TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

SharePoint Online Access and Security Controls Need Improvement

March 18, 2026

Report Number: 2026-200-010

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: SharePoint Online Access and Security Controls Need Improvement

Final Audit Report issued on March 18, 2026 **Report Number 2026200010**

Why TIGTA Did This Audit

SharePoint Online (SPO) is a cloud-based service that allows organizations to store, share, and manage their content, knowledge and applications. This includes data elements that are Sensitive But Unclassified, proprietary processes, and other confidential information.

SPO replaced SharePoint 2013, which was no longer supported by the vendor as of April 2023. We assessed the deployment and migration of all SharePoint 2013 data to SPO and evaluated the effectiveness of user account access and security controls of SPO.

Impact on Tax Administration

The IRS's Enterprise Operations function determined that SPO would improve operational efficiencies by reducing system complexities and increasing collaboration and standardization across the enterprise.

Sharing data in collaborative environments, such as SPO, may offer valuable benefits, but also has privacy risks. Therefore, the IRS needs to ensure that there are appropriate access, privacy, and security controls in place for employees using SPO.

What TIGTA Found

The IRS needs to improve SPO user access and security controls. We reviewed more than 18,000 SPO sites and found that 52 percent were missing audit logs and 47 percent did not report an access control method. Missing audit logs limited site administrators' abilities to verify and ensure that appropriate access was granted. One percent of sites reported using the Business Entitlement Access Request System as its method of access control. Effective access controls ensure that users only have access to the information they need to accomplish their work.

In addition, a scanning tool used by the IRS to identify sensitive information could not be migrated to SPO. This resulted in restricted files and information being uploaded and made accessible to users. SPO sites should not store Personally Identifiable Information or Federal Tax Information. In a sample of 20 sites, we identified 2 sites that uploaded restricted file types, and 7 sites contained sensitive information, which should not have been stored on the sites. The scanning tool has not been redeveloped.

Further, SPO reports did not provide sufficient information to ensure that the IRS complied with certain requirements. For example, we identified 686 sites that did not have 2 site administrators as required. In addition, our review of SPO sites with two assigned site administrators found that the site administrators were not always from the appropriate business unit, *i.e.*, from the same business unit as the SPO site. For a sample of 20 sites, 9 had a primary or secondary site administrator that were not from the business unit responsible for the site.

Finally, the migration to SPO took 2 years longer than originally scheduled, which resulted in the IRS paying more than $1 million to maintain its older system. These delays were caused by a contractor hired to assist the IRS with certain tasks related to the migration. Due to these delays, the IRS had to pay an extended service contract to maintain the operating system and the SharePoint 2013 servers. This cost approximately $950,00 in Fiscal Year 2024 and $105,000 in Fiscal Year 2025.

What TIGTA Recommended

We made seven recommendations. These recommendations are related to improving access controls and ensuring the appropriateness of site administrators. In addition, we recommended that the IRS identify opportunities to recover the amounts paid for extended service contracts due to contractor delays and ensure that future contracts include more stringent performance monitoring.

The IRS agreed with five of the seven recommendations and partially agreed with the remaining two recommendations. The IRS's planned corrective actions for the two partially agreed to recommendations meet the intent of our recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

March 18, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – SharePoint Online Access and Security Controls Need Improvement (Audit No.: 2024200015)

This report presents the results of our review to assess the deployment and security of SharePoint Online. This review was part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenges of *Modernizing Information Technology* and *Protecting Taxpayer Data.*

Management's complete response to the draft report is included in Appendix III. If you have any questions, please contact me or Linna K. Hung, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

SharePoint Online (SPO) is a cloud-based service that allows organizations to store, share, and manage their content, knowledge and applications. SPO replaced the Internal Revenue Service's (IRS) SharePoint 2013, which was no longer supported by the vendor as of April 2023. The Information Technology organization's Enterprise Operations function is responsible for the development, deployment, and operation of SPO. Within Enterprise Operations, the Web Infrastructure Services Division provides the governance, development, expansion, operations, and management of the SPO sites. Individual business units own and manage the content on their SPO sites and delegate owners and administrators to manage site permissions and ensure that only authorized information is stored on their sites.[1]

The Enterprise Operations function transitioned to SPO to:

- Modernize its legacy information technology.
- Improve operational efficiencies by reducing system complexities.
- Increase collaboration and standardization across the enterprise.
- Improve security, reliability and user productivity.

