PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 29, 2026

Control Number: PGLD-10-0526-0007
Expiration Date: 05-28-2028
Affected IRM(s): 10.5.1; 2.25.20; proposed 10.3.1

MEMORANDUM FOR ALL BUSINESS UNITS

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

SUBJECT: Data Classification and Sensitivity Labeling Privacy Protections

This memorandum issues guidance on data classification and sensitivity labeling privacy protections, effective May 29, 2026. Please distribute this information to all affected personnel in your organization.

Purpose: This interim guidance clarifies privacy data classification and sensitivity labeling requirements, aligns with the Zero Trust security strategy, and the forthcoming phased implementation of controlled unclassified information (CUI). This update includes renamed and new subsections.

Background/Source(s) of Authority: This interim guidance falls under the authorities found within IRM 10.5.1.1.6, Authority, and:

- Federal Information Security Modernization Act of 2014 (FISMA)
- OMB M-22-09 (pdf), Federal Zero Trust Strategy
- Cybersecurity and Infrastructure Security Agency (CISA) High Value Asset Control Overlay
- Treasury Directive Publication (TD P) 80-08, Controlled Unclassified Information

- NIST SP 800-53 Revision 5
- Federal Information Security Modernization Act of 2014 (FISMA)

IRS personnel reviewed and approved Artificial Intelligence (AI) tool recommendations to update this content, including plain language, punctuation, and grammar revisions.

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 May,28 2028. Authors of affected IRMs will incorporate likewise.

Effective Date: May 29, 2026

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

Distribution: FOIA Library (external) on IRS.gov

Attachment Interim Guidance: PGLD-10-0526-0007

Interim Guidance: PGLD-10-0526-0007

The following changes take effect May 29, 2026**, for** IRM 10.5.1, Privacy Policy.

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

10.5.1.6.5
(05-29-2026)
Data Classification and Sensitivity Labeling Privacy Protections

(1) The IRS will transition from legacy terms of sensitive but unclassified (SBU) data, personally identifiable information (PII), and federal tax information (FTI) to data classification terms aligned with controlled unclassified information (CUI) to prepare for phased CUI implementation.

NOTE: This policy does not address the treatment of classified information (top secret, secret, and confidential). Refer to IRM 10.9.1, Classified National Security Information (CNSI).

(2) Data classification is the process of identifying and organizing information based on its sensitivity so the IRS can manage and protect sensitive information from unauthorized access, disclosure, alteration, or loss. Sensitivity labels apply these data classification decisions to help enforce them.

(3) Data classification and security categorization are related but distinct processes. Data classification identifies the sensitivity of information. Security categorization applies that decision to systems. Data classification does not replace system security categorization. Refer to IRM 10.8.1.4.16.1, RA-02 Security Categorization.

(4) The IRS will implement the CUI program in phases. During the transition period, personnel may use both legacy IRS terminology and CUI markings. Personnel should proactively adopt CUI terminology and begin phasing out legacy IRS terms as implementation progresses. For more information on CUI, refer to the internal Controlled Unclassified Information site and Interim Guidance (IG) Regarding the Receipt and Handling of Controlled Unclassified Information (CUI) Prior to CUI Policy Implementation. CUI requirements will become mandatory across the IRS when IRM 10.3.1, Controlled Unclassified Information (CUI), is published.

Note: IRS uses legacy designations (SBU, PII, and FTI) extensively throughout existing IRMs and related guidance. This interim guidance does not revise all references at once. The IRS will transition to CUI terminology in phases. Authors must update IRMs and related publications accordingly. The IRS may add CUI category markings as implementation progresses.

