DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

September 13, 2013

Control #: PGLD-10-0913-0006
Affected IRM: 10.5
Expiration Date: September 13, 2014

MEMORANDUM FOR DISTRIBUTION

FROM: Susan B. Greer /s/ Susan B. Greer
Acting Director, Privacy and Information Protection

SUBJECT: Interim Guidance on SharePoint Privacy Impact Assessment Policy

This memorandum issues guidance on when Privacy Impact Assessments (PIAs) are required for SharePoint site collections.

Purpose: The interim guidance (IG) provides Privacy Impact Assessment (PIA) requirements that must be followed when SharePoint site collections contain Personally Identifiable Information (PII) or Sensitive But Unclassified (SBU) data. For current definitions of PII/SBU, please see links above on the PGLD website.

This guidance must be distributed to all personnel responsible for protecting PII/SBU. The policy applies to all employees, contractors and vendors of the Service.

Background/Sources of Authority: These procedures and guidance in IRM 10.5 comply with the Privacy Act of 1974, the Taxpayer Browsing Protection Act of 1997, the E-Government Act of 2002 (to include accompanying guidance outlined in OMB memoranda), the Consolidated Appropriations Act of 2005, §522, 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 PII or SBU data.

Note: This PIA policy does not apply to limited PII/SBU that normally appears on the SharePoint site collections, such as names and contact information about site members.

SharePoint PIAs Required

(1) Internal collaborative application sites (e.g., SharePoint) that will contain PII or SBU data require a Privacy Impact Assessment (PIA) at the site collection level. See the SharePoint PIA template at the PIA website to complete the SharePoint PIA process. Submit the SharePoint PIA via *Privacy, not PIAMS. Contact *Privacy with questions.

(2) New site collections with PII/SBU cannot be created without an approved PIA. Visit SharePoint Central for more information on the site collection creation process.

(3) Existing site collections that transitioned to SharePoint 2010 and have PII/SBU are required to go through a SharePoint re-certification. Part of that process will be to verify that an approved PIA exists for that SharePoint site collection.

Overarching PIAs Encouraged

(4) While the SharePoint PIA requirement is for the site collection level, ***overarching PIAs*** for multiple site collections are encouraged. Business units (ideally via Business Systems Planning representatives or SharePoint Stakeholders) should designate a management official at each major program area level to prepare an ***overarching PIA*** for multiple site collections as long as those collections all serve the same operational purpose and contain similar types