PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

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

Date of Issuance: 07-09-2025

Control Number:
PGLD-10-0725-0004
Expiration Date: 07-09-2027
Affected IRM(s): 10.5.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

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

SUBJECT: Office Privacy in Shared Spaces with Non-IRS Agency Employees

This memorandum issues guidance on Office Privacy and is effective as of July 09, 2025. Please distribute this information to all affected personnel within your organization.

Purpose: This interim guidance points to Privacy Act and Internal Revenue Code requirements and adds new subsections to clarify privacy protections in the office environment and highlights key existing policies for office privacy.

> **Note:** This policy covers privacy protections only. For more guidance on office requirements, refer to the internal Return to In-Person Work site.

Background/Source(s) of Authority: This interim guidance falls under the authorities listed in IRM 10.5.1.1.6, Authority.

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

Effect on Other Documents: We will incorporate this interim guidance into IRM 10.5.1, Privacy Policy by July 09, 2027.

Effective Date: July 09, 2025

Contact: Please email questions to the Associate Director, Privacy Policy, at *Privacy.

Distribution: FOIA Library (external) on IRS.gov
Attachment Interim Guidance: PGLD-10-0725-0004

Interim Guidance: PGLD-10-0725-0004

The following changes take effect July 9, 2025**, for** IRM 10.5.1.

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

10.5.1.1.2
(07-09-2025)
Audience

(1) The audience to which the provisions in this manual apply includes:

a. All IRS organizations.
b. All IRS employees with any access to sensitive but unclassified (SBU) data, including personally identifiable information (PII) and tax information (FTI).
c. All IRS personnel, which includes those outlined in paragraph (2) who have any staff-like access as defined in IRM 10.23.2.1, Program Scope and Objectives.

…

(2) For this IRM, IRS personnel or users includes:

- IRS employees
- IRS seasonal or temporary employees
- IRS interns
- IRS detailees
- IRS consultants
- IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers)
- Non-IRS employees from other agencies.
- The Department of the Treasury (Treasury) and its other bureaus.

…

(3) The term “authorized personnel” applies to whether federal law, policy, and procedure authorizes them to take an action. To be authorized, all personnel must have a need to know under federal law, policy, and procedure, and must complete required training (such as IRS annual and role-based privacy, information protection, and disclosure training requirements, unauthorized access (UNAX) awareness briefings, records management briefings, and all other specialized privacy training) and background investigations before given access to SBU data (including PII and FTI). Review IRM 10.5.1.2.10, Authorization. [OMB A-130]

10.5.1.2.4
(07-09-2025)
Federal Tax Information (FTI)

...

(4) The Internal Revenue Code (IRC) protects FTI from unauthorized disclosure under IRC 6103(b)(2). It also includes criminal and civil penalties for unauthorized access and willful or negligent unauthorized disclosure under IRC 7213 and 7431. Refer to IRM 11.3.1.4, Disclosure and Safeguarding of Returns and Return Information.

(5) You may mark tax information as FTI to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking. FTI is a category of SBU data. When FTI relates to an individual, it also is PII. For marking purposes, use FTI for all tax information.

Note: Not all SBU data or PII is FTI, just as not all FTI is PII.

...

10.5.1.2.7
(07-09-2025)
Privacy Act Information

(1) The Privacy Act forms the core of IRS privacy policy. It protects certain individuals from an invasion of personal privacy by requiring federal agencies to (among other things):

a. Limit identifiable personal information to what is relevant, accurate, necessary, and timely (RANT).
b. Prevent unauthorized disclosure.
c. Allow authorized access.
d. Issue rules of conduct and privacy awareness training.
e. Use safeguards.

The Privacy Act also includes criminal and civil penalties for willful unauthorized disclosures and violations of the act under sections (i) and (g). For details, refer to IRM 10.5.6.2 , Privacy Act General Provisions, and its subsections.

...

(5) You may mark non-tax Privacy Act information as PII to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking. Privacy Act information is PII because it identifies individuals. It can also be FTI if it relates to a tax return or an individual's liability or potential liability under the tax laws. That means it is also a category of SBU data. As with any other SBU data, you must mark it as sensitive and allow access only to those with an authorized need to know. For marking purposes, use PII for all non-tax Privacy Act information and FTI for all tax related information.

Note: Not all PII is Privacy Act information, just as not all PII is tax information.

...

