## Student Guide

# Trusted Download Short

### *Requirements*

Trusted downloading requires a comprehensive review by a knowledgeable, authorized user. Authorized users must:

- Be trained
- Have signed briefing forms
- Maintain a log of all downloads
- Use approved file formats
- Follow approved procedures

### *Approved File Formats*

DSS has authorized the following file formats to be released from the IS at or below the accreditation level of the IS, without acceptance of risk from the government customer. An authorized user will convert the necessary files – for example, Microsoft Office files such as Word, Excel, or PowerPoint - into one of these formats to perform a trusted download. Take a moment to review the approved formats.

| Approved Formats | Description | Examples |
|---|---|---|
| **ASCII** | • Raw text<br>• Files may be read with any standard text editor | .txt .fil<br>.dat .asc<br>.c .bat<br>.for |
| **HTML** | • Format used for web pages | .html<br>.htm |
| **JPEG** | • Joint Photographic Experts Group image files | .jpg |
| **BITMAP** | • Window bitmapped graphics files | .bmp |
| **GIF** | • Graphics Interchange Format | .gif |

### *Authorized Procedures*

An authorized user will use these procedures for trusted downloading of Microsoft Office files including Word, Excel, and PowerPoint.

The authorized user will first review the file in its native format and remove any classified information. Then he or she will convert the files to the new format and review, and transfer files to new media and verify the transfer was done correctly. Finally, the authorized user will document the classification level and file transfer.

Review Procedures

1. **Review file and remove classification markings:**
   a. Review Headers and Footers.
   b. Review Slide Masters in PowerPoint presentations.
   c. Ungroup graphics to delete any classified information or links.
2. **Convert the file and review:**
   a. Convert the file into one of the following formats:
      - ASCII/Text
      - HTM/HTML
      - Graphic Files - JPEG, BMP, or GIF
   b. Review files using a compatible application, such as Microsoft Photo Editor or NotePad.
3. **Transfer files and verify:**
   a. Save or transfer file to target factory fresh media.
   b. “Write-protect” the file.
   c. Verify that only the intended files were transferred.
   d. Compare the transferred files to the original files.
4. **Document classification level and file transfer:**
   a. Apply the appropriate level of classification to the target factory fresh media.
   b. Record the transfer and maintain accurate and current audit records.

Note: This list should not serve as an all-inclusive summary of the authorized file formats for trusted download. Refer to the Office of the Designated Approving Authority (ODAA) Process Manual for additional information.

### *Review Procedures*

Once a file is saved in one of the authorized formats and transferred, the authorized user must review the file on the new media in its entirety. Utilities other than the application should be used to view the transferred file on the new media.

| File Type | Review Method | Notes |
|---|---|---|
| **ASCII text** | • Preferred application: NotePad<br>• Alternate application: Hex editing software (used for larger file sizes) | Check file names and sizes. |
| **BMP and JPEG files** | • Graphics file viewer (e.g., MS Photo Editor) | |
| **GIF** | • Internet Explorer or Netscape. | GIF files may contain a 3D/animation/multi-page image and must be viewed with a program that will show all the information.<br><br>MS Photo Editor will **not** display all GIF images. |

### *Other Considerations*

Other considerations for trusted downloading include hidden data and slack space.

One of the most serious problems in downloading is that many applications have areas where classified information can reside, but not be immediately viewable. This is known as *hidden data*. The user may or may not be aware of these areas to check.

*Slack space* is a data storage space that exists from the end of the file to the end of the last cluster assigned to the file. It can potentially contain randomly selected bytes of classified data from computer memory.

Areas to check for hidden data include, but are not limited to:

- Speaker notes in PowerPoint slides
- Words hidden under graphics
- Text hidden in the footer or header of the file
- Information stored in 'undo' files attached to the original file
- Track changes which do not show up on the screen
- Software programs may have many levels of information that can be turned on or off (e.g., Computer-Aided Design (CAD) systems and mapping software)

Systems that are known to produce slack space with unpredictable results include, but are not limited to:

- MAC (not including MAC O/S X)
- Window 95, including release 1
- Some earlier versions of Window 98

### *Use of Alternate Procedures*

DSS has approved trusted downloading for files saved in an authorized format. However, at times, the authorized user is not able to convert files to these formats.

