DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

November 18, 2021

Control Number: NHQ-01-1121-0004
Expiration Date: 10/31/2023
Affected IRMs: 1.10.3.2.1; 4.10.1; 10.5.1; 10.8.1; 10.10.1; 11.3.1; 25.6.22

MEMORANDUM FOR ALL SERVICES AND ENFORCEMENT EMPLOYEES

FROM: Douglas W. O'Donnell
Deputy Commissioner for Services and Enforcement

Douglas W. Odonnell
Digitally signed by Douglas W. Odonnell
Date: 2021.11.18 16:17:31 -05'00'

SUBJECT: (1) Approval to accept images of signatures and digital signatures
(2) Approval to receive documents and transmit encrypted documents by email

This memorandum supersedes the April 15, 2021, memorandum (Control Number NHQ-01-0421-0001) to provide additional employee guidance and an extended expiration date.

In response to the COVID-19 situation and stakeholder requests, we are taking steps to protect employees and taxpayers while still delivering on our mission-critical functions. We are maximizing the ability to execute on critical duties in a remote working environment where employees, taxpayers and their representatives are working from alternate locations. In accordance with IRM 1.11.2.2.4, *When Procedures Deviate from the IRM*, this memorandum extends temporary deviations that allow IRS employees (1) to accept images of signatures and digital signatures on documents related to the determination or collection of tax liability and (2) to send or receive documents to or from taxpayers using email with encrypted attachments when no other approved electronic alternative is available. These deviations apply to any statement or form traditionally exchanged between IRS personnel and taxpayers during a compliance interaction outside of standard filing procedures. Refer to Attachment 1, Procedures, for additional guidance.

This memorandum is effective upon issuance through October 31, 2023. The signature and email exceptions permitted under this memorandum do not establish a precedent for acceptable use of alternative signatures or email in other circumstances.

Attachments (2)

Attachment 1. Procedures

A. Applicability of this Guidance

1. This guidance covers interactions between IRS employees and taxpayers related to the determination or collection of tax liability ("compliance interactions"). The scope of documents affected include any statement or form traditionally exchanged between IRS personnel and taxpayers during a compliance interaction and outside of standard filing procedures, including but not limited to:

Document Category	Examples
Extensions of statute of limitations on assessment or collection	Forms 872 and 921 series, Forms 900, 952, 977, 2750, 4016, SS-10
Waivers of statutory notices of deficiency and consents to assessment	Forms 870, 890, 2504, 4089-B, 4549, 5564-A, 13449
Agreements to specific tax matters or tax liabilities (closing agreements)	Forms 866, 906, 14490, 14491, 14492
Prior-year (delinquent) tax returns secured through an examination or collection interaction **Caution:** Returns which are not yet due to be filed, including extensions, should be filed in accordance with the instructions for the respective form.	Forms 940/941, 1040, 1120, 1065
Other statements or forms needing the signature of a taxpayer or representative traditionally collected outside of standard filing procedures	Forms 433-A/B/D, 2159, 2297, 3363, 4669, 4670, 8626, 12153
Other statements or documents relevant to development of a case, not limited to IRS forms or signed documents	

Note: IRS has provided two digital alternatives for submitting third-party authorizations (Forms 2848 and 8821), Submit Forms 2848 and 8821 Online and Tax Pro Account. Practitioners should be encouraged to use these applications to the extent possible. If a practitioner indicates they are unable to use these options, you may accept case-specific authorization forms by email.

Caution: Documents that contain a notice required by law (e.g., notice of third-party contacts under IRC 7602(c)(1), a notice of deficiency under IRC 6212, etc.) must be delivered by the means, if any, prescribed by the applicable legal authority.

2. This guidance describes procedures for the exchange of electronic information when the taxpayer or representative requests to use email. Employees should encourage taxpayers to use established secure messaging systems when available before using email.
3. The use of the flexibilities in this interim guidance is voluntary for both the taxpayer and the employee. Employees cannot require taxpayers to use these flexibilities.
4. Employees may contact their respective program policy offices for additional guidance on issues not specifically addressed in this memorandum.

B. Acceptable Signatures

1. The IRS will accept images of documents with original signatures (scanned or photographed) in any common file type such as JPEG, TIFF, PDF, etc.
2. In addition, the IRS will accept digital signatures that use encryption techniques that provide proof of original and unmodified documentation when transmitted by an approved secure messaging or file transfer system or by email as described in Section C below. If a taxpayer does not have this capability, the employee may suggest the use of an imaged signature as described in Section B.1. above.

C. Receiving Emails from Taxpayers or Representatives

1. If the taxpayer or representative asks to send documents by email, the employee must authenticate the identity of the taxpayer or representative in person or by phone. In addition, the employee must advise the taxpayer or representative that communication by unencrypted email is not secure and recommend that they:
    a. Exclude sensitive information, including portions of the taxpayer's TIN or name, from the subject line and body of emails.
    b. Transmit any potentially sensitive information, including personally identifiable information (PII), only via encrypted, password-protected attachments.
2. Direct taxpayers to the User Guide at *IRS.gov/UsingEmail* for additional information about encrypting files and sending documents to IRS by email.
3. After authenticating the taxpayer or representative and explaining the items in Section C.1. above, the employee may verbally provide their official IRS email address. At the same time, verify the taxpayer or representative's email address to associate any incoming email with the proper case file.