(5) IRS personnel must complete the data classification process and label sensitive information at document creation (source) either automatically or manually. Follow this data classification table (from highest to lowest sensitivity) to select the label that reflects the highest sensitivity, even if multiple categories apply:

Data classification category	CUI marking	IRS legacy term	Examples (not all inclusive)
Tax	CUI//SP-TAX	FTI	Taxpayer PII, social security numbers (SSNs), tax returns, and tax case files
Privacy	CUI//SP-PRVCY	PII	Non-tax employee PII (employee SSNs and personnel records such as the SF-50)
Controlled Unclassified Information (CUI)	CUI	SBU	Non-tax, non-PII sensitive information we must protect (such as passwords, IT and physical security, contract negotiations, and budget deliberations)
Uncontrolled	Uncontrolled	Uncontrolled	Information proactively released to the public (such as information on IRS.gov)

Note: This table further applies IRM 10.5.1.2.2.1, Examples and Categories of SBU Data, with these additional clarifications:

- Tax includes tax information and associated PII (protected by IRC 6103).
- Privacy includes PII that is not tax information (protected by the Privacy Act).

(6) The IRS Privacy Principles include data minimization, purpose limitation, accountability, confidentiality, and security. IRS personnel must understand and protect the information they use in the performance of their duties. Restrict access to those with a legitimate and authorized need to know. Decide on proper data sharing based on this need. Review IRM 10.5.1.3.2, IRS Privacy Principles, and its subsections.

(7) This policy aligns privacy requirements with federal directives for data classification, CUI, and sensitivity labeling protections and includes more details in these subsections:

IRM Section	Title
10.5.1.6.5.1	Data Classification Responsibilities
10.5.1.6.5.2	Sensitivity Labeling Protections
10.5.1.6.5.2.1	Automated Labeling and Marking
10.5.1.6.5.2.2	Manual Labeling and Marking
10.5.1.6.5.3	Data Classification on IRS Shared Storage
10.5.1.6.5.4	Data Classification Process

10.5.1.6.5.1
(05-29-2026)
Data Classification Responsibilities

(1) All IRS personnel have a role in data classification and sensitivity labeling.
(2) Executives and program leaders are responsible for making sure their programs and employees understand and follow data classification and sensitivity labeling requirements.
(3) System and information owners, based on responsibilities in IRM 10.8.2.3, IT Security Roles and Responsibilities, must implement and maintain the technical capabilities that support data classification processes and sensitivity labeling, including:
    a. Deploy and configure automated classification and sensitivity labeling tools.
    b. Manage encryption and access control technologies.
    c. Implement and tune data loss prevention (DLP) controls.
    d. Monitor data access, sharing, and usage.
    e. Continuously evaluate and enhance automated protections.
(4) End users are IRS personnel who create, modify, access, or share data as part of their assigned duties. End users handling data in their daily duties must:
    a. Identify sensitive data to support data classification decisions.
    b. Apply proper sensitivity labels. Refer to IRM 10.5.1.6.5.2.2, Manual Labeling and Marking.
    c. Make sure labels reflect the highest sensitivity of the data.
    d. Follow access and sharing restrictions associated with applied labels.

10.5.1.6.5.2
(05-29-2026)
Sensitivity Labeling Protections

(1) Sensitivity labeling applies and enforces data classification decisions. The IRS uses automated and manual sensitivity labeling to apply data classification decisions that help identify and protect sensitive information across IRS systems and environments.
(2) The IRS must apply automated sensitivity labeling unless it is not technologically feasible. Refer to IRM 10.5.1.6.5.2.1, Automated Labeling and Marking.
(3) End users must apply manual labeling and marking when automation is unavailable or when automated labeling does not accurately reflect the sensitivity of the data. Refer to IRM 10.5.1.6.5.2.2, Manual Labeling and Marking.
(4) When labels conflict, apply the label that provides the higher level of protection.

10.5.1.6.5.2.1
(05-29-2026)
Automated Labeling and Marking

(1) Automated labeling is the system-enforced application of sensitivity labels based on predefined rules and data pattern recognition to apply data classification decisions. System and information owners must make sure automated labeling capabilities meet the following requirements:
    a. Align with IRS data classification and CUI marking requirements.
    b. Apply sensitivity labels based on detected data types using the data classification schema in IRM 10.5.1.6.5(4), Data Classification and Sensitivity Labeling Privacy Protections.

c. Enforce protections associated with the applied label, such as encryption, access restrictions, and data loss prevention (DLP) controls.
d. Prevent or warn when downgrading labels and document justification.
e. Support audit logging and monitoring.

