History Log

Date	Version	Description	Author
09-20-2007	V.1.0	Initial Version	Eric Pastuszek

This document was prepared for the U.S. Department of Labor, Employment Standards Administration, Office of Management Administration & Planning's Division of Information Technology Management and Services (DITMS), Washington, D.C.

Restriction
This document includes data that shall not be disclosed outside the U.S. Department of Labor, Employment Standards Administration and shall not be duplicated, used, or disclosed-in whole or in part- for any purpose other than to evaluate this document. This restriction does not limit your right to use information contained in this data if it is obtained from another source without restriction.

This information within this document was created at the U.S. Department of Labor as an instruction manual for educational usage by Pointsec users at the U.S. Department of Labor.

Table of Contents

1. POINTSEC ENCRYPTION FREQUENTLY ASKED QUESTIONS

Pointsec Encryption Frequently Asked Questions (FAQs)

What is Pointsec?

Pointsec protects sensitive information on your computer by making it unreadable to those not authorized to access your computer. Pointsec also makes the files on external storage devices unreadable except for those you wish to access the files.

What is a typical workflow when using Pointsec?

A typical Pointsec workflow is as follows:

1) On ESA PC encrypt file(s) into encrypted package
2) On ESA PC copy encrypted package from ESA PC to external storage device
3) On non-ESA PC decrypt the encrypted package
4) On non-ESA PC modify the decrypted file(s)
5) On non-ESA PC re-encrypt file(s)

What are acceptable external storage devices that may be used with Pointsec?

External storage devices approved for use with Pointsec are 3.5" floppy disks, CDs, thumb drives, flash drives, and external hard drives only.

Are there any limitations with the acceptable external storage devices?

CDs have limited use with Pointsec Encryption. You can store encrypted packages from your ESA PC and decrypt the package on a non-ESA PC (Pointsec Not Installed). You cannot re-encrypt the file once decrypted nor can you use Secure Delete when using a Non-ESA PC (Pointsec Not Installed).

DVDs are not an approved External Storage Media for use with Pointsec Encryption at this time.

How does Pointsec affect me?
Will I have to change how I do things on my computer?

Most of the time, you won't notice any difference with your computer. You'll log in and use your computer as you normally would. Pointsec will silently work in the background. You will notice a difference when you copy files to a CD, diskette, USB device, or other removable media. The *Pointsec User Guide* describes those differences.

How do I verify Pointsec installation?

To verify Pointsec installation, look for the Pointsec icon in the System Tray in the bottom right corner of your desktop:

Please also review the *Pointsec Installation Verification Guide* for further details about verifying Pointsec installation.

Where can I find step-by-step instructions on how to encrypt a file using Pointsec?

Refer to the *Pointsec User Guide*.

Is there a Quick Reference Guide available?

Yes. Refer to the *Pointsec Quick Reference Guide*.

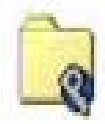
Does Pointsec encrypt email?

Pointsec is for the protection of files and folders when stored on external storage devices/media only. **It does not protect or encrypt files attached to e-mails.**

How do I know if a folder or file on my internal drive is protected by Pointsec?

As Pointsec is transparent on your internal hard disk, a Pointsec icon doesn't appear on files/folders on your internal hard disk. Be aware, even though the files and folders appear normal, **all files and folders on your internal drive are encrypted and protected** for the purpose of storing them on external media devices/media and can only be opened, viewed, revised, and re-saved on external storage devices/media using an ESA PC with Pointsec Encryption installed or processed through the Pointsec Encryption/Decryption process when using a non-ESA PCs.

How do I know if a folder or file on external media is protected by Pointsec?



A Pointsec icon appears on the encrypted folder.

A Pointsec icon appears on the encrypted file.

How do I know if an encrypted package exists on my internal drive or on external media?

