



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 09-25-2026

Control Number: PVCY-10-0926-0009

Expiration Date: 09-30-2028

Affected IRM(s): 10.5.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: Stephen Brooks /s/ *Stephen Brooks*
Acting Director, Data Oversight and Records

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

This memorandum issues temporary guidance on Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives and is effective as of September 30, 2026. Please distribute this information to all affected personnel within your organization.

Purpose: This temporary policy:

- Is temporary until September 30, 2028.
- 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 (limited to field compliance, Appeals, Counsel, and Taxpayer Advocate Service personnel).
- Mandates business units to support transition of their programs and personnel to available and accessible alternative secure electronic communication methods, as appropriate to business needs.

Background/Source(s) of Authority: This temporary interim guidance falls under the authorities listed in the Authority section of [IRM 10.5.1](#). This guidance helps IRS meet requirements for privacy and security of taxpayer data as described in federal laws and regulations. Use of email to communicate taxpayer information creates risks for improper disclosures.

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 September 30, 2028. It supersedes the September 24, 2025, memorandum (Control Number PGLD-10-0925-0007) that expires October 31, 2026.

Effective Date: September 30, 2026

Contact: If you have any questions, please email the Associate Director, Strategy and Oversight, at [*Privacy](#).

Distribution: [FOIA Library on IRS.gov](#)

Attachment Temporary Interim Guidance: PVCY-10-0926-0009

Temporary Interim Guidance: PVCY-10-0926-009

The following temporary changes take effect September 30, 2026, 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

(09-30-2026)

Email and Other Electronic Communications

...

(5) For external electronic communications, IRS personnel must 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

(09-30-2026)

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

(09-30-2026)

Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives

- (1) This policy is temporary and will remain in place until September 30, 2028. After this date, you must use an available and accessible alternative secure electronic communication channel to communicate with taxpayers and their representatives (hereafter combined and referred to as taxpayers) instead of email.

Note: In this context, available means an alternative secure communication channel that is available within the IRS and accessible means that the solution is designed for access by 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 (limited to 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 flexibility in this temporary policy is voluntary for both the taxpayer and the employee.
- (4) Business units need to identify and adopt available and accessible alternative secure electronic communication methods that meet business needs before this guidance expires on September 30, 2028. This allows time for business units to plan for and implement alternative methods that meet this requirement. Business units must require personnel to use the implemented method instead of email. Exceptions only apply when such a method is unavailable and inaccessible. Business units must document exceptions with approved entitlements, using a process approved by Privacy Oversight. For examples of alternative methods, refer to [IRM 10.5.1.6.8.6](#), Other Secure Electronic Communication Methods.
- (5) You must obtain consent from the taxpayer to communicate by email (see [\(9\) Consent](#)).
- (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:
- Manually authenticate the taxpayer's identity and authority to receive the information (see [\(7\) Authentication](#) and [\(8\) Authorization](#))
 - Get taxpayer consent (see [\(9\) Consent](#))
 - Encrypt the email with IT-approved technology (see [\(10\) Encryption](#))
 - 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 external email in [IRM 10.5.1.6.8](#), 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. 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:
- Verbally verify your IRS email address and the taxpayer's email address.
 - Tell taxpayers that consent is valid for the span of the current interaction only and that they may revoke this consent at any time.
 - 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 \(7\)](#) of [IRM 10.5.1.6.8](#), Email. Direct taxpayers to the website [IRS.gov/UsingEmail](https://www.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, including the taxpayer's consent, 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.