



Memorandum from the Office of the Inspector General

August 7, 2024

Tammy W. Wilson

**REQUEST FOR MANAGEMENT DECISION – AUDIT 2024-17492 – SHAREPOINT®
ACCESS MANAGEMENT**

An audit we are currently performing of the Tennessee Valley Authority's (TVA) Privacy Program¹ identified nonpublic critical and sensitive information, including restricted personally identifiable information (RPII), that was accessible on TVA's SharePoint® by all TVA users. We reported those issues to TVA management in a management alert on March 13, 2024, and scheduled this audit of TVA's management of access to nonpublic critical and sensitive information. Our objective was to determine if TVA manages access to nonpublic critical and sensitive information in accordance with TVA information management policy. Our scope for this audit was limited to TVA's SharePoint® sites, as of March 19, 2024.

TVA responded to our management alert by deploying a process to identify and restrict access to RPII on SharePoint® sites. However, we determined TVA's management of access to nonpublic critical and sensitive information could be improved. Specifically, other types of nonpublic critical and sensitive information were not included in the process. In addition, we determined TVA was not providing SharePoint® site owners with the appropriate training to properly manage access to TVA nonpublic critical and sensitive information.

In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

BACKGROUND

Microsoft SharePoint® is a collaboration tool that provides a secure place to store, organize, share, and access information from any device. SharePoint® sites are created by SharePoint® administrators who can assign a standard user as the site owner. In addition, when a standard user creates a Microsoft 365® Group,² a SharePoint® site is automatically created and the user is assigned as the site owner. SharePoint® site owners are responsible for access management to their sites. As of March 19, 2024, TVA had 13,082 total SharePoint® sites.

An audit we are currently performing of TVA's Privacy Program (Audit 2024-17478) identified nonpublic critical and sensitive information, including RPII, that was accessible on

¹ Audit 2024-17478, *TVA's Privacy Program*.

² Groups in Microsoft 365® let you choose a set of people that you wish to collaborate with and easily set up a collection of resources for those people to share, including a SharePoint® site.

TVA's SharePoint® by all TVA users. TVA Standard Program and Process (SPP) 12.002, *TVA Information Management*, requires access to this information be limited to those with a need to know. Due to the nature of the issues we identified under audit 2024-17478, we issued a management alert to TVA on March 13, 2024, that provided details of our findings. We also scheduled this audit of TVA's management of access to nonpublic critical and sensitive information.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA manages access to nonpublic critical and sensitive information in accordance with TVA information management policy. Our scope for this audit was limited to TVA's SharePoint® sites, as of March 19, 2024. To achieve our objective, we:

- Reviewed TVA-SPP-12.002, *TVA Information Management Policy*, to gain an understanding of TVA's requirements for information management.
- Inquired of TVA personnel to gain an understanding of TVA's SharePoint® implementation.
- Identified and assessed internal controls to the extent necessary to address the audit objective, including:
 - Identified training as a significant internal control and access management as a significant information systems control.
 - Assessed design of internal controls by reviewing training documentation and default access permissions.
 - Assessed implementation and operating effectiveness of internal controls by surveying a sample of site owners and reviewing access to a sample of sites for appropriateness.
- Reviewed training materials available to SharePoint® site owners to determine if owners are provided with the training necessary to properly secure SharePoint® sites.
- Performed a walkthrough of TVA's process to identify and restrict RPII on SharePoint® to obtain an understanding of actions taken in response to the OIG's management alert.
- Selected two statistical samples, as shown in Table 1, of SharePoint® sites (sites created in SharePoint® and by 365® Groups) using random sampling (with a 90 percent confidence level with a 5 percent error rate) to review permissions and determine if sites were appropriately restricted. Since this was a statistical sample, the results can be projected to the population.

Site Type	Total Population	Sampled
SharePoint®	2,352	50
365® Group	<u>10,730</u>	<u>51</u>
Totals	13,082	101

Table1

- Selected two statistical samples, as shown in Table 2, of SharePoint® site owners (based on sites created in SharePoint® and by 365® Groups), active as of March 19, 2024, using random sampling (with a 90 percent confidence level with a 5 percent error rate) to survey owners and obtain their:
 - Understanding of site access management.
 - Understanding of data protection.
 - Awareness of available training.
 - Feedback on training content.

Since this was a statistical sample, the results can be projected to the population.

Owner Type	Total Site Owners	Number Surveyed
SharePoint®	808	48
365® Group	<u>2,908</u>	<u>51</u>
Totals	3,716	99

Table 2

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

In response to our management alert, TVA management implemented a new process to identify and restrict access to RPII on SharePoint® sites. However, we determined TVA's management of access to nonpublic critical and sensitive information could be improved. Specifically, other types of nonpublic critical and sensitive information were not included in the new process to identify and restrict access. In addition, we determined TVA was not providing SharePoint® site owners with appropriate training to properly manage access to TVA nonpublic critical and sensitive information.