SPO was deployed in three-phases:

- Phase 1 started in April 2020 and included building the infrastructure, working through the enterprise life cycle, and budgeting.
- Phase 2 deployed SPO in December 2021 and started migrating nearly 19,000 SharePoint 2013 sites and network drives to SPO in January 2022.
- Phase 3 continued the migration and incorporated additional SPO functionalities.

The IRS completed the work for Phase 1 and hired a contractor to help deliver work as part of Phases 2 and 3. Specifically, in September 2022, the IRS contracted with a vendor to develop existing forms and workflows in SharePoint 2013 that would work in the SPO environment. This contract was a 1 year contract with a one-year optional extension totaling $21.2 million.

Results of Review

SharePoint Online User Access and Security Controls Need Improvement

Our review of 18,353 SPO sites identified 18,156 (99 percent) SPO sites were either missing audit logs, or the sites did not report an access control method. More specifically, we found:

- 9,543 (52 percent) of the 18,353 SPO sites used either the manual documentation or a permission workflow in SPO for access controls. These sites relied on SPO audit logs to identify when users were provided access and by whom. However, the SPO audit logs were not enabled until October 2024. As a result, site administrators could not complete

[1] See Appendix IV for a glossary of terms.

the required biannual access reviews from January 2022 to October 2024 to ensure that only authorized users with a business need were provided access to SPO sites. Without audit logs, a site administrator is unable to verify and ensure that only users with a business need are given access to a SharePoint site.

- 8,613 (47 percent) of the 18,353 SPO sites did not report an access control method at the time of site creation. SPO reports also did not include this information. While the site administrator might have been using one of the three access control methods for their sites, there was no record of which method they used.

The remaining 197 (1 percent) SPO sites reported using the Business Entitlement Access Request System as its method of access control. The Business Entitlement Access Request System provides user entitlement reports, including management approval. In addition, the Business Entitlement Access Request System can be used to request, modify, and remove access for active users to systems; re-certify and validate user access; and remove access for separated and furloughed users and for user inactivity on the system.

We selected a judgmental sample of 20 SPO sites to further evaluate the IRS's ability to monitor appropriate access and identify or prevent sensitive data from being on SPO sites.[2] We tested user access controls for 3 of the 20 sampled sites. The 3 selected sites had 479 authorized users. The IRS could not provide us with justification for about 87 percent of the authorized users (415 of 479 users). As a result, we could not determine who provided the 415 users with access, when these users received their access, or if their access was still necessary.[3]

The privacy and security of taxpayer and personnel information is one of the IRS's highest priorities. Sharing data in collaborative data environments, such as SPO, may offer valuable benefits but also has privacy risks. Understanding these risks is key to ensuring that appropriate access, privacy, and security controls are in place. Some of the privacy risks associated with collaborative data sites can include data breaches and inadvertent disclosures, unauthorized access of data without a need to know, and sharing data without proper permissions or authorizations. Effective access controls ensure that users only have access to the information they need to accomplish their work.

Sensitive data was uploaded and accessible to users because a scanning tool was not migrated to SPO

The IRS used an automated tool to identify if files uploaded to SharePoint 2013 contained sensitive data. However, this tool could not be migrated to SPO, and a similar tool has not been developed, so the risk that sensitive data can be uploaded still exists.

The Chief Information Officer stated that SPO sites should not store Personally Identifiable Information (PII) or Federal Tax Information (FTI). In addition, there are certain restricted file types which are not allowed within SharePoint. However, our review of the 20 sampled sites identified:

[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population. See Appendix I for details about the sample.

[3] The IRS had documentation to show when the remaining 64 (13 percent) of 479 authorized users were provided access and by whom.

