U.S. Department of Labor

EMPLOYMENT STANDARDS ADMINISTRATION

OFFICE OF MANAGEMENT ADMINISTRATION & PLANNING (OMAP)

DIVISION OF INFORMATION TECHNOLOGY MANAGEMENT AND SERVICES (DITMS)

Pointsec

Quick Reference Guide

Document Version: **V.1.0**

Document Date: **September 19, 2007**

Version & Change History Log

Date	Version	Description	Author
09-19-2007	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.

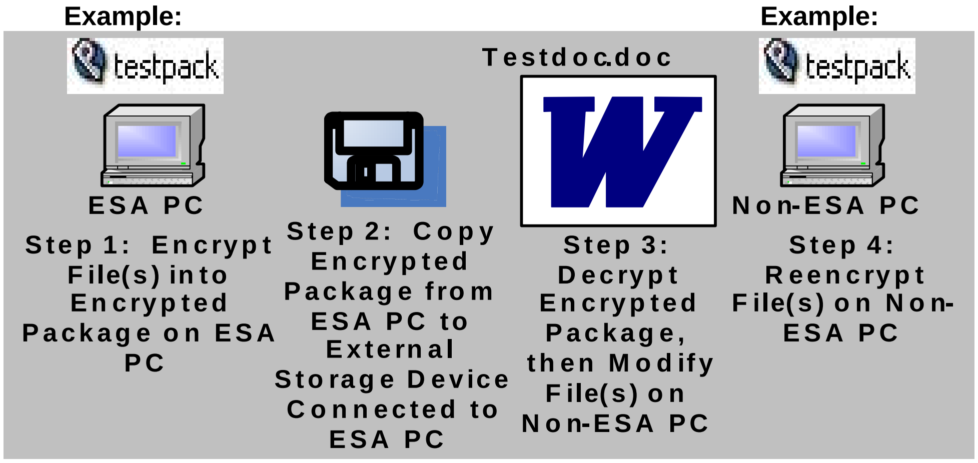
This information within this document was created at the U.S. Department of Labor as an instruction manual for educational usage by Pointsec users at the U.S. Department of Labor.

Table of Contents

1. General Information

ALWAYS ENCRYPT EXTERNALLY STORED DOL FILES AND FOLDERS. WHEN ENCRYPTING A FILE DO NOT USE DRAG & DROP OR SAVE AS!!

1.1. Typical Pointsec Workflow



Step 1: Encrypt File(s) into Encrypted Package on ESA PC

Step 2: Copy Encrypted Package from ESA PC to External Storage Device Connected to ESA PC

Step 3: Decrypt Encrypted Package, then Modify File(s) on Non-ESA PC

Step 4: Reencrypt File(s) on Non-ESA PC

1.2. Password Assignment

Password must be 8 – 13 alphanumeric characters, with one upper-case character; special characters are not permitted.

1.3. Examples of Encryption Icons

Pointsec Encrypted Folder Icon

The folder contains at least one encrypted file.

Pointsec Encrypted File Icon

The file is encrypted.

2. ENCRYPTION PROCESS FOR 3.5" FLOPPY DISK OR USB DEVICE

2.1. CREATING ENCRYPTED PACKAGE ON ESA PC

1. **On your ESA PC**, select file(s)/folder(s) to encrypt.
2. Right-click one file or folder selected in Step 1.
3. Select **Encryption**.
4. Click **Create Encrypted Package**.
5. Type the same password in Password field and Confirm Password field, and remember it. For details about acceptable password format, refer to Section 1.2, Password Assignment.
6. Do not select **Create package without extractor**.
7. Click **OK**.
8. Browse and select location to save encrypted package.
9. Type a filename for the package such as **testpack**.
10. Click **Save**. Message 'successfully created' appears.
11. Click **OK**.
12. Confirm encrypted package was created by browsing to the location of the saved, encrypted package.

