PRIVACY, GOVERNMENTAL LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 28, 2015

Control #: PGLD-10-0815-0002
Affected IRM: 10.5
Expiration Date: August 28, 2017

MEMORANDUM FOR ALL EMPLOYEES

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

SUBJECT: Interim Guidance on SharePoint Privacy Policy

This memorandum issues privacy policy guidance for SharePoint site collections, including Privacy and Civil Liberties Impact Assessment (PCLIA) requirements.

Purpose: The interim guidance (IG) provides privacy policy and PCLIA requirements that SharePoint site collection owners, or their management official designees, shall follow when SharePoint site collections contain Sensitive But Unclassified (SBU) data, including Personally Identifiable Information (PII). For current definitions of SBU data and PII, refer to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, or the Privacy, Governmental Liaison and Disclosure (PGLD) website.

This guidance applies to all SharePoint site collection owners and designated management officials responsible for protecting SBU data in SharePoint site collections.

Background/Sources of Authority: These procedures and guidance comply with the E-Government Act of 2002, Section 208, Office of Management and Budget (OMB) Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Treasury Directives, and other Federal guidance. For a full listing of Privacy Law relevant to this IRM section, refer to Exhibit 10.5.1-2, *References*.

Procedural Change: The following procedural changes apply any time a SharePoint site collection contains SBU data.

Note: This policy does not apply to PII the IRS proactively makes available to all employees on resource sites (including, but not limited to, Discovery, Outlook Address Book, IRWeb, and SharePoint site collections), such as names and business contact information.

SharePoint PCLIAs Required

(1) Internal collaborative application sites (for example, SharePoint) that contain SBU data, including PII, require a PCLIA at the site collection level.

   a. Each site collection shall identify a site owner who shall be a management official, per IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance.*

   b. SharePoint site collection owners shall designate management officials to prepare SharePoint PCLIAs for new and existing site collections with SBU data.

   c. Privacy Review analysts in Privacy Compliance and Assurance (PCA), within PGLD, review and approve SharePoint PCLIAs.

   d. Refer to the PCLIA website for SharePoint PCLIA procedural details.

(2) New site collections with SBU data cannot be created without an approved PCLIA. Refer to SharePoint Central for more information on the site collection creation process.

(3) A PCLIA remains effective for up to three years from the date of approval, or until significant changes occur to the data or use of the site, whichever occurs first.

Overarching PCLIAs Encouraged

(4) Overarching SharePoint PCLIAs for multiple site collections are allowed as long as those collections all serve the same operational purpose and contain similar types and uses of SBU data.

(5) SharePoint site collection owners shall designate a management official at each major program area level to prepare an overarching SharePoint PCLIA for multiple site collections as long as those collections all serve the same operational purpose and contain similar types and uses of SBU data.

Data Access Limited

(6) SharePoint SBU data shall have strong access controls based on least privilege and need-to-know principles as designated in IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance*, related to Collaborative Technology and Systems, and the IRS Privacy Principles.

a. Restrict Internal Revenue Code (IRC) § 6103 data on SharePoint to cases where no other reasonable avenue exists to share the information with those assigned the case. Do not use SharePoint as a substitute for an existing system in place for sharing such data or working accounts. For example, if multiple people in different locations are assigned an account that is on the Integrated Data Retrieval System (IDRS), do not post IDRS information on SharePoint. Each person can access IDRS to view the account. However, if the taxpayer provides paper documentation (for all assigned the case) that cannot be scanned into another system for access, then it may be acceptable to scan and post on SharePoint, with proper access controls and safeguards.

b. Note: Information removed from SharePoint, such as scanned documents, no longer carry the SharePoint access protections. Additional steps (such as password-protected zip files) may be required to safeguard that information if it is moved or stored elsewhere.

(7) If IRC § 6103, Privacy Act, Title 18, Bank Secrecy Act, or other SBU data must be placed on SharePoint, strongly consider using SharePoint User Groups tied directly to Active Directory authentication for managing access. In limited circumstances, password-protected files may be necessary. Share the password(s) only with those who have a need to access the documents while working the accounts.

(8) The Privacy review of a SharePoint PCLIA may require other privacy risk mitigations, such as password protection, for certain site collections.

Compliance Monitored

(9) The PCA staff will monitor SharePoint site collections to ensure compliance with this policy and the use of SBU data as stated in that site collection's PCLIA.

(10) It is essential that SharePoint site collection owners, or their management official designees, also monitor their site collections for compliance with this policy. This includes, but is not limited to:

a. Preparing SharePoint PCLIAs for existing site collections discovered to contain SBU data

b. Submitting renewal SharePoint PCLIAs prior to the end of the three-year certification period for current PCLIAs

c. Ensuring new site collections with SBU data submit SharePoint PCLIAs prior to creation

d. Overseeing access controls and security per IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance.*

(11) Ultimately, it is the burden of the parent organization or Business Operating

Division's management officials to adhere to IRS SBU data protection standards for SharePoint site collections as specified in this policy.

(12) If SBU data is found on a SharePoint site collection that does not have a current or accurate PCLIA, that SharePoint site collection will be considered non-compliant, and the SharePoint site collection owner or designated management officials will be notified. Failure to respond puts the SharePoint site collection at risk for suspension from use until a SharePoint PCLIA is submitted and approved.

Effect on Other Documents: This guidance will be incorporated into IRM 10.5, *Privacy and Information Protection,* no later than August 28, 2017*.*

Effective Date: Immediately

Contact: If you have any questions, please contact John J. (Jack) Walker, Manager, Privacy Review, PCA, at *Privacy.

Distribution

www.IRS.gov