- **Restricted file types** on 2 (10 percent) of the 20 sampled sites. The IRS's Site Management Guide states there are several restricted file types, such as compressed, *i.e.*, zipped, files and database files are not allowed within SharePoint. The remaining 18 (90 percent) SPO sites did not have restricted file types.
- **Incorrectly stored PII or FTI** on 7 (35 percent) of the 20 sampled sites. In addition, the PII and FTI on these sites did not have the correct sensitivity label, and in some cases, was not encrypted. For example, one site contained nearly 2,000 tax return files and 725 Social Security Numbers. The remaining 13 (65 percent) SPO sites were labeled with the correct sensitivity levels.

The Internal Revenue Manual states that documents and SPO sites should contain sensitivity labels. These labels help highlight the sensitivity level of data to ensure that it is appropriately safeguarded. The IRS uses the following sensitivity label categories, from most sensitive to least:

- FTI includes taxpayers' identity, income, payments, tax liability investigation status, *etc*.
- PII (without FTI), includes name, address information, Social Security Numbers, *etc*.
- Sensitive But Unclassified (without PII or FTI), which includes proprietary processes or business information, and other confidential information.
- Uncontrolled, which includes data that is not sensitive and not FTI, PII or Sensitive But Unclassified data.

When the IRS migrated to SPO, Enterprise Operations could not migrate the automated tool to identify files and sites containing sensitive data. Therefore, it lost the ability to scan uploaded documents. The automated tool provided an efficient means for site administrators to scan sites on an ongoing basis to ensure that no restricted information was uploaded. In its absence, site administrators and owners must manually review each individual file to ensure the accuracy of the data sensitivity label. With SPO sites averaging approximately 5,000 files, this is a very inefficient and time-consuming task. According to the Chief Information Officer, the IRS plans to buy a new automated tool to detect and remove sensitive data from SPO sites.

SPO reports did not provide sufficient information to appropriately assign site administrators

Our review identified 686 sites that did not have 2 site administrators assigned as required by the Internal Revenue Manual. Site administrators provide support and manage permissions and access across all sites. In addition, they manage other aspects of the site, *e.g.*, templates and site branding. Two site administrators ensure business continuity. If one administrator is unavailable, the second can manage the site without interruption. In addition, having two administrators improves decision-making processes by ensuring that one person does not have the sole responsibility to restrict site access or prevent external sharing.

In addition, our review of SPO sites with two assigned site administrators found that the site administrators were not always from the appropriate business unit, *i.e.*, from the same business unit as the SPO site. Allowing site administrators to be from different business units provides these individuals unnecessary access to information for which they do not have a business need. In addition, site administrators from a different business unit would not be able to effectively manage the sites or review user privileges because they are not as aware of employees joining or leaving the business unit.

Our review of the 20 sampled SPO sites found:

- 11 (55 percent) of the 20 sites had a primary and secondary site administrator that were from the business unit responsible for the site.
- 9 (45 percent) of the 20 sites had a primary or secondary site administrator that were not from the business unit responsible for the site.

SPO provides the IRS with reports that include site name, primary administrator, creation date, number of files, sensitivity label, *etc.* However, these reports do not identify an SPO site's secondary site administrator or either site administrators' assigned business unit. As a result, the IRS cannot ensure that it is complying with the requirements outlined in its Internal Revenue Manual.

Management Action: The IRS is offering regular biweekly training for site administrators to improve the controls for the SPO environment. In June 2025, we attended one of these trainings where they presented a site certification tool that would be rolled out in phases through September 2025. The site certification process includes:

- Reviewing user permissions and the site's audit log.
- Validating the site's sensitivity level.
- Validating the site has two administrators within the appropriate business unit.

While biweekly training classes for site administrators are being offered, additional actions are needed to improve the ability to monitor appropriate access and identify or prevent sensitive data from being on SPO sites.

The Chief Information Officer, should:

Recommendation 1: Ensure that the site owners using manual documentation or a permission workflow method of access control review the SPO logs to ensure that only authorized users with a business need have access.