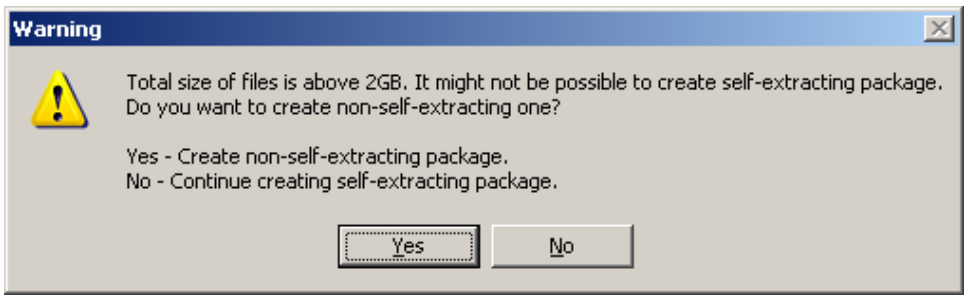
A Pointsec icon appears on the encrypted package.

What is the maximum size limitation for each encrypted package?

Within Pointsec there is a 2 gigabyte (GB) maximum limitation for each encrypted package. You can include multiple files and folders within a single encrypted package; however, the overall size of the combined files/folders cannot exceed 2 GB. Multiple encrypted packages (each less then 2 GB) are ok based on the size limitation of the selected external storage device or media.

What happens if I try to encrypt a package larger than 2 GB?

A warning message appears, similar to the following, advising the user that the package to be encrypted exceeds the maximum limitation of 2 GB:



CAUTION!!

If you receive the warning message above, perform these steps to end the creation of the encrypted package using Windows Task Manager:

1. Press **Ctrl-Alt-Delete**.
2. Click **Task Manager**.
3. Click **Applications**.
4. Select '**Pointsec Media Encryption …**'
5. Click **End Task**.
6. If a box appears with the End Now button, click **End Now**.
7. Click **X** to close Windows Task Manager.

If Windows Task Manager fails to terminate the creation of the encrypted package, reboot your computer.

If your data to be encrypted exceeds 2 GB, split your files to be encrypted into several groups, each of which is less than the maximum limitation of 2 GB. Then, create an encrypted package for each group of files that is less than the maximum limitation of 2 GB. Stay below the 2 GB threshold with each encrypted package!!!

What is the purpose of the Pointsec Account Name and Password?

Account Names and Passwords are also used to prevent unauthorized use of your external storage devices/media. Again be sure to remember both the Account Name and Password or else access to your external storage device/media will be denied. In this instance the only remedy is to reformat the external storage device/media and start over. Reformatting will result in the loss of all data stored on the external storage device/media.

What password is used when decrypting an encrypted package?

When decrypting an encrypted package use the same password that was used when the encrypted package was created.

What are the parameters when assigning a Pointsec password?

A password must have **at least eight alphanumeric characters**, including **at least one upper-case letter**, and **cannot exceed a maximum of 13 alphanumeric characters**. Alphanumeric means any combination of letters and numbers. **Special Characters** and **Symbols** such as **- ! @ # $ % ^ & * ( ) _ - + = < > ? / { } [ ]** are **not allowed**.

What is Pointsec Secure Delete?

The Secure Delete function allows the user to permanently remove a file.
Secure Delete writes 0s and 1s over the data in the file, thereby rendering the file unreadable.

Is a file recoverable after using Secure Delete?

No.

What do I do when the Encryption menu doesn't display, yet Pointsec has been fully installed?

This situation rarely happens. If, however, this occurs, simply reboot your computer, and the Encryption menu should display.

How does Pointsec affect the giving of a file(s) on removable media to someone outside of ESA?

Assign a Pointsec password to a file(s) on external media before sharing that file(s), and then provide the password to the receiving user.

Can the Pointsec password be reset?

No.

What happens if the Pointsec password, assigned to the external storage device, is forgotten?

The external storage device must be reformatted.

Is it permissible to use an external storage device with hardware encryption already installed?

No. It is not recommended to use an external storage device with hardware encryption already installed.

Is it acceptable to use a personal external storage device, such as your own USB device?

No. We do not recommend the use of personal USB devices (this is against DOL policy).