PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D C. 20224

Date of Issuance: 09-24-2025

Control Number: PGLD-10-0925-0007
Expiration Date: 10-31-2026
Affected IRM(s): 10.5.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: John Hardman /s/ *John K. Hardman*
Acting Director, Privacy Policy and Compliance

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

This memorandum issues interim guidance on Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives and is effective as of September 24, 2025. Please distribute this information to all affected personnel within your organization.

Purpose: This temporary policy:

- Is temporary until October 31, 2026.
- 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, IRS Independent Office of Appeals, Chief Counsel, and Taxpayer Advocate Service personnel).
- Mandates business units to transition to the available and accessible alternative secure electronic communication methods.

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, 2026. It supersedes the October 23, 2023, memorandum (Control Number PGLD-10-1023-0002) that expires October 31, 2025.

Effective Date: September 24, 2025

Contact: If you have any questions, please email the Associate Director, Privacy Policy,

at *Privacy.

Distribution: FOIA Library on IRS.gov

Attachment Temporary Interim Guidance: PGLD-10-0925-0007

The following temporary changes take effect September 24, 2025, 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
(09-24-2025)
Email and Other Electronic Communications

…

(5) For external electronic communications, IRS personnel should use IRS-approved alternatives to email such as secure messaging or secure portals when available. Review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information about emailing outside the IRS, review the following subsections:

- IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives
- IRM 10.5.1.6.8.2, Emails to Other External Stakeholders
- IRM 10.5.1.6.8.3, Emails to IRS Accounts
- IRM 10.5.1.6.8.4, Emails with Personal Accounts
- IRM 10.5.1.6.8.7, Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives

…

10.5.1.6.8.1
(09-24-2025)
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
(09-24-2025)
Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives

(1) This policy is temporary until October 31, 2026. After this date, you must use alternative secure electronic communication channels to communicate with taxpayers and their representatives.
(2) This temporary guidance is limited and applicable to IRS personnel working person to person with taxpayers and representatives to address compliance or resolve issues in ongoing or follow-up authenticated interactions (including field compliance, IRS Independent Office of Appeals, Chief 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 flexibility in this temporary policy is voluntary for both the taxpayer and the employee.
(4) Once this policy expires, the use of alternatives to email is mandatory for both employees and taxpayers if they want to communicate electronically. All business units must transition to the available and accessible alternative secure electronic communication methods, outlined in IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods.
(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 take these steps:
    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)
    d. Document such in the case file (see (11) Documentation)
(7) **Authentication:** Follow applicable business unit functional policy to manually authenticate the taxpayer's identity either by phone, in person, or via online meetings. Review IRM 10.5.1.2.9, Authentication.
(8) **Authorization:** Verify the taxpayer's authority to receive the information. Review 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] for the duration of this [examination/ collection/appeal/etc.] interaction."
(10) **Encryption:** Use IT-approved encryption methods outlined in paragraph (7) 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.

Caution: Encryption does not encrypt the subject line. Follow existing policy for protecting SBU data in the subject line of the external email in IRM 10.5.1.6.8, Other Electronic Communications.

(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.