DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

June 21, 2016

Control #: PGLD-10-0616-0003
Affected IRM: 10.5.1
Expiration Date: June 21, 2017

MEMORANDUM FOR DISTRIBUTION

FROM: Frances W. Kleckley */S/ Frances W. Kleckley*
Director, Privacy Policy and Compliance

SUBJECT: Using IRS and Personal Email Accounts

This Emergency Interim Guidance (IG) memorandum is to issue PGLD-10-0616-003, Using IRS and Personal Email Accounts.

Purpose: The IG reiterates existing policy by providing specific procedures that employees must follow when they send emails to stakeholders, taxpayers, other IRS employees, and themselves.

Background/Sources of Authority: IRM 10.5.1 is issued under the authority of the Internal Revenue Code, Privacy Act of 1974, the Taxpayer Browsing Protection Act of 1997, the E-Government Act of 2002 (to include accompanying guidance outlined in OMB memoranda), the Consolidated Appropriations Act of 2005, §522, Treasury Directives, and other federal guidance. Specific mandates for this IG include the Protecting Americans from Tax Hikes (PATH) Act of 2015, §402, Division Q of the Consolidated Appropriations Act of 2016, and Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*,. For a full listing of privacy law and authorities relevant to this IRM section, refer to Exhibit 10.5.1-2, *References*.

Procedural Change: The following procedural changes apply when employees send emails to other stakeholders, taxpayers, other IRS employees, and themselves.

Policy for Using IRS and Personal Email Accounts

In December 2015, Congress passed a law specifically to address the use of personal email accounts at the IRS. The Protecting Americans from Tax Hikes (PATH) Act of 2015, §402, Division Q of the Consolidated Appropriations Act of 2016 reads:

> "No officer or employee of the Internal Revenue Service may use a personal email account to conduct any official business of the government."

The IRS has always required employees to use their IRS email accounts for sending or receiving email when conducting official business of the government, with a few exceptions. The policy and business rules outlined here address common email situations and provide guidance for better understanding of the law in the context of everyday work situations.

For existing IRS email policy, refer to these IRMs:

- IRM 10.5.1, *Privacy Policy* (in the Email section), incorporating June 2015 IG and Memorandum of Understanding on Sending Sensitive But Unclassified Information and/or Work-Related Documents to External Email Addresses
- IRM 1.10.3, *Standards for Using Email*
- IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance* (in the Electronic Mail Security section)
- IRM 10.8.2, *Roles and Responsibilities* (in the Employees section)
- IRM 11.3.1, *Introduction to Disclosure* (in the Electronic Mail and Secure Messaging section)

Two guiding principles support the key considerations of all legislation, directives, and guidance for the use of email in conducting official business.

1) Emails used for business communications become records of IRS operations, and the IRS must manage them accordingly. Employees must always use their IRS email accounts when using email to conduct the official business of the IRS. Law enforcement employees should refer to their divisional or law enforcement manuals for special rules.
2) IRS employees hold a legal responsibility to protect all IRS SBU data, including the PII entrusted to us by taxpayers, fellow employees, and other individuals.

Emailing External Stakeholders

A. Taxpayers

1. In general, IRS employees may not use email to conduct business with taxpayers, even if requested, because of the risk of improperly disclosing or exposing their SBU data (including PII). When taxpayers request email contact and accept the risk of such, limited allowable instances include:

a. Message sent under a previously authorized IT-approved secure email program (rare). For example, see the LBI Secure Email program here: http://lmsb.irs.gov/hq/bsp/SEMS/index.asp
b. Brief, unencrypted message confirming the date, time, or location of an upcoming appointment, but not the nature of the appointment. Include no SBU data (including PII) in the email, subject line, or attachment. Permit no follow-up email discussion of any taxpayer account or case.
c. Link to the publicly available forms and publications sections of IRS.gov. Avoid sending information about specific tax matters (revenue rulings, court cases, and specific IRS forms), which may unintentionally disclose the nature of a tax matter to an unauthorized third party.