(2) Sensitivity labels must persist across databases, systems, and cloud environments to make sure continuous protection throughout the data lifecycle. This requirement applies to:
a. Information at rest, such as mainframes (Tier I), Linux servers (Tier II), Windows environments (Tier III), High Value Assets (HVAs), databases, tables, email systems, and cloud platforms.
b. Information in use, including data processed by applications, electronically transmitted, incorporated into spreadsheets, or manually manipulated.

10.5.1.6.5.2.2
(05-29-2026)
Manual Labeling and Marking

(1) End users apply manual labeling and marking. End users must:
a. Apply labels when automation does not detect sensitive data.
b. Apply labels when creating or using documents, spreadsheets, presentations, emails, or other materials that have sensitive information.
c. Make sure labels reflect the highest sensitivity based on the data contents.
d. Apply labels before sharing.

(2) The label or marking must remain with the data throughout the data lifecycle.

Exception: In limited situations, information may change sensitivity over time. For example, congressional documents or drafts that are initially designated CUI may become uncontrolled after the IRS properly releases the final product to the public. End users must update the label to reflect the lower sensitivity classification and label and provide a justification for the change.

(3) Manual labeling includes applying required CUI banner markings to documents and physically marking printed materials.

(4) Personnel must not remove or downgrade automated labels without justification.

(5) Manual labeling supplements automated labeling and does not replace required automated protections when available.

10.5.1.6.5.3
(05-29-2026)
Data Classification on IRS Shared Storage

(1) The IRS must use sensitivity labels on shared storage and collaboration platforms such as SharePoint and Teams sites. Refer to IRM 2.25.20, Integrated Enterprise Portal-Web Services, SharePoint, for more detailed SharePoint policies.

(2) Site owners must select and maintain the correct site sensitivity for internal SharePoint and Teams sites following the data classification schema and associated labeling requirements described in IRM 10.5.1.6.5, Data Classification and Sensitivity Labeling Privacy Protections, and IRM 10.5.1.6.5.4, Data Classification Process.

(3) The applied site sensitivity label must align with the highest level of sensitive information stored within the site. Site sensitivity labels control access, restrict sharing based on authorized need to know, and apply proper protections. Apply the following site sensitivity label rules:

Site Label	Allowed Data	Restricted Data
Tax	Tax, Privacy, CUI, Uncontrolled	None
Privacy	Privacy and CUI	Tax
CUI	CUI	Tax and Privacy
Uncontrolled	Uncontrolled	Tax, Privacy, and CUI

(4) The IRS uses automated tools where technologically feasible to enforce protections, identify incompatible data, and correct content to align with site sensitivity labels.

Exception: A site does not require a sensitivity label solely because it contains routine personnel information the IRS proactively makes available to all personnel on resource sites (including Discovery Directory, Outlook™ (calendar, profile information, and address book), and SharePoint™ or Teams™ site collections), such as names and business contact information. If a site contains other sensitive data, personnel must apply the proper privacy or tax label.

(5) Refer to IRM 10.5.1.6.18.3, Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites).

10.5.1.6.5.4
(05-29-2026)
Data Classification Process

(1) IRS leadership, system owners, and end users carry out the data classification process in different ways, based on their role within the organization.
(2) Identify: Collect information about IRS data assets, including structured and unstructured data such as file type, metadata, and content, as close as possible to the time of their creation, discovery, or import.
    a. System owners and leadership implement this step by identifying and understanding the sensitivity of data within their systems and programs, including configuring tools and scanning storage locations to discover data assets.
    b. End users implement this step by identifying and understanding the data they create, access, use, or share.
(3) Analyze: Evaluate data to determine its sensitivity based on content, context, and applicable classification criteria.
    a. System owners implement this step by using automated tools and defined rules to analyze data and determine proper classifications.
    b. Leadership implements this step by making sure classification criteria and the data classification schema are defined, communicated, and consistently applied across programs.
    c. End users support this step by recognizing when data may require a higher sensitivity classification based on its content.