MANAGEMENT OF ACCESS TO NONPUBLIC CRITICAL AND SENSITIVE INFORMATION COULD BE IMPROVED

In response to our management alert, dated March 13, 2024, TVA management implemented a new process to identify and restrict access to RPII on SharePoint® sites on March 18, 2024. As part of this audit, we reviewed a sample of 101 SharePoint® sites and verified access to information was properly restricted. However, other types of nonpublic critical and sensitive information, as defined by TVA-SPP-12.002, were not included in the new process to identify and restrict access. In addition, site owners have the ability to modify these access restrictions, possibly allowing access to nonpublic critical and sensitive information without a need to know as defined in TVA-SPP-12.002.

TRAINING COULD BE IMPROVED

We surveyed a sample of SharePoint® site owners (based on sites created in SharePoint® and by 365® Groups) to determine their understanding of their site access management responsibilities and training received. See Table 3 for sample sizes and responses received.

Owner Type	Number Surveyed	Responses Received
SharePoint®	48	35
365® Group	<u>51</u>	<u>42</u>
Totals	99	77

Table 3

The survey responses revealed 50 percent of the 42 sampled 365® Group site owners who responded to our survey, were not aware they were a SharePoint® site owner. In addition, 75 percent of the 77 combined SharePoint® site owners who responded to our survey did not recall receiving any training relevant to managing access to TVA nonpublic critical and sensitive information on SharePoint® sites. Since all 99 recipients of the survey did not respond, the results of the responses were not projected.

Based on the responses received, we determined (1) there was a general lack of knowledge surrounding the various methods of creating a SharePoint® site, and (2) TVA is not providing SharePoint® site owners with the knowledge and awareness to properly manage access to TVA nonpublic critical and sensitive information. While TVA provides SharePoint® training materials, our review of the training materials determined they were high level in nature and did not provide TVA-specific requirements for information protection and access management.

RECOMMENDATIONS

We recommend the Vice President and Chief Information and Digital Officer, Technology and Information:

1. Perform a risk assessment of SharePoint® access management to identify additional controls to mitigate inappropriate access to nonpublic critical and sensitive information.
2. Update TVA's SharePoint® training to provide site owners with the knowledge they need to properly protect TVA nonpublic critical and sensitive information.
3. Create a process to identify SharePoint® site owners and require them to complete initial and periodic refresher training.

TVA Management's Comments – In response to our draft report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

Tammy W. Wilson
Page 5
August 7, 2024

This report is for your review and information. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance. If you have any questions, please contact Scott A. Marler, Audit Manager, at (865) 633-7352 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.



David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

BPR:KDS

cc: TVA Board of Directors

Jessica A. Anthony

Brett A. Atkins

Faisal Bhatti

Tammy C. Bramlett

Janda E. Brown

Kenneth C. Carnes II

Sherri R. Collins

Melissa R. Crane

Buddy Eller

David B. Fountain

Melissa A. Livesey

Jeffrey J. Lyash

Christopher A. Marsalis

Jill M. Matthews

Todd E. McCarter

Dustin C. Pate

John M. Thomas III

Josh Thomas

Ben R. Wagner

OIG File No. 2024-17492

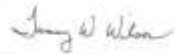
August 02, 2024

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2024-17492 SHAREPOINT
ACCESS MANAGEMENT

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Scott Marler, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.



Tammy Wilson
Vice President and Chief Information & Digital Officer
Technology and Innovation

KCC: BAA
cc (Attachment): Response to Request

Kenneth C. Cames
Dustin C. Pate
Brett A. Atkins
Sherri R. Collins
Jessica A. Anthony
Bradford W. King
Faisal Bhatti
Bradley E. Bennett
Bill Greer

David B. Fountain
Gregory G. Jackson
Melissa A. Livesey
Todd E. McCarter
Christopher A. Marsalis
John M. Thomas III
Melissa R. Crane
OIG File No. 2024-17492

Audit 2024-17492 SharePoint Access Management
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	We recommend the Vice President and Chief Information & Digital Officer, T&I: Perform a risk assessment of SharePoint® access management to identify additional controls to mitigate inappropriate access to nonpublic critical and sensitive information.	Management agrees.
2	Update TVA's SharePoint® training to provide site owners with the knowledge they need to properly protect TVA nonpublic critical and sensitive information.	Management agrees.
3	Create a process to identify SharePoint® site owners and require them to complete initial and periodic refresher training.	Management agrees.