4. Remind taxpayers to use strong passwords for encrypting files (at least twelve characters, including a mix of upper- and lower-case letters, numbers and special characters).
5. Employees must follow BOD-specific guidance for national standard timeframes for case actions with respect to acknowledging receipt of the taxpayer or representative's email.
6. If the taxpayer or representative sends a document that requires managerial signature (e.g., an executed Form 872), the employee must take all administrative steps related to the document and forward the complete signature package via an encrypted email to the manager for approval.
7. All actions to support email transmission must be documented contemporaneously in the case file.

D. Sending Emails to Taxpayers or Representatives

1. Initial contact with a taxpayer or representative must never be made by email. The decision to send or receive documents by email is at the discretion of the taxpayer and should only be used if the taxpayer or representative is unable to use another approved electronic alternative.
2. The guidance in this section only extends to the taxpayer and their authorized representative(s). Employees must not email third-party contacts.
3. Before sending the taxpayer or representative any documents containing sensitive but unclassified (SBU) data (including PII and tax information) by email, the employee must:
    a. Authenticate the taxpayer or representative by phone to ensure they are authorized to receive taxpayer information. See IRM 11.3.2.3.2, *Requirements for Verbal or Electronic Requests*.
    b. Obtain the taxpayer or representative's consent to transmit encrypted documents by email (Section D.4-5. below).
    c. Verbally verify the taxpayer's or representative's email address.
4. IRS employees must not email taxpayers or representatives unless they have provided consent to receive email. Follow applicable guidance to ensure that the person providing consent is authorized to do so, particularly if multiple individuals are involved.
5. The employee must obtain consent initially and preserve it as documentation. Advise taxpayers/representatives that consent is valid for the span of the current compliance interaction only and that they may revoke this consent at any time. Before emailing a taxpayer or representative for the first time, the taxpayer and/or representative must email the employee the following statement of consent:

    "I consent to receive encrypted documents by email from [employee name] and associated IRS personnel for the duration of this [examination/ collection activity/appeal/etc.]."

6. After satisfying these requirements for sending email to the taxpayer and/or representative, the employee may send email with encrypted attachment(s). Employees must follow these guidelines **every** time documents are transmitted to a taxpayer and/or representative by email:
    a. Remove all identifying information (e.g., taxpayer name, last four digits of the taxpayer's TIN, taxpayer's name control, etc.) from the subject line and body of the email. Exclude identifying information from the name(s) of attached file(s) as well.
    b. Encrypt and password protect all attachments (see Attachment 2, *Encryption of Outgoing Email Attachments*). Create a strong password that includes at least twelve characters and at least one of each of the following: uppercase letter, lowercase letter, number, and special character.
    c. Inform the taxpayer or representative of the password verbally. **Never transmit the password via email.**
7. All actions to support email transmission must be documented contemporaneously in the case file.

E. Records Management

Records created through electronic interactions with taxpayers are subject to the record management guidance in IRM 1.15, including IRM 1.15.6, *Managing Electronic Records*.

F. Incident Reporting

Immediately report incidents. To report data loss, inadvertent disclosure, or other incidents pertaining to these flexibilities, refer to the procedures described in IRM 10.5.4.3, *Reporting Losses, Thefts and Disclosures*. You can also refer to the *If/Then Guide for Reporting Incidents and Data Breaches* for reporting requirements for specific types of incidents.

G. Case Processing

Follow the case file maintenance guidance from your business unit for instructions on how to manage electronic records from taxpayers and third parties. The examiner is responsible for ensuring that electronic records are maintained in the case file as appropriate.

Attachment 2. Encryption of Outgoing Email Attachments

File Type	Encryption Instruction
Word or Excel (Microsoft Office versions 2016 or 365)	1. Open a Word or Excel document 2. Click on the **File** tab 3. Click on **Info** 4. Click the **Protect Document/Workbook** button 5. Select **Encrypt with Password** from drop-down menu 6. Create a strong password of at least twelve characters 7. Reenter Password – Select **OK** 8. Save the document 9. Inform the taxpayer or representative of the password by phone. **Do not transmit the password via email.**
Adobe Acrobat Pro DC	1. Open a PDF document 2. Click on the **Tools** tab 3. Click on the **Protect** icon 4. Click **Advanced Options** and select **Encrypt with Password** from the drop-down menu 5. Click **Yes** if asked to apply new security settings 6. In the Settings window, under Document Open, check "Require a password to open the document," then enter a strong password of at least twelve characters 7. In the same window, under Options, ensure that Compatibility is set to "Acrobat X and later" and "Encrypt all document contents" is selected 8. Click **OK** 9. In the pop-up box, confirm the password that was created earlier and click **OK** 10. Click **File** and **Save** the document (use **Save As…** if you want to change the filename) 11. Inform the taxpayer or representative of the password by phone. **Do not transmit the password via email**. **Note**: Digitally signed PDFs cannot be encrypted. To transmit a digitally signed PDF to the taxpayer or representative by email, the PDF must be flattened (i.e., printed to PDF) *before* encrypting. Do not overwrite the original signed document when printing to PDF. The original signed document (i.e., un-flattened version) must be maintained in the case file with the employee's valid digital signature.

SecureZIP	1. Open SecureZIP 2. Ensure “Enable Encrypt Files” is checked 3. In the drop-down list to the right of the “Enable Encrypt Files” toggle, select “Traditional: Passphrase” 4. Select **Add Files** 5. Select desired file(s) then click **Add to List** 6. Once all desired files are added, click **OK** 7. Select the folder location and provide a filename then **Save** the zipped file 8. At the prompt enter and confirm a passphrase of at least twelve characters 9. Inform the taxpayer or representative of the password by phone. **Do not transmit the password via email**.