2.2. STORING ENCRYPTED PACKAGE USING 3.5" FLOPPY DISK OR USB DEVICE ON ESA PC

1. Insert 3.5" floppy disk into (or connect USB device to) **your ESA PC**.
2. Go to your Desktop.
3. Double-click **My Computer**.
4. Browse to one location containing the encrypted package(s) to copy.
5. Select encrypted package(s) to copy to floppy disk or USB device.
6. Click **Edit**.
7. Click **Copy to Folder**.
8. If copying to floppy disk, select Floppy Disk Drive (A:).
   If copying to USB device, select USB Device (Removable Disk).
9. Click **Copy**. If a message appears indicating that a file already exists on the destination device, click **Yes** to overwrite the file and to complete the copy process; otherwise, click **No** to terminate.

   Note: Upon initial usage (or after reformat) of an external storage device, Pointsec requests entry of account name (user name), password, and confirmation of password.
10. On your Desktop, double-click on **My Computer**.
11. Double-click on external storage device (floppy disk or USB device) to which you just copied the encrypted package(s).
12. Verify encrypted package(s) was copied to floppy disk or USB device.
13. Click **X** to close the window.

2.3. DECRYPTING ENCRYPTED PACKAGE USING 3.5” FLOPPY DISK OR USB DEVICE ON NON-ESA PC

1. Insert 3.5” floppy disk into (or connect USB device to) a **non-ESA PC**. The disk inserted or device connected to a non-ESA PC must contain the encrypted package to be decrypted.
2. Go to your Desktop.
3. Double-click **My Computer**.
4. Double-click the disk or device, such as USB device (Removable Disk), containing encrypted package(s).
5. Double-click encrypted package to decrypt such as **testpack** or **testpack.exe**.
6. Deselect (*uncheck*) each of the following checkboxes:

   Overwrite Existing Files
   Create Directory Tree
   Save Long Names in 8.3 Format
7. Type the password to open the encrypted package.

   Note: Type the same password that was used when the package was encrypted.
8. Click **OK**.
9. Click where you want the decrypted file(s) to be stored, such as Desktop.
10. Click **OK**.
11. Go to Desktop.
12. Double-click **My Computer**.
13. Confirm decrypted file(s) exist(s) in location selected in Step 9.
14. Open each decrypted file with proper application, e.g., Word.
15. Verify each decrypted file opens decrypted, without a request for a Pointsec password.
16. Modify file(s) as needed in application such as Word, PowerPoint, Visio, etc., then save file(s).

2.4. UPDATING AN ENCRYPTED FILE(S) [RE-ENCRYPT] ON NON-ESA PC

1. Retrieve and insert the 3.5” floppy disk or USB device containing the encrypted package that was decrypted.
2. Insert 3.5” floppy disk into (or connect USB device to) a **non-ESA PC**. Use same disk or device as in Step 1.
3. Go to Desktop.
4. Double-click **My Computer**.
5. Double-click disk or device (3.5” Floppy or USB Device) containing encrypted package that was decrypted.
6. Double-click **pme** or **pme.exe** file.

   Note: Account Name is user name of user who created **Encrypted Package**.
7. Type the password used to encrypt and decrypt.
8. Click **OK**.
9. Click **Next**.
10. Select **Update encrypted files**.
11. Click **Next**.
12. Click **Browse**.
13. Select the location, such as Desktop, of the file(s) you want to update for re-encryption on the non-ESA PC.
14. Click **OK**.
15. **Confirm selected folder** is the correct location of the file(s) to update (re-encrypt) on the non-ESA PC.
16. Click **Next**.
17. Select file(s) to be re-encrypted.
18. Click **Next**.
19. If you want to securely delete the original, unencrypted version of each re-encrypted file, select (check) ‘**Select whether you want to securely delete the original files after they ….**’
20. Click **Finish**.
21. Click **OK**.

3. Encryption Process for CD

CAUTION!!

Regarding CDs, you cannot re-encrypt a file once decrypted.

3.1. Creating Encrypted Package on ESA PC

1. **On your ESA PC**, select file(s)/folder(s) to encrypt.
2. Right-click one file or folder selected in Step 1.
3. Select **Encryption**.
4. Click **Create Encrypted Package**.
5. Type the same password in Password field and Confirm Password field, and remember it. For details about acceptable password format, refer to Section 1.2, Password Assignment.
6. Do not select **Create package without extractor**.
7. Click **OK**.
8. Browse and select location to save encrypted package.
9. Type a filename for the package such as **testpack**.
10. Click **Save**. Message ‘successfully created’ appears.
11. Click **OK**.
12. Confirm encrypted package was created.