> **Management's Response:** IRS management agreed with this recommendation and revised its policy to require site owners to conduct monthly reviews of audit logs.

Recommendation 2: Ensure that all SPO sites identify their access control method.

> **Management's Response:** IRS management agreed with this recommendation and implemented a requirement that all SPO sites identify their access control method at the time of site creation through the Permission Access Lookup tool.

Recommendation 3: Implement an automated tool that can identify and remove sensitive data (such as PII and FTI) on SPO sites.

> **Management's Response:** IRS management partially agreed with this recommendation. The Chief Information Officer will implement an automated tool to identify and remove incompatible sensitive data (such as PII and FTI) from SPO sites.
>
> > **Office of Audit Comment:** The IRS's planned corrective action of implementing an automated tool to identify and remove incompatible sensitive data meets the intent of our recommendation.

Recommendation 4: Implement an automated tool that can block restricted file types on SPO sites.

> **Management's Response:** IRS management agreed with this recommendation and will implement an automated tool to block restricted file types on SPO sites.

Recommendation 5: Establish a process to identify and update sites that are missing appropriate site administrators.

> **Management's Response:** IRS management agreed with this recommendation and implemented the Permission Access Lookup tool to identify sites missing appropriate site administrators and to update those sites accordingly.

The Migration to SharePoint Online Was Significantly Delayed

The migration of workflows and forms from SharePoint 2013 to SPO took 2 years longer than originally scheduled, which resulted in the IRS paying more than $1 million to maintain its older system. The migration was originally scheduled to be completed by April 2023 when the vendor ended its software support for SharePoint 2013. However, the IRS did not finish the migration until May 2025.

The contract's scope of work included 3,040 workflows and 603 forms. In August 2024, Enterprise Operations determined that the contractor would not complete the work in the required time frame and stopped all payments, withholding $1.1 million of the $21.2 million contracted amount. In addition, site owners found deficiencies with the contractor's completed work. This contractor was involved with 14 additional contracts with the IRS totaling $77.8 million from Fiscal Years 2020 to 2023. According to IRS management, there have been similar performance issues present in other IRS contracts with the contractor.

While the majority of the workflows and forms were successfully migrated, we found that 37 (1 percent) workflows and 27 (4 percent) forms were not migrated. According to Enterprise Operations management officials, the migration activities were not completed because the original contractor did not finish the work in accordance with the contract. The contract was a firm fixed-price contract, *i.e.*, the contractor was responsible for delivering the scope of work outlined in the agreement on time and for a defined price. In addition, the IRS did not stipulate milestones or deliverable dates in the contract, so the work could not be measured against performance standards until the work was completed. This made it difficult for Enterprise Operations to monitor the contractor's performance to ensure the work could be completed within the time frames of the contract.

Due to the contractor's delays, the IRS paid for an extended service contract to maintain the operating system and the SharePoint 2013 servers. This cost the IRS an additional $950,000 in Fiscal Year 2024 and $105,500 in Fiscal Year 2025, totaling more than $1 million. In addition, there was no extended support for the SharePoint 2013 platform.

As a result of these delays, the IRS had to complete the remaining work to migrate the workflows and forms internally or implement manual workarounds. Further, the continued use of SharePoint 2013 put the stored information, including FTI and PII data, at risk because the vendor was no longer available to provide support to patch security vulnerabilities.

The Chief Information Officer, should:

Recommendation 6: Coordinate with the Office of Chief Counsel to identify opportunities to recover, from the original contractor, the amount paid for the SharePoint 2013 extended service contracts due to delays and deficiencies in the original contractor's work.

> **Management's Response:** IRS management agreed with this recommendation. The Chief Information Officer will coordinate with the Office of Chief Counsel to identify opportunities to recover funds from the original contractor's work.

Recommendation 7: Ensure that future information technology contracts include milestones, deliverables, and/or more stringent performance monitoring.