(4) Label: Apply sensitivity labels to data based on data classification decisions and embed labels as metadata to support protection and handling requirements.
    a. System owners implement this step by configuring systems to automatically apply labels based on classification rules.
    b. End users implement this step by applying and updating labels when automated labeling is unavailable or does not accurately reflect the sensitivity of the data.
(5) Mark: Apply required visual or embedded markings (such as CUI banners, headers, footers, or watermarks) to communicate data sensitivity.
    a. System owners implement this step by enabling systems to apply required markings where supported.
    b. End users implement this step by applying required markings to documents and materials when automated marking is unavailable.
(6) Protect: Apply cybersecurity and privacy controls to protect data based on its classification.
    a. System owners implement this step by applying technical controls such as access restrictions, encryption, and data loss prevention (DLP).
    b. Leadership implements this step by making sure proper safeguards and policies are in place and followed.
    c. End users implement this step by following access, sharing, and handling restrictions associated with labeled data.
(7) Train: Provide training to personnel on data classification and sensitivity labeling requirements.
    a. Leadership implements this step by making sure personnel receive required training and understand their responsibilities.
    b. System owners implement this step by supporting training related to system capabilities and tools.
    c. End users implement this step by completing required training and applying it in their daily duties.
(8) Monitor: Monitor data assets and systems for classification accuracy, labeling consistency, and compliance with protection requirements.
    a. System owners implement this step by monitoring systems, auditing data usage, and correcting classification or labeling inconsistencies.
    b. Leadership implements this step by overseeing compliance and making sure corrective actions are taken when needed.
    c. End users support this step by reporting issues with data classification, labeling, or access.
(9) Disposition: Keep sensitive information only as long as necessary following legal requirements. Purge expired sensitive data securely. Disposition and destruction of tax information must follow IRM 1.15 series, Records and Information Management.

10.5.1.6.18.3 (05-29-2026)

Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites)

…

(2) Collaborative environment owners also must make sure their users follow rules and protect privacy. Refer to IRM 10.5.1.6.5.3, **Data Classification on IRS Shared Storage.**

…

Exhibit 10.5.1-1
(05-29-2026)
Glossary and Acronyms

Term	Definition or description
…	…
Controlled Unclassified Information	Refer to the Controlled Unclassified Information within the Disclosure and Privacy Knowledge Base. See also IRM 10.8.1.4.16.1.2, Controlled Unclassified Information (CUI), and IRM 10.8.1-1, Terms and Acronyms.
Data	A representation of information, including digital and non-digital formats.
Structured Data	Structured data (databases, applications) is information organized in a predefined and consistent format, enabling efficient storage, retrieval, and analysis. Also, please refer to IRM 1.15.6.2, Basic Electronic Records Management Definitions
Unstructured Data	Unstructured data (documents, PDFs, spreadsheets, emails, images, audio files, etc.) is more free form and does not necessarily follow any format or hierarchical sequence, nor does it follow any relational rules. Unstructured data refers to masses of (usually) computerized information which do not have a data structure that is easily readable by a machine. Also, please refer to IRM 1.15.6.2, Basic Electronic Records Management Definitions
Data Asset	Information-based resource such as a database, document, webpage, or service.
Data Classification	The process of identifying and organizing information based on its sensitivity so the IRS can manage and protect sensitive information from unauthorized access, disclosure, alteration, or loss.
Data Classification Schema	Taxonomy of all of IRS's known data asset types.
Data Protection	The controls needed to protect a data asset following its data classification.

Label	Practical attachment of metadata or identifiers to data for tracking and managing its usage based on classification.
Metadata	Information about the context of a specific data asset, like who or what created the data asset (data provenance) and when and where the data asset was collected. Also, please refer to IRM 1.15.6.2, Basic Electronic Records Management Definitions
Marking	Visual or embedded indicator (such as header, footer, or watermark) to protect sensitive information and show its sensitivity.
Sensitivity Labeling	The process of applying sensitivity labels to data to enforce data classification decisions and associated protections.
...	...