Overview

Sensitive information is any data or other information for which public disclosure, or disclosure to users who do not have a need to know to perform their jobs, can harm individuals, the U.S. government, or private organizations. Personally Identifiable Information (PII) is a type of sensitive information that includes but is not limited to social security numbers (SSN), dates of birth, medical information, names of minor children, etc.

To help protect PII during email transmission, the U.S. Courts has provided this process for prospective employees emailing sensitive employment-related documentation with PII.

WARNING: Adherence to the process is strongly recommended to help protect PII during email transmission.

Software Requirements

The processes below require the following software:

- Windows 7 or 10
- 7 Zip

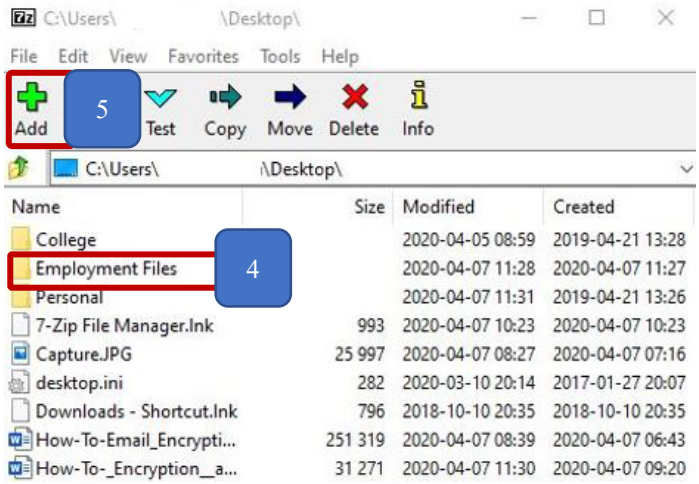
Encrypting and Password Protecting a Folder

Note: While this process follows the 7 Zip, other file encryption software programs generally follow a similar process.

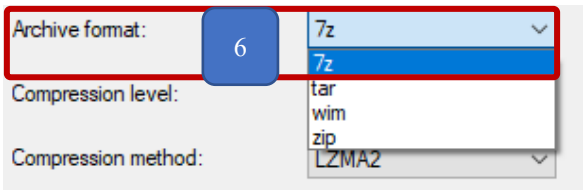
1. Create a new folder on the Windows desktop

   Note: For this process, the folder has been aptly named "**Employment Files**".

2. Place all files desired files in the folder intended for encryption and password protection.
3. Open the 7-Zip File Manager.
4. Left-click once on the desired folder.
5. Click the "**Add**" button.



6. In the "**Add to Archive**" window "**Archive Format**" drop-down menu, select "**7z**".

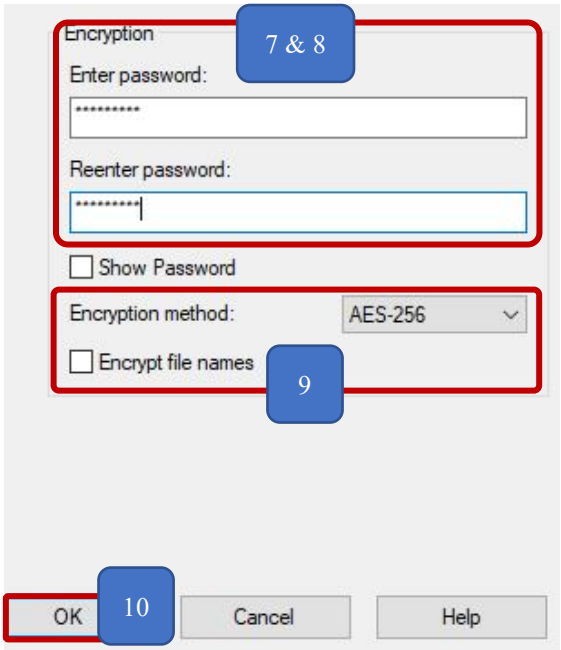


7. Set a password in the "**Enter Password Field**".
8. Reenter same the password in the "**Reenter Password Field**".

   WARNING: It is essential to develop a strong password for protecting sensitive information. To develop a strong password, consider all the following:

   - Use at least eight characters (the longer the better, but no more than sixteen);
   - Use a combination of lower case and upper-case letters interspersed with numbers;
   - Don't use dictionary words in any language;
   - Don't use words spelled backwards, common misspellings, or abbreviations; and
   - Include at least two special characters such as #, $, %, ^.

9. In the "**Add to Archive**" window "**Encryption Method**" drop-down menu, select "**AES-256**".
10. Click "**OK**".



11. End process.

WARNING: For security reasons, **DO NOT** send the password for the encrypted files in the same email with the encrypted files. Instead, provide the password to the recipient by phone or in a separate email.

Table of Contents

1 Introduction

Sensitive information is any data or other information for which public disclosure, or disclosure to users who do not have a need to know to perform their jobs, can harm individuals, the U.S. government, or private organizations. Personally Identifiable Information (PII) is a type of sensitive information that includes but is not limited to social security numbers (SSN), dates of birth, medical information, or the names of minor children.

To help protect PII during email transmission, the U.S. Courts requires incumbent personnel to encrypt sensitive documentation containing PII during email transmission. To unencrypt 7 Zip files, HR personnel should follow the 7 Zip File Extraction Process below.

WARNING: This process shall not be conducted on a personal device. This process is for use on **JUDICARY-ISSUED LAPTOPS ONLY**.

For additional details on handling sensitive judiciary information, refer to the Guide to Judiciary Policy:

- Vol. 2: Ethics and Judicial Conduct
- Vol. 10, Ch. 6: Records Management
- Vol. 15, Ch. 3: IT Security

1.1 Scope

This document provides a step-by-step process for unencrypting 7 Zip files.

2 7 Zip File Extraction Process

2.1 Inputs

- 7 Zip software
- Encrypted **.7z** file selected for extraction
- Password to unlock encrypted **.7z** file

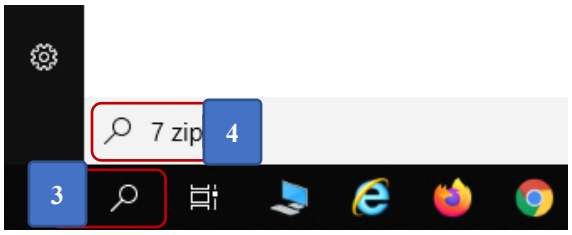
  WARNING: For security reasons, **DO NOT** allow prospective employees to send the password for the encrypted files in the same email with the encrypted files. Instead, instruct prospective employees provide the password to the recipient by phone or in a separate email. Passwords should be a combination of letters, numbers, and special characters, e.g. “007isaBritishSpy!”; “NYC1theBigApple!”

Note: For older judiciary laptops or personal devices, contact your local help desk.

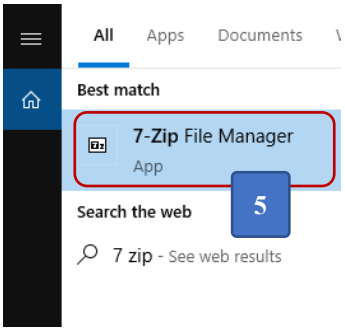
2.2 Procedure: 7 Zip File Extraction Process

1. Log into the judiciary-issued laptop.
2. Remove the encrypted **.7z** file from email selected for extraction and place it in the organizationally designated repository, as applicable.
3. Next, click on the “**Magnifying Glass**” next to the “**Windows Start Menu**” button.
4. Type “**7 Zip**” in the search field.

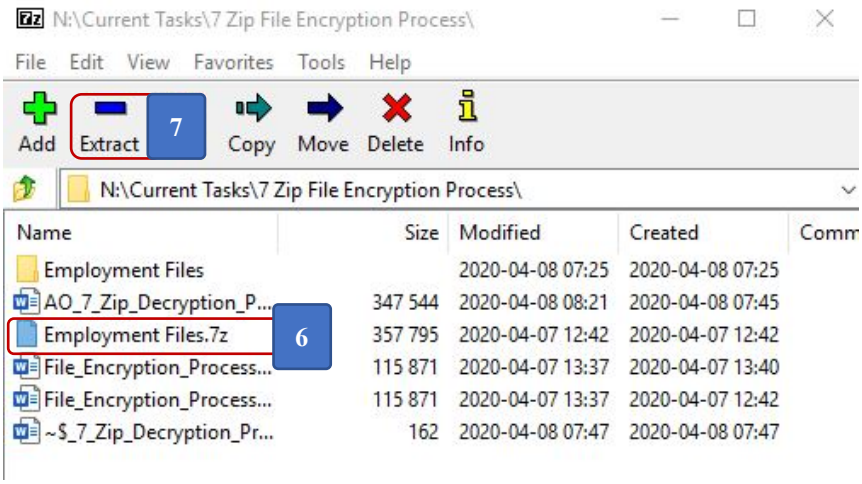
WARNING: If 7 Zip is not installed on the judiciary laptop, contact the AO Help Desk at (202) 502-4357 or by email at AO_Helpdesk@ao.uscourts.gov.



5. Click on "**7 Zip File Manager**" to open the application.



6. Left click once on the desired "**.7z**" file.
7. Left click once on the "**Extract**" button.



8. Check the file path in the "**Extract to:**" filed to ensure the extracted file will be placed where desired (i.e., organizationally designated repository).
9. To set a new location, click on the "**…**" button and select the correct folder (organizationally designated repository), as applicable.
10. In the "**7Z Extract:**" window, enter the password provided by the sender to unlock the "**.7z**" file.

WARNING: For security reasons, **DO NOT** allow prospective employees to send the password for the encrypted files in the same email with the encrypted files. Instead, instruct prospective employees provide the password to the recipient by phone or in a separate email.

11. Click "**OK**".

12. End process.

2.3 Touch Points

Users may need to acquire the 7 Zip software to complete this process.

The sender must provide the password to the recipient.

2.4 Outcome

Process users will be able to successfully read unencrypted files.

Administrative Office of the U.S. Courts
Department of Technology Services

Guide to Creating and Protecting Strong Passwords

September 2018

Poor Password Management Can Be Costly.

We've all seen the headlines:

Poor password management can open the door to costly personal and enterprise headaches.

If someone guesses or steals your password, they can access all of the information tied to that password, including your files, email, bank accounts, credit cards, and personal information. Other judiciary resources could be affected as well, providing the bad guys with an entry point to access and control additional systems on your network, compromising the security of those systems and the data contained on them.

How Are Passwords Stolen?

Hackers have many tools used to steal passwords. Malware (malicious software) can be used to access a computer system without the owner's consent, providing an entry point to gather information about the user and their system.

Phishing attempts try to scam users into surrendering sensitive information by sending an email that looks like a legitimate request for personal or financial data.

End users play an active and important role in password security by avoiding common password mistakes and adopting good password management practices.

How Can I Avoid Common Password Mistakes?

- Don't share passwords.
- Don't use dictionary words in any language.
- Don't use words spelled backwards, common misspellings, or abbreviations.
- Don't write down your passwords.
- Don't store your passwords on your computer in an unencrypted file.
- Don't use the same password on multiple accounts.
- Don't use sequences or repeated characters (12345678, 222222, abcdefg, or adjacent letters on your keyboard, for example qwerty).
- Don't use personal information that could easily be researched, e.g., telephone number, license plate, date of birth, marriage, graduation, or name of pet, child, spouse, etc.
- Don't provide your password in an email or in response to an email request—Internet phishing scams use fraudulent email messages to entice you to reveal your user names and passwords to try to steal your identity.
- Don't provide your password or other personal information in response to unsolicited telephone requests.

What Are Good Password Management Practices?

- Use at least eight characters.
- Use a combination of lower case and upper case letters interspersed with numbers.
- Include special characters such as #, $, %, ^.
- Memorize your passwords, rather than writing them down.

- Change your default passwords when you first log in.
- Change your password frequently—every 60 to 90 days. This protects against use of passwords that may have been compromised.
- Use different passwords for each account.
- Create new passwords rather than recycling passwords you've used previously (they may have already been compromised).

Can I Check To Find Out How Safe a Password Is?

Password checkers, such as the one below, evaluate your password's strength: *https://www.microsoft.com/protect/fraud/passwords/checker.aspx*

How Can I Remember Multiple Complex Passwords That I Frequently Change?

One way is to select a strong, memorable password as a "core." Then add numbers and special characters in front, inside, or at the end of the core. For each application or system add a different character, such as "E" for email or "F" or finance.

For example: Use lines from a childhood verse or a favorite song (e.g., My country tis of thee) plus numbers and characters.

Core Password: M2ctot&

Email Password: M2ctot&E

Finance Password: M2ctot&F

AO Video Provides Help on Managing Multiple Passwords

The AO DTS-ITSO and the Office of Public Affairs (OPA) produced a six-minute video that offers additional assistance on how to create core passwords and customize them for multiple applications and systems.

See the video at: *http://jnet.ao.dcn/information-technology/it-security-judges.*

The following table is based on a Microsoft Online Safety guide and offers a slightly different version of how to create passwords so they can be remembered:

What to do	Suggestion	Example
Start with a sentence or phrase.	Think of something you'll remember.	***Complex passwords are safest*** (four words)
Turn your sentences into a row of letters.	Use the first letter of each word.	***cpas*** (four characters
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	***CpAs*** (four characters)
Add numbers, symbols, and punctuation to increase length.	Embed characters that are meaningful to you.	***Cp3+?As*** (seven characters)
Add a system identifier	Put a system identifier at the beginning or end (e.g., "E" for email)	***ECp3+?As*** (eight characters)

Are There Automated Tools to Help Manage My Passwords?

There's an easy and secure way to keep track of the many passwords you need for your work and personal accounts: a password vault. With a password vault, all you have to remember is the master password to the vault.[1]

A password vault is a software program that electronically protects your passwords, just like a physical vault or safe that locks up your valuables. Unlike a physical key, which can be stolen and immediately used to open a safe's door, the password vault encrypts[2] your passwords and stores them in an electronic format. So, even if your computer is stolen (or the password file is hacked), your passwords cannot be readily understood and used to access your information. Doing so would require unlocking the vault, to which only you hold the "key"!

Check with Your IT Staff for Local Guidance

While there are many free versions of password vaults (albeit with reduced capabilities), your local IT staff may decide to provide licenses for a full-featured version. Or, the staff may simply have knowledge of a particular tool and can help you quickly get up to speed on it. Absent local guidance, consider these password vault examples:

KeePass:
http://www.keepass.info

MiniKeePass (for IOS devices):
https://itunes.apple.com/app/id451661808

Keeper (desktop and mobile support):
https://keepersecurity.com/

Password Safe:
http://www.schneier.com/passsafe.html

Thycotic Secret Server:
http://www.thycotic.com/products_secretserver_overview.html

[1] ITSO Security Tip: *Password Vaults–Taking the Guesswork out of Passwords!*

[2] The Guide to Judiciary Policy, Vol. 15, Ch. 3, Section 330.60.60: Security Responsibilities for Remote Access Users states that "…using an encryption product (e.g., password vault software) to store passwords is acceptable."

Ensure the Vault Does Not Send Information Over the Internet

The password vault should be installed on your desktop, laptop, mobile device, or on your court local area network. When selecting a solution, do not use a password vault that requires you to transmit your passwords across the Internet to a vendor's "secure" server. Your passwords—whether encrypted or not—should never leave your (or the judiciary's) control.
The security provided by non-judiciary systems is not guaranteed.

Coming Changes to Password Policy

Federal guidance[3] on password best practices is in the process of being reevaluated, and the Judiciary will consider any updates ultimately published. In the interim, users may consult **Appendix C: NIST Issues New Password Guidance – Practically Speaking, What Does This Mean?** within the *Password Policy Resource Packet* for more information.

For Additional Information:

IT Security Awareness Tip

- *Strong Passwords Reap Rewards*

[3] NIST SP 800-53, Rev. 5, will replace Rev. 4, and recommends changes to password implementation.

Information Technology Security Office (ITSO) Contacts:

Visit the Department of Technology Services (DTS) ITSO website on JNet at *Information Technology* and click on the ***Security*** heading.

For questions or comments contact the AO-IT Security Office at (202) 502-2350 or email: *AO_ITSO@ao.uscourts.gov*

Original Date Published: January 2011