> **Management's Response:** IRS management partially agreed with this recommendation. The Chief Information Officer will coordinate with the Chief Procurement Officer to develop and provide guidance to information technology acquisition personnel stating that future service-related information technology contracts should include milestones, deliverables, and/or stringent performance monitoring.
>
> > **Office of Audit Comment:** The IRS's planned corrective action of coordinating with the Chief Procurement Officer to develop and provide guidance to information technology acquisition personnel for future service-related information technology contracts meets the intent of our recommendation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the IRS's deployment and security of SPO. To accomplish our objective, we:

- Assessed whether the IRS fully deployed and migrated all SharePoint 2013 data to SPO.
- Evaluated the effectiveness of user account access and security controls for SPO sites in the cloud environment by reviewing a judgmental sample of 20 SPO sites.[1] The sample selection included SPO sites with all reported data sensitivity levels and access control methods from different IRS business unit owners with a minimum of 50 files per site to review.
- Evaluated the accuracy of data sensitivity levels for the 20 SPO sites selected in our judgmental sample.

Performance of This Review

This review was performed with information obtained from the Enterprise Operations function located in the New Carrollton Federal Building in Lanham, Maryland, and from the Privacy, Governmental Liaison and Disclosure Office located at the IRS Headquarters in Washington, D.C., during the period October 2024 through June 2025. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

We performed tests to assess the reliability of data from the SharePoint 2013 and the SPO applications. We evaluated the data by 1) performing electronic testing of required data elements, 2) reviewing existing information about the data and the system that produced them, and 3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the Government Accountability Office's *Standards for Internal Control in the Federal Government*, and various federal and IRS policies, procedures, and guidelines related to the deployment and security of SPO. We evaluated these controls by interviewing Information Technology organization and Privacy,

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Governmental Liaison and Disclosure Office personnel, and by reviewing relevant documentation.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Funds Put to Better Use – Potential; $1,055,782 paid for extended service contract to maintain the operating system and the SharePoint 2013 servers. There was no extended support for the SharePoint 2013 platform. (See Recommendation 6).

Methodology Used to Measure the Reported Benefit:

Vendor support for SharePoint 2013 ended in April 2023. Due to delayed migration, the IRS had to purchase extended security updates for the servers and operating system for Fiscal Years 2024 and 2025. This cost the IRS $950,329 in Fiscal Year 2024 and $105,453 in Fiscal Year 2025, totaling $1,055,782.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

February 14, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Chief Information Officer

Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2026.02.14 12:37:55 -05'00'

SUBJECT: Draft Audit Report – SharePoint Online Access and Security Controls Need Improvement (Audit #2024200015)

Thank you for the opportunity to respond to the draft audit report. The IRS appreciates the Treasury Inspector General for Tax Administration's continued oversight as we modernize our internal digital workspace through the migration to SharePoint Online (SPO).

This has been a complex and multi-layered effort involving every business unit and operating division within the IRS, and we appreciate the opportunity to highlight the benefits of work completed so far. Throughout the process, we remained focused on implementing and managing the upgrade in alignment with federal standards and internal policies while minimizing disruptions for employees who rely on these applications every day. We successfully deployed SPO enterprise-wide and completed the migration of more than 18,000 internal sites used by IRS employees in performing their job duties.

We also implemented several key initiatives to strengthen oversight, security, and data governance and continue to explore automation and process improvements that will deliver additional efficiencies. The attached corrective action plan outlines steps we plan to take to further strengthen program management and internal controls.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact my office at (202) 317-5000, or a member of your staff may contact Lou Capece, Infrastructure Technology Operations, Coordinating Director, at (484) 636-0479.

Attachment

Attachment

Audit #2024200015, *SharePoint Online Access and Security Controls Need Improvement*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure that the site owners using manual documentation or a permission workflow method of access control review the SPO logs to ensure that only authorized users with a business need have access.

CORRECTIVE ACTION 1: The IRS agrees with the recommendation. In November 2025, the Chief Information Officer revised policy to require site owners to conduct monthly reviews of audit logs.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 2: The Chief Information Officer should ensure that all SPO sites identify their access control method.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer has implemented a requirement that all SPO sites identify their access control method at the time of site creation through the Permission Access Lookup (PAL) tool.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 3: The Chief Information Officer should implement an automated tool that can identify and remove sensitive data (such as PII and FTI) on SPO sites.

