PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 07-08-2024

Control Number: PGLD-10-0724-0016
Expiration Date: 07-08-2026
Affected IRM(s): 10.5.1
1.10.3; 10.8.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: John J. Walker */s/ John J. Walker*
Acting Director, Privacy Policy and Compliance

SUBJECT: Privacy Policy Encryption Updates

This memorandum issues privacy policy interim guidance on encryption and is effective as of August 16, 2024. Please distribute this information to all affected personnel within your organization.

Purpose: This interim guidance implements privacy policy changes related to IRS Information Technology encryption requirements. Privacy policy explains what sensitive information to encrypt to protect privacy. For IT policy on email encryption, refer to IRM 10.8.1, the Electronic Mail (Email) Security subsection (and related interim guidance).

Background/Source(s) of Authority: This interim guidance falls under the authorities listed in the Authority subsection of IRM 10.5.1, Privacy Policy.

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

Effect on Other Documents: This interim guidance adopts the encryption section of the temporary Interim Guidance Memorandum PGLD-10-1023-0002, Interim Guidance on Email Encryption and Temporary Flexibility for Encrypted Emails with Taxpayers and Representatives. We will incorporate this interim guidance into IRM 10.5.1, by July 8, 2026.

Effective Date: August 16, 2024

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

Distribution: FOIA Library (external) on IRS.gov.

Attachment Interim Guidance: PGLD-10-0724-0016

Interim Guidance: PGLD-10-0724-0016

The following changes take effect August 16, 2024**, for** IRM 10.5.1.

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

10.5.1.6.2
(08-16-2024)
Encryption

(1) ~~Encryption is a crucial tool in the IRS's protection of~~ The IRS uses its IT-approved encryption as a crucial tool to protect SBU data (including PII and tax information). [OMB A-130, Security, SC-13, SI-03]
(2) Protect all SBU data (including PII and tax information) with IT-approved encryption methods and access controls, limiting access only to approved personnel with a need to know. This includes, but is not limited to, SBU data in email, removable media (such as USB drives), on mobile computing devices, and on computers and mobile devices.
Note: The IRS restricts the ability to save data on removable media storage devices. Refer to IRM 10.8.1, the Media Use subsection, and removable media guidance on internal IRS Service Central site.
(3) For IT policy on email encryption, refer to IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, in the Electronic Mail (Email) Security subsection (and related interim guidance).
(4) For more details about emailing and encrypting SBU data, see IRM 10.5.1.6.8, Email and Other Electronic Communications.
Note: Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information and requirements about emailing outside the IRS, see 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; and IRM 10.5.1.6.8.4, Emails with Personal Accounts; and IRM 10.5.1.6.8, Email and Other Electronic Communications.
(5) Refer to the internal Encryption site for encryption instructions. ~~Instructions for using SecureZip to encrypt attachments also are available on the internal IRS Service Central site. See the Virtual Library for more information about encrypting documents, emails, and email attachments on the internal Encryption site.~~
~~(6) Refer to specific requirements in these IRMs:~~
- ~~IRM 1.15 series, Records and Information Management.~~
- ~~IRM 10.2 series, Physical Security Program.~~

- ~~IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, in the Cryptographic Protection, Access Control, Media Protection, and Physical and Environmental Protection sections.~~

10.5.1.6.8
(08-16-2024)
Email and Other Electronic Communications

…

(7) 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 in transit.
   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 (external), 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, Other Secure Electronic Communication Methods. 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 in transit.

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

(8) Refer to the internal Encryption site for encryption instructions.
(9) Refer to these IRMs for more policy on email and other electronic communications:

- IRM 1.10.3, Standards for Using Email.
- IRM 1.15.6, Managing Electronic Records.
- IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, in the Electronic Mail Security and Use of External Information Systems sections.
- IRM 10.8.27, Personal Use of Government Furnished Information Technology Equipment and Resources.
- ~~IRM 11.3.1, Disclosure of Official Information, Introduction to Disclosure, in the Electronic Mail and Secure Messaging section.~~

10.5.1.6.8.3
(08-16-2024)
Emails to IRS Accounts

(1) IRS personnel must use IRS email for email communications with other IRS personnel about official business matters. They must encrypt all internal email messages with SBU data (including PII and tax information) using IT-approved encryption. ~~, which includes secure messaging or password-protected encrypted attachments.~~

Caution: Encryption methods do not encrypt the subject line or the header (email address information).

…

10.5.1.6.8.4
(08-16-2024)
Emails with Personal Accounts

(1) No officer, employee, or contractor of the IRS may use a personal email account to conduct any official business of the government. [PATH] Three limited allowable circumstances include:

Note: In these circumstances, you must copy (or send to or from) an IRS email account at the same time to make sure you keep a record of the communication in the IRS email system for transparency and information management purposes.

a) Personal Information – You may send your own SBU data (including your PII and your tax information) to or from your personal email accounts, if ~~it is in a password- protected encrypted attachment~~ you encrypt it with IT-approved encryption.

…

c) Exigent circumstances, such as in emergencies. This includes when the IRS network is down and there is an urgent need to communicate or in disaster recovery situations, and you do not have other options. Refer to IRM 10.8.60, Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance, the Activation and Notification Phase subsection. ~~and IRM~~ ~~10.8.62.~~ Limit SBU data to that necessary for the situation. Encrypt necessary SBU data ~~in password-protected attachments, if possible, in emergencies~~ with IT-approved encryption.

…

10.5.1.6.8.5
(08-16-2024)
Limited Exceptions to Email SBU Data Encryption

...

(5) Limited exception: IRS employees sending their personal SBU data via IT-approved encrypted email ~~or encrypted attachment~~. Personal SBU data is information pertaining only to you.

a) You may choose to send only your personal SBU data outside the IRS via IT-approved encrypted email.
~~b) You must send this information only if you encrypt the email or attachment(s) and send only your personal SBU data.~~
b) This exception does not include IRS usernames and passwords.
c) For privacy policy on encryption, see IRM 10.5.1.6.2, Encryption.
d) Refer to the internal Encryption site for encryption instructions.

...

10.5.1.6.18.1
(08-16-2024)
Shared Calendar

...

(7) For Non-Taxpayer-Related Meetings or Appointments:
a) An entry on the calendar for meetings with external parties doing business with the IRS (Enrolled Agents, for example) that does not concern specific taxpayers, would consist of the name of the external representative, the name of the organization (if applicable), or the subject matter of the meeting.
b) You may send any meeting-related non-taxpayer-related PII or SBU data in a separate email (with ~~encrypted, password-protected attachments using~~ IT-approved encryption), with directions in the calendar invite to look for the separate email.
c) Examples of situations where you may use this practice include, but are not limited to:
    i. Where Counsel hosts informational meetings with external parties, such as trade groups or other professional organizations, in conjunction with its published guidance program.
    ii. Where IRS organizations meet with external parties to plan or deliver presentations or for procurement matters.

~~iii. Examples of emails requiring encrypted PII or SBU data attachments in these scenarios include details on speakers (such as resumes) or procurement issues (such as contract information).~~

...