In these cases and where authorized in the DD Form 254 or as a contract line item, alternative procedures must be developed and tested with DSS and approved and accepted by the data owner.

The DSS Information System Security Professional (ISSP) must certify the alternate procedures before the contractor Information System Security Manager (ISSM) can submit the procedures with a Risk Acknowledgement Letter to the Government Contracting Activity (GCA) and/or data owner(s) for signature.

Upon receiving the signed Risk Acceptance Letter from the GCA or data owner, the ISSM must modify the System Security Plan (SSP) to include the approved alternative procedures.

The ISSM must then submit the signed letter and modified SSP to DSS to notify them of the GCA's approval of the procedures.

### *Review Activities*

Question 1: Susana is an authorized user who is performing a trusted download. Which of the following file formats should she save her download as?

- ☐ .PDF
- ☐ .HTML
- ☐ .GIF
- ☐ .DOC
- ☐ .TXT

Question 2: What order should Susana use when completing the trusting download?

- ○ Review file in native format and remove any classified information, convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly, and document the classification level and file transfer.
- ○ Review file in native format and remove any classified information, convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly
- ○ Convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly, and document the classification level and file transfer.

## *Answer Key*

Question 1: Susana is an authorized user who is performing a trusted download. Which of the following file formats should she save her download as?

- ☐ .PDF
- ☑ .HTML
- ☑ .GIF
- ☐ .DOC
- ☑ .TXT

***Feedback****: Approved file formats include HTML, GIF, and ASCII Text (i.e., .TXT).*

Question 2: What order should Susana use when completing the trusting download?

- ⊙ Review file in native format and remove any classified information, convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly, and document the classification level and file transfer.
- ○ Review file in native format and remove any classified information, convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly
- ○ Convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly, and document the classification level and file transfer.

***Feedback****: The authorized user will review file in native format and remove any classified information, convert the files to the new format and review, transfer the files to new media and verify the transfer was done correctly, and document the classification level and file transfer.*

## *Summary*

This Short examined the procedures for trusted downloading. It is important you are vigilant in following these procedures ensuring the protection and safeguarding of classified information.

## Approved File Formats

DSS has authorized the following file formats to be released from the information system (IS) at or below the accreditation level of the IS, without acceptance of risk from the government customer.

| Approved Format | Description | Examples |
|---|---|---|
| **ASCII** | • Raw text<br>• Files may be read with any standard text editor | .txt .fil<br>.dat .asc<br>.c .bat<br>.for |
| **HTML** | • Format used for web pages | .html<br>.htm |
| **JPEG** | • Joint Photographic Experts Group image files | .jpg |
| **BITMAP** | • Window bitmapped graphics files | .bmp |
| **GIF** | • Graphics Interchange Format | .gif |

## General Trusted Download Procedures

Authorized users should use these procedures for trusted download of Microsoft Office files:

1. **Review file and remove classification markings:**
    a. Review Headers and Footers.
    b. Review Slide Masters in PowerPoint presentations.
    c. Ungroup graphics to delete any classified information or links.
2. **Convert the file and review:**
    a. Convert the file into one of the following formats:
        - ASCII/Text
        - HTM/HTML
        - Graphic Files - JPEG, BMP, or GIF
    b. Review files using a compatible application, such as Microsoft Photo Editor or NotePad.
3. **Transfer files and verify:**
    a. Save or transfer file to target factory fresh media.
    b. "Write-protect" the file.
    c. Verify that only the intended files were transferred.
    d. Compare the transferred files to the original files.
4. **Document classification level and file transfer:**
    a. Apply the appropriate level of classification to the target factory fresh media.
    b. Record the transfer and maintain accurate and current audit records.

*This list should not serve as an all-inclusive summary of the authorized file formats for trusted download. Refer to the Office of the Designated Approving Authority (ODAA) Process Manual for additional information.*