2. When responding to unsolicited emails from taxpayers or tax professionals, respond by letter or phone; if address or phone number are not available, respond by email. Employees must:
   a. Delete any SBU data (including PII) appearing in the original email, and
   b. Discourage the taxpayer from continuing the discussion by email. Sample response:

      To ensure your privacy, we discourage you from sending your personal information to us by email. Further, IRS doesn't allow its employees to exchange unencrypted personally identifiable or other sensitive information with email accounts outside of the IRS network, even with your permission. For further discussion about the matters included in your original email, please contact us by telephone, fax, or mail.

B. Other External Stakeholders

Similar rules apply to authorized IRS email exchanges with external stakeholders, such as contractors (without IRS email accounts), applicants, other government agencies, journalists, and professional organizations.

1. Send SBU data (including PII) through password-protected encrypted attachments or through a previously authorized IT-approved secure email program (example here).
2. Email taxpayer data outside the Service only when specifically authorized by established written procedures.
3. Email taxpayer data to officials and employees of another government agency only when the individual recipient has:
   - A need to know, and
   - Authorization to receive it by email
   - See IRM 11.3, Disclosure of Official Information, for detailed guidance.
4. Interact with applicants or prospective contractors by email only to answer questions about their information, qualifications, or administrative matters; minimize the exposure of their personal information.
5. Follow the procedures in A2, above, when receiving unsolicited emails from external parties that contain SBU data (including PII).

6. Tell those who must provide IRS with their PII to facilitate a business arrangement to fax or mail that information or upload it to a secure system, such as USAJobs.

Emailing Other IRS Accounts

1. Employees must use IRS email for email communications with other IRS employees about official business matters. They must encrypt all internal email messages that contain SBU data (including PII) with secure messaging or in password-protected encrypted attachments.
2. IRS does not define email for Union purposes as official business.

Emailing with Personal Accounts

Three limited allowable circumstances include:

1. Personal Information – Employees may send their own SBU data (including PII) to or from their personal email accounts, as long as it is in a password-protected encrypted attachment. Examples may include, but are not limited to:
   a. Personnel forms or records
   b. Financial records being used to prepare an OGE Form 450 or OGE Form 278 or other form for financial reporting related to the job
   c. Records needed for a personal transaction
   d. Job application, resume, self-assessment or appraisal
   e. Health records or fitness for duty information
   f. Travel itinerary (by adding personal email address for ConcurGov notifications related to their own travel, not approvals for others)
2. Training or publicly available information– Employees may transmit content, including links, to and from themselves when IT Security constraints prevent access. Examples of this include online training or meetings, such as webinars and seminars, as well as publicly available information.
3. 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. See IRM 10.8.60 and 10.8.62. Limit SBU data to that necessary for the situation. Examples may include, but are not limited to:
   a. Reporting for work
   b. The condition or availability of the workplace
   c. An emergency situation
   d. The well-being of IRS employees

   Note: In all instances, employees must copy an IRS email account at the same time to ensure they retain a record of the communication in the IRS email system for transparency and information management purposes.

For further guidance and frequently asked questions on email scenarios, see the Email section of the PGLD Privacy and Disclosure Virtual Library on the Disclosure and Privacy Knowledge Base.

Effect on Other Documents: PGLD will incorporate this guidance into IRM 10.5.1, *Privacy and Information Protection, Privacy Policy,* no later than June 21, 2017.
Effective Date: Immediately

Contact: If you have any questions, please contact me, or a member of your staff may contact Greg Ricketts, Associate Director, Privacy Policy and Knowledge Management, at 901-546-3078, or email *Privacy (privacy@irs.gov).

Distribution

Commissioner of Internal Revenue
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Commissioner, Large Business and International Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax-Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief of Staff
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Communications and Liaison
Chief Counsel
Chief, Criminal Investigation
Chief Financial Officer
Chief, Planning, Programming and Audit Oversight
Chief, Risk Officer
Chief Technology Officer
Director, Affordable Care Act Office
Director, Office of Compliance Analytics
Director, Office of Online Services
Director, Office of Professional Responsibility
Director, Office of Research, Analysis and Statistics
Director, Privacy, Governmental Liaison and Disclosure
Director, Return Preparer Office
Director, Whistleblower Office
Executive Director, Equity, Diversity and Inclusion
IRS Human Capital Officer
National Taxpayer Advocate
Treasury Inspector General for Tax Administration (TIGTA)
Associate Chief Information Officer, Cybersecurity
www.IRS.gov