DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

DEPUTY COMMISSIONER

Date: June 12, 2020

Control Number: NHQ-01-0620-0002
Expiration Date: 12/31/2020
Affected IRMs: 1.10.3.2.1;4.10.1; 10.5.1; 10.10.1; 10.8.1; 11.3.1; 25.6.22

MEMORANDUM FOR ALL SERVICES AND ENFORCEMENT EMPLOYEES

FROM: Sunita B. Lough /s/ *sunita lough*
Deputy Commissioner, Services and Enforcement

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 March 27, 2020 memorandum (Control Number NHQ-01-0320-001) with an extended expiration date and additional information on encryption technologies.

As part of our response to the Coronavirus COVID-19 situation, we are taking steps to protect employees 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. With this memorandum, pursuant to IRM 1.11.2.2.4 (When Procedures Deviate from the IRM), we are implementing a temporary deviation that allows IRS employees to accept images of signatures (scanned or photographed) and digital signatures on documents related to the determination or collection of tax liability. We are also implementing a temporary deviation that allows IRS employees to accept documents via email and to transmit documents to taxpayers using some secured messaging systems. This memorandum is effective upon issuance.

The categories of documents included in the scope of this memorandum include: extensions of statute of limitations on assessment or collection, waivers of statutory notices of deficiency and consents to assessment, agreements to specific tax matters or tax liabilities (closing agreements), and any other statement or form needing the signature of a taxpayer or representative traditionally collected by IRS personnel outside of standard filing procedures. Questions on whether this memorandum applies to a specific form or document should be addressed to the applicable Business Operating Division's policy office. This memorandum does not narrow the scope of any category of document that a Business Operating Division's policy office previously stated was included in the March 27, 2020 memorandum.

Signatures

The IRS will accept images of signatures (scanned or photographed), including but not limited to, the following common file types supported by Microsoft 365: tiff, jpg, jpeg, pdf, Microsoft Office suite, or Zip.

The IRS will accept Digital Signatures that use encryption techniques (for example, DocuSign) to provide proof of original and unmodified documentation on one of the following common file types supported by Microsoft 365: tiff, jpg, jpeg, pdf, Microsoft Office suite, or Zip.

Additional Methods to Receive Documents Electronically

To eliminate mailing documents to the extent possible, IRS employees should use all existing and previously allowable means of receiving and transmitting documents, such as, eFax or established secured messaging systems.

The choice to transmit documents electronically is solely that of the taxpayer. If the taxpayer is not able to eFax the executed document or to provide it through established secure messaging, the taxpayer may use email with attachments to transmit the document to the IRS if the following steps are taken:

1. Using existing policies for taxpayer contacts, authenticate the identity of the taxpayer or representative by phone to ensure they are authorized to send and receive taxpayer information. In addition, verbally verify the email address.

2. Advise the taxpayer or representative by phone that communications via unencrypted email over the internet are not secure. Explain that, except for minimal identifying information in the body of the email, for example, name, last four digits of a TIN, they should keep sensitive information out of the subject line and body of emails, as much as possible, and should use password-protected encrypted attachments via SecureZip or other encryption method discussed below.

3. The taxpayer or representative must include a statement, either in the form of an attached cover letter or within the body of the email to the effect, “The attached [name of document] includes [name of taxpayer]’s valid signature and the taxpayer intends to transmit the attached document to the IRS.” If a taxpayer fails to include this statement, request it in a follow up telephone call. Retransmitting attachments is not required.

4. After you receive the document via email, make a notation in the work activity record of the case file about step 2 and include the document as well as the email or cover letter, as appropriate, in the case file.

5. If a taxpayer transmits a document that requires your manager’s signature, such as, an executed Form 872, immediately forward the document via an encrypted email to your manager for the manager’s signature.

Transmitting Documents Electronically to a Taxpayer

If the taxpayer or representative does not have fax capability or the IRS employee does not have eFax capability, an IRS employee, with the taxpayer's consent, may transmit documents to the taxpayer with SecureZip or one of the other encryption methods discussed below. If using an encrypted attachment, the IRS employee must take the following steps:

1. Follow the same procedures in (1), above, AND ask the taxpayer or representative to send you a test email to confirm the email address, with a statement indicating "[Name of taxpayer] consents to receiving [name of documents] by encrypted attachment."
2. Inform the taxpayer or representative by phone call that you will be transmitting the document through a password-protected attachment.
3. Keep sensitive information out of the subject line and body of emails; instead use password-protected encrypted attachments as described in steps 4 and 5 below.
4. These links provide resources on creating and transmitting SecureZip files. (**Do not transmit the password via email.)**
5. Create a strong password that meets the software's protocols. Inform the taxpayer or representative of this password via telephone. **Do not transmit the password via email.**
6. Make a notation in the activity record in the case file regarding the process used.
7. **Successful use of SecureZip** – To reduce issues with taxpayers opening the file, change the Passphrase Type to "Traditional." This link provides tips on setting a Passphrase Type.

For email recipients who don't have zip software, you can create a "self-extracting" file. Please access SEE: Self-Extracting Files link for instructions on how to create a self-extracting file.

As an alternative to SecureZip an IRS employee may follow these steps to encrypt an attachment that is a Microsoft Office 2016, 365, Word, or Excel file:

1. Open Word or Excel document
2. Click on the FILE tab
3. Click on PROTECT DOCUMENT
4. Select ENCRYPT WITH PASSWORD from drop-down menu
5. Create a strong password that meets the software's protocols.
6. Reenter Password – Select OK
7. Inform the taxpayer or representative of this password via telephone. **Do not transmit the password via email.**

As an alternative to SecureZip, an IRS employee may follow these steps to encrypt an attachment that is an Adobe PDF document:

1. Open PDF document.
2. Click on TOOLS tab
3. Click on the PROTECT icon
4. Select ENCRYPT
5. Select ENCRYPT WITH PASSWORD from the drop-down menu
6. Under OPTIONS, set compatibility using the drop-down menu to Acrobat X and later
7. Verify that Encrypt all documents contents is selected
8. Create a strong password that meets the software's protocols.
9. Select Require a Password to open the document and click OK
10. Enter the password that was created earlier in the pop-up box and click OK
11. Click FILE and SAVE the document
12. Inform the taxpayer or representative of this password via telephone. **Do not transmit the password via email.**

Note: Digitally signed PDFs cannot be encrypted.

For further reference: The U.S. Department of the Treasury website contains a link on "How to encrypt/password protect Microsoft Office and Adobe Acrobat (PDF) documents."

Other Procedural Requirements and Important Reminders

Follow existing procedures and include any forms or publications that must accompany signature documents.

Employees are prohibited from using personal email accounts for IRS government work.

For further information regarding this deviation, please contact your Business Operating Division's policy office.

CC: Independent Office of Appeals
Taxpayer Advocate Service

Distribution: IRS.gov (http://www.IRS.gov)