3.2. Storing Encrypted Package Using CD on ESA PC

1. Insert CD into CD drive **on your ESA PC**.
2. Go to Desktop.
3. Double-click **My Computer**.
4. Click **Folders**.
5. Select encrypted package(s) to copy from your PC’s internal disk to external storage device.
6. Click **Edit**.
7. Click **Copy to Folder**.
8. Select the external storage device to copy the encrypted package(s) to.
9. Click **Copy**.
10. If a message appears that file already exists on the destination device, click **Yes** to overwrite file and to complete copy process; otherwise, click **No** to terminate.
11. If the message **‘Files Ready to Be Written to the CD’** displays, perform substeps 11.1 through 11.6:

    11.1. Click the Balloon to go directly to the **CD Drive Content Box**, or double-click **My Computer** on your Desktop.
    11.2. Browse to and click encrypted package(s) to copy.
    11.3. Click **Write these files to CD**.
    11.4. Enter a name for the CD in the CD Name box.
    11.5. Click **Next** when the CD Writing Wizard appears.
    11.6. Wait for the CD Writing Wizard to complete copying the data.

3.3. DECRYPTING AN ENCRYPTED PACKAGE USING CD ON NON-ESA PC

1. Insert CD, containing encrypted package(s), into CD drive **on a non-ESA PC**.
2. Go to your Desktop.
3. Double-click **My Computer**.
4. Double-click the CD drive.
5. Double-click encrypted package to decrypt.
6. Deselect (*uncheck*) <u>each</u> of the following checkboxes:

   Overwrite Existing Files
   Create Directory Tree
   Save Long Names in 8.3 Format

7. Type the password to open the encrypted package.

   Note: Type the same password that was used when the package was encrypted.
8. Click **OK**.
9. Click where you want the decrypted file(s) in the decrypted package to be stored, such as Desktop.
10. Click **OK**.
11. Go to your Desktop.
12. Click **My Computer**.
13. Confirm decrypted file(s) exist(s) in location selected in Step 9.
14. Open the file(s), found in the location selected in Step 9, with the proper application such as Word®, PowerPoint®, etc.,.
15. Verify that the decrypted file(s) opens decrypted, without a request for a Pointsec password.
16. Modify file(s) as needed in application such as Word, PowerPoint®, etc, then save the file(s).

4. Secure Deletion of File(s) and/or Folders(s)

4.1. Securely Deleting File(s)/Folder(s) on ESA PC

1. **On an ESA PC**, select file(s)/folder(s) to securely delete.
2. Right-click on one file or folder within the file(s)/folder(s) selected in Step 1.
3. Select **Encryption**.
4. Click **Secure Delete**.
5. Click **Yes**.
6. Verify file(s)/folder(s) was/were deleted.

4.2. Securely Deleting File(s) on Non-ESA PC

1. Insert or connect external storage device, such as USB device, previously used to transport an encrypted package/file, to a **non-ESA PC**.
2. Go to Desktop.
3. Double-click **My Computer**.
4. Locate and double-click on the external storage device inserted or connected in Step 1.
5. Confirm that the **pme** or **pme.exe** file resides on the external storage device used in Step 1.
6. Double-click the **pme** or **pme.exe** file.
7. Confirm Account Name is user name who originally created the encrypted package; change Account Name if it doesn't match user name who originally created encrypted package.
8. Type the password -- entered when encrypted package was created -- in Password box.
9. Click **OK**.
10. Click **Next**.
11. Select **Securely delete files**.
12. Click **Next**.
13. Click **Browse**.
14. Browse, then select, location containing file(s) to securely delete.
15. Click **OK**.
16. Verify path displayed is correct.
17. Click **Next**.
18. Select (check) each file to be securely deleted.
19. Click **Next**.
20. Click **Finish**.
21. Click **OK**.
22. Verify file(s) was/were deleted.