PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 10-20-2023

Control Number: PGLD-10-1023-0002
Expiration Date: 10-31-2025
Affected IRM(s): 10.5.1;
1.10.3; 4.10.1; 10.8.1;
10.10.1; 11.3.1;
25.6.22

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: Peter C. Wade */s/ Peter C. Wade 10-20-2023*
Director, Privacy Policy and Compliance

SUBJECT: Interim Guidance on Email Encryption and Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives

This memorandum issues temporary guidance on Email Encryption and Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives and is effective as of October 31, 2023. Please distribute this information to all affected personnel within your organization.

Purpose: This temporary policy:

- Adds email encryption examples.
- Converts the pandemic-related email flexibility and embeds it into privacy policy for encrypted emails with taxpayers (or their representatives, referred to collectively as “taxpayer(s)”).
- Is limited and applicable to IRS personnel working person to person with taxpayers to address compliance or resolve issues in ongoing or follow-up authenticated interactions (including field compliance, Independent Office of Appeals, Counsel, and Taxpayer Advocate Service personnel).
- Remains in effect only until the IRS fully implements long-term solutions for secure electronic communication capabilities with taxpayers as alternatives to encrypted email.
- No longer applies once your business unit decides (with input from PGLD, IT, and other stakeholders) that it and the taxpayers it serves have available and accessible alternative secure electronic communication methods, such as the Taxpayer Digital Communication secure messaging platform or the Document Upload Tool.

Background/Source(s) of Authority: This temporary interim guidance falls under the authorities listed in the Authority section of IRM 10.5.1.

Procedural Change: The procedural changes in the attached temporary interim guidance apply.

Effect on Other Documents: This temporary interim guidance to IRM 10.5.1 and other listed affected IRMs will expire October 31, 2025. It supersedes the November 18, 2021, memorandum (Control Number NHQ-01-1121-0004) that expires October 31, 2023.

Effective Date: October 31, 2023

Contact: If you have any questions, please contact me, or a member of your staff may contact John J. Walker, Acting Associate Director, Privacy Policy and Knowledge Management, at (267) 466-2416, or John.J.Walker@irs.gov.

Distribution: FOIA Library on IRS.gov (https://www.irs.gov/privacy-disclosure/foia-library)

Attachment Temporary Interim Guidance: PGLD-10-1023-0002

The following temporary changes take effect October 31, 2023, for IRM 10.5.1.

> This memorandum uses ellipses (…) to show existing policy not changed and only shows the paragraphs with changes.

[Existing Policy, adding references and encryption examples]

10.5.1.6.8
(10-31-2023)
Email and Other Electronic Communications

…

(7) For emails with taxpayers and representatives, unless authorized by IRM 10.5.1.6.8.7, Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives, you must follow existing policy in IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives.

(8) Examples of IRS IT-approved encryption technology include:

a. Internal (within the IRS network): Secure email encryption using the Encrypt-Only option. This encrypts the body of the email and attachments.
b. External (outside the IRS network):
   - Recommended: Use alternatives to email. Once your business unit decides (with input from PGLD, IT, and other stakeholders) that it and the taxpayers it serves have available and accessible alternative secure electronic communication methods, such as the Taxpayer Digital Communication secure messaging platform or the Document Upload Tool, you must stop emailing with taxpayers, except in the limited allowable situations in IRM 10.5.1.6.8.1. For alternatives to email, see IRM 10.5.1.6.8.6, the Other Secure Electronic Communication Methods section. For more information about when you can offer these alternatives, refer to your business unit procedures.
   - If alternatives are not available: Secure email encryption using the Encrypt-Only option. This encrypts the body of the email and attachments.

> **Reminder:** Encryption protects only the body of the email and attachments, not the subject line. Do not put SBU data in the subject line.

(9) See the internal Encryption site for more information about

encryption.…

10.5.1.6.8.1
(10-31-2023)
Emails to Taxpayers and Representatives

(1) Except as authorized by the temporary policy in IRM 10.5.1.6.8.7, Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives, do not send emails that include SBU data (including PII and tax information) to taxpayers or their authorized representatives, even if requested, because of the risk of improper disclosure or exposure.

…

[Temporary Policy for Recurring, Authenticated Interactions]

10.5.1.6.8.7
(10-31-2023)
Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives

(1) This policy is temporary until the IRS implements alternative secure electronic communication channels to end the need for encrypted email with taxpayers.
(2) This temporary guidance is limited and applicable to IRS personnel working person to person with taxpayers to address compliance or resolve issues in ongoing or follow-up authenticated interactions (including field compliance, Appeals, Counsel, and Taxpayer Advocate Service personnel). All other personnel must follow existing policy in IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives.
(3) The use of the flexibilities in this temporary policy is voluntary for both the taxpayer and the employee.
(4) Once your business unit decides (with input from PGLD, IT, and other stakeholders) that it and the taxpayers it serves have available and accessible alternative secure electronic communication methods, such as the Taxpayer Digital Communication secure messaging platform or the Document Upload Tool, you must stop emailing with taxpayers, except in the limited allowable situations in IRM 10.5.1.6.8.1.
(5) Taxpayers must agree to receive email (see (9) Consent). Do not require taxpayers to send or receive email.
(6) For ongoing or follow-up authenticated interactions with taxpayers, you may send encrypted email to the taxpayer when they agree if you:
    a. Manually authenticate the taxpayer's identity and authority to receive the information (see (7) Authentication and (8) Authorization);
    b. Get taxpayer consent (see (9) Consent);
    c. Encrypt the email with IT-approved technology (see (10) Encryption); and
    d. Document such in the case file (see (11) Documentation).

    Caution: Encryption does not encrypt the subject line. Follow existing policy for protecting SBU data in the subject line of the email in IRM 10.5.1.6.8, Email and Other Electronic Communications.
(7) **Authentication:** Follow applicable business unit functional policy to manually authenticate the taxpayer's identity either by phone, in person, or via online meetings. See IRM 10.5.1.2.9, Authentication.

(8) **Authorization:** Verify the taxpayer's authority to receive the information. See IRM 10.5.1.2.10, Authorization.

(9) **Consent:** Do not make initial contact by email. If the taxpayer does not have access to an alternative secure electronic communication method and asks to receive email, get their written consent following these steps before securely emailing them:

a. Verbally verify your IRS email address and the taxpayer's email address.
b. Tell taxpayers that consent is valid for the span of the current interaction only and that they may revoke this consent at any time.
c. Ask the taxpayer to email the following statement of consent before emailing them for the first time:
"I consent to receive and send encrypted email with [employee name] and associated IRS personnel for the duration of this [examination/ collection/appeal/etc.] interaction."

(10) **Encryption:** Use IT-approved encryption methods outlined in paragraph (8) of IRM 10.5.1.6.8, Email. Direct taxpayers to the website IRS.gov/UsingEmail for more information about encrypting files and sending and receiving documents to and from IRS by encrypted email.

(11) **Documentation:** Document encrypted email actions in the case file. Follow the case file maintenance guidance from your business unit.

Reminder: Electronic interactions with taxpayers become federal records subject to the record management guidance in the IRM 1.15 series, including IRM 1.15.6, Managing Electronic Records.

(12) Contact your respective program policy offices for guidance on issues not specifically addressed here.