CORRECTIVE ACTION 3: The IRS partially agrees with this recommendation. The Chief Information Officer will implement an automated tool to identify and remove incompatible sensitive data (such as PII and FTI) from SPO sites.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

Attachment

Audit #2024200015, *SharePoint Online Access and Security Controls Need Improvement*

RECOMMENDATION 4: The Chief Information Officer should implement an automated tool that can block restricted file types on SPO sites.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will implement an automated tool to block restricted file types on SPO sites.

IMPLEMENTATION DATE: September 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 5: The Chief Information Officer should establish a process to identify and update sites that are missing appropriate site administrators.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer has implemented the Permission Access Lookup (PAL) tool to identify sites missing appropriate site administrators and to update those sites accordingly.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 6: The Chief Information Officer should coordinate with the Office of Chief Counsel to identify opportunities to recover, from the original contractor, the amount paid for the SharePoint 2013 extended service contracts due to delays and deficiencies in the original contractor's work.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The Chief Information Officer will coordinate with the Office of Chief Counsel to identify opportunities to recover funds from the original contractor's work.

IMPLEMENTATION DATE: May 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Strategy & Product Management

Attachment

Audit #2024200015, *SharePoint Online Access and Security Controls Need Improvement*

RECOMMENDATION 7: The Chief Information Officer should ensure that future information technology contracts include milestones, deliverables, and/or more stringent performance monitoring.

CORRECTIVE ACTION 7: The IRS partially agrees with this recommendation. The Chief Information Officer will coordinate with the Chief Procurement Officer to develop and provide guidance to IT acquisition personnel stating that future service-related information technology contracts should include milestones, deliverables, and/or stringent performance monitoring.

IMPLEMENTATION DATE: May 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Strategy & Product Management

Appendix IV

Glossary of Terms

Term	Definition
Access Controls	A policy that is uniformly enforced across all subjects and objects within the boundary of an information system.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Business Entitlement Access Request System	A system that manages identity access management. It is used to request, modify, and remove access for active users to IRS systems by managing the digital identity of individuals, roles, resources, and entitlements granted or removed.
Business Unit	A title for IRS offices and organizations such as the Office of Appeals, the Office of Professional Responsibility, and the Information Technology organization.
Cloud	The use of computing resources, *e.g.*, hardware and software, which are delivered as a service over a network (typically the internet).
Enterprise Operations Function	Responsible for providing server and mainframe computing services for all IRS business entities and taxpayers.
Federal Tax Information	Consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Need to Know	Personnel may access sensitive data (including personally identifiable and tax information) only as authorized to meet a legitimate business need, which means personnel need the information to perform their official duties.
Permission Workflow	Method of controlling access to a requested site that is addressed through a workflow on SharePoint. The workflow routes a document or other item to designated people for their approval or rejection.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of PII are name, Social Security Number, date of birth, place of birth, address, and biometric record.
Privacy, Governmental Liaison and Disclosure Office	The IRS organization responsible for protecting the sensitive information and privacy of taxpayers and employees; ensuring only authorized disclosures and data.

Term	Definition
Security Vulnerabilities	Weaknesses in configuration or design that attackers may target and exploit.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552 a (the Privacy Act of 1974), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Site	A site allows the IRS to organize and store all content in SharePoint; the content can be lists, libraries (document, picture, report, and form), web pages, or sites. Further, a site can have subsites in its hierarchy.
Site Administrator	Responsible for all aspects of the site and manages core elements *e.g.*, metadata, navigation, permissions, templates, branding across all sub-sites. Provides support for any issues with all sub-sites.

Appendix V

Abbreviations

FTI	Federal Tax Information
IRS	Internal Revenue Service
PII	Personally Identifiable Information
SPO	SharePoint Online

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at
TIGTACommunications@tigta.treas.gov.

Information you provide is confidential, and you may remain anonymous.