10.5.1.5.3
(07-09-2025)

Office Privacy

(1) To protect privacy in the office environment, IRS personnel and non-IRS employees from other agencies must follow all the policies in IRM 10.5.1, Privacy Policy. All requirements listed align with IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities. This subsection highlights key policies for office privacy that safeguard sensitive information as required by laws such as the Privacy Act (PA), Internal Revenue Code (IRC), and Federal Information Security Modernization Act (FISMA).
Note: This policy covers privacy protections only. For more guidance on office requirements, refer to the internal Return to In-Person Work site.
(2) To protect privacy in spaces shared with other non-IRS agencies, follow this subsection and its subsection, IRM 10.5.1.5.3.1, Shared Spaces.
(3) It is the policy of the IRS to protect privacy and safeguard confidential federal tax information. Review IRM 1.2.1.17.2, Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information, and IRM 10.5.1.1.1, Purpose of the Program.
(4) You are always responsible for protecting the sensitive information you work with. Do not expose sensitive but unclassified (SBU) data, including personally identifiable information (PII) and federal tax information (FTI), to others who do not have an authorized need to know. Review:
- IRM 10.5.1.2.4, Federal Tax Information (FTI)
- IRM 10.5.1.2.7, Privacy Act Information
- IRM 10.5.1.4.1, Employees and Personnel
- IRM 10.5.1.2.8, Need to Know
- IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data.

(5) Follow IRM 10.5.1.5.1, Clean Desk Policy. This applies to all personnel, including IRS employees, contractors, and non-IRS agency employees in all work environments. To protect SBU data when not in your possession, you must lock it up.
(6) Under the clean desk policy, personnel who work with SBU data must have access to lockable storage. Review IRM 10.5.1.5.1, Clean Desk Policy, IRM 10.2.14, Physical Security Program, Methods of Providing Protection.
(7) Properly dispose of SBU data following IRM 10.5.1.6.10, Disposition and Destruction, and its subsections.
(8) The IRS profiles certain IRS positions needing more privacy and security, per IRS Facilities Management and Security Service's (FMSS) IRS National Workspace Standards (NWS) (pdf). IRS managers and other IRS employees with such positions, but not assigned to profiled space, must take precautions to protect privacy and request proper space through their immediate supervisor. Refer to IRM 10.5.1.4.1, Employees and Personnel, Return to In-Person Work Q&As, IRM 1.14.3.3, NWS, and IRM 1.14.3.4.1, Office Furniture Standards. Examples of improper space for enhanced privacy include:
    a. IRS employees profiled for general office space but temporarily assigned to a smaller shared room discussing FTI or private personnel matters without access to other spaces for the conversations.
    b. IRS managers of direct supervisory reports profiled for a private office but not assigned one.
    c. IRS employees profiled for stand-alone suites or enclosed offices but not assigned to those spaces.

d. IRS employees profiled for open/private space but not assigned to those spaces.

(9) When handling documents with SBU data, mark them as sensitive, preferably with a sensitivity label. Use a sensitive but unclassified (SBU) Cover Sheet, Other Gov TDF 15-05.11, to prevent unauthorized or inadvertent disclosure when those without a need to know are present or casual observation would reveal SBU data. Review IRM 10.5.1.6.5, Marking.

(10) Secure your equipment. You are responsible for securing the equipment assigned to you. Store your laptop and equipment in secure locations, such as via cable lock to a permanent furniture fixture, in a locker, or designated storage area. If you do not have a cable lock request one via IRS Service Central. Review IRM 10.5.1.6.3, Computers and Mobile Computing Devices, and Return to In-Person Work Q&As.

(11) Keep sensitive conversations private. For conversations about sensitive matters, if possible, reserve a space or find a separate area, minimize the noise level, use a headset instead of device speakers, and follow office etiquette. Review IRM 10.5.1.6.7, Phone, IRM 10.5.1.6.18.2, Online Meetings, and Return to In-Person Work Q&As.
Reminder: Do not disclose sensitive information overheard in the office without an authorized need to know. You could lose your job or go to jail with penalties under the IRC and Privacy Act. Review IRM 10.5.1.2.4 (4), Federal Tax Information (FTI), and IRM 10.5.1.2.7(1), Privacy Act Information.

(12) Report incidents and data breaches immediately upon discovery following IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures. Refer to IRM 10.5.1.4.1, Employees and Personnel.

(13) Refrain from taking photos or other electronic recordings unless you have a business need, approval, consent, precautions, and government-approved equipment. Follow IRM 10.5.1.6.14.2, Recordings in the Workplace.

10.5.1.5.3.1
(07-09-2025)
Shared Spaces

(1) Non-IRS employees from other agencies, in spaces shared with IRS must follow policies outlined in IRM 10.5.1.3, Office Privacy, and meet the requirements in this subsection.

(2) These requirements serve as privacy rules of conduct and safeguards under the Privacy Act, 5 USC 552a sections (e)(9) and (e)(10), respectively. They also serve to prevent unauthorized access to FTI as required by IRC 6103.

(3) Agencies may share space under Executive Order 14274, Restoring Common Sense to Federal Office Space Management – The White House, and OMB M-25-25, Implementation of Utilizing Space Efficiently and Improving Technologies Act.
Note: The IRS should consider documenting risks of shared space by following the Form 14675, Decision Making Framework Risk Acceptance Form and Tool (RAFT), process in consultation with the CPO. Review IRM 10.5.1.1.5, Background. [OMB A-130, TD P 85-01]

(4) IRS officials in FMSS are responsible for allowing shared space with other agencies and must provide the other agency personnel with this guidance and Inadvertent Access to Sensitive Information training (pdf), and vice versa. Personnel must follow their own agency's privacy guidelines in addition to that of the hosting agency. Refer to IRM 10.5.1.8.11.1, PS-06 Personnel Security — Access Agreements [J] {Org}. [Privacy Act]

(5) If both the hosting and visiting agency personnel use SBU data (which might include PII for both and FTI for the IRS) in their normal course of business and must protect it from unauthorized disclosure. Neither agency has a need to access the other agency's information. Personnel at either agency must not ask the other for SBU data. We are sharing space, not information. Review IRM 10.5.1.5.3(11). [IRC 6103; Privacy Act]
(6) Under Publication 1075, the IRS requires agency recipients of FTI to share facilities with other agencies in a way that does not allow access to FTI by others using the shared facility. Their information systems also must prevent unauthorized and unintended information transfer via shared system resources. The IRS must apply these requirements to our shared spaces.
(7) For unescorted staff-like access, other non-IRS agency personnel must access space with a personal identity verification (PIV) card and meet requirements like those in IRM 10.5.1.6.15, Contracts, and IRM 10.2.18.6.1, Unescorted Access, including:
    a. Agency memorandum of understanding (MOU) outlining privacy requirements and consequences for non-compliance. Request MOU privacy language approval via email to *Privacy.
    b. Visitor Clearance Verification from the home agency that will verify:
        i. Adjudicated favorable background investigation, as evidenced by a valid PIV card issued by the home agency, or alternatively verified through a Visitor Access Request. [5 CFR Part 731, Suitability and Fitness]
        ii. Interim or final staff-like access approval per IRM 10.23.2, Contractor Investigations (except for tax compliance check, which the IRS must not do for a non-tax administration purpose under IRC 6103 and will not ask for consent to do).
        iii. Documented completion of Inadvertent Access to Sensitive Information training (pdf) (or approved Treasury or bureau equivalent that outlines protections and penalties) within the required time limits per IRM 10.23.2.10, Security Awareness Training (SAT) Requirements. Do not need other security or privacy training unless direct access to IRS systems or data. [Privacy Act]
        iv. Signed non-disclosure agreements (NDAs) from other non-IRS agency employees. Request NDA privacy language approval via email to *Privacy.
(8) Other agency personnel must not have access to limited or controlled areas defined in IRM 10.2.14.3.5, Security Areas, unless approved following IRM 10.2.18.10.1, Limited Area Unescorted Access.
(9) Other agency employees must not have access to campuses or areas with clean desk policy waivers described in IRM 10.5.1.5.1, Clean Desk Policy, unless approved following IRM 10.2.18.10.1, Limited Area Unescorted Access. They also must not have access to areas with specific privacy space requirements under the IRS National Workspace Standards (pdf).
(10) Take all other available precautions to protect privacy and safeguard SBU data outlined in IRM 10.5.1.3, Office Privacy, and IRM 10.5.1 in general.
(11) Restrict other agency employees from using IRS networks, unless specifically granted staff-like access to such following IRS policy with a PIV card under IRM 10.23.2.8.1, Access to IT Systems and Sensitive Information. This means other agency employees must have another way for internet, printer, copier, and scanner access, unless specifically granted staff-like access.

10.5.1.6.5
(07-09-2025)
Marking

…

(1) Mark or label SBU data (including PII and FTI) correctly to highlight its sensitivity. The lack of SBU data markings does not relieve the holder from safeguarding responsibilities. **Reminder**: Do not disclose marked data without an authorized need to know. You could lose your job or go to jail with penalties under the IRC and Privacy Act. Review IRM 10.5.1.2.4 (4), Federal Tax Information (FTI), and IRM 10.5.1.2.7, Privacy Act Information. **Caution**: For efficiency, avoid marking all data as sensitive by default. Non-sensitive data doesn't need a sensitive marking.

…