

Sending Encrypted Court Documents by Email

Audience and Scope

This guide is intended for **attorneys and legal staff** who are required to submit court documents by email. It is written for non-technical users and provides generally accepted methods for protecting confidential information.

This guide does **not** replace:

- Court rules or filing instructions
- Local rules of procedure
- Organizational security or confidentiality policies

Why Encryption Is Required

Court filings often contain confidential, privileged, or personally identifiable information. Encrypting documents:

- Helps prevent unauthorized access
- Reduces risk if an email is misdirected or intercepted
- Supports ethical and professional confidentiality obligations

Best practice: Encrypt the document itself before sending it by email.

Step 1: File level Encryption

Encrypting the document ensures it remains protected even after it leaves your control.

Option A (Recommended): Encrypting a Document in Word, Excel, or PDF

This is the **preferred option for attorneys** because it is simple and built into common legal document formats.

Steps:

1. Open the document.
2. Select **File > Info** or **Protect** (menu names may vary).
3. Choose **Encrypt with Password** or **Password Protect**.
4. Create a strong password.
5. Save the document.

Option B (Advanced): Encrypting a File Using a Password-Protected ZIP File

This option is considered **advanced** and should be used only when Option A is not available.

Important Notes by Platform:

- **Windows:** Does not natively support password-protected ZIP files. Third-party software is required, such as **7-Zip** or another IT-approved tool.
- **macOS:** Does not provide a simple graphical option for password-protected ZIP files. This requires either approved third-party software or use of the Terminal (command line).

Windows (Using 7-Zip or Similar Software)

1. Right-click the document.
2. Select **7-Zip > Add to archive**.
3. Choose **ZIP** as the archive format.
4. Enter a password. Under Encryption, must successfully enter the password twice

5. If available, select **AES-256 encryption**.
6. Click **OK** to create the ZIP file.

macOS (Using Terminal – Advanced Users Only)

Only use this method if you are comfortable with command-line tools.

1. Open **Terminal**.
2. Navigate to the folder containing your document.
3. Enter:
`zip -er filename.zip originalfile.ext`
4. Enter and confirm a password when prompted.

Step 2: Send the Encrypted Document by Email

Once the document is encrypted, attach it to your email.

Instructions for sending encrypted emails will vary based on the email provider (Gmail, Yahoo, Apple, etc.). Please reference your email provider or your organization's IT instructions for how to send encrypted emails. See below for Outlook-specific instructions.

Outlook

1. Create a new email.
2. Address it to the court's official email address.
3. Attach the encrypted document.
4. If available, select **Options** or **Security** and enable **Encrypt**.
5. Send the email.

Note: If email encryption is unavailable, file-level encryption alone is still acceptable unless court rules state otherwise.

Step 3: Share the Password Separately

The password **must not** be included in the same email as the document.

Acceptable Methods:

- Phone call
- Separate follow-up email
- Secure messaging method approved by the court or your organization

Do Not:

- Include the password in the same email
- Place the password in the subject line or file name

Step 4: Confirm Receipt

After sending:

1. Confirm the court received the document.
2. Confirm the document can be opened.
3. Do not resend unencrypted documents to resolve access issues.

Compliance Notes and Best Practices

- Verify the recipient's email address before sending.
- Use strong, unique passwords.
- Retain copies of transmitted documents according to record retention requirements.
- When in doubt, contact IT or follow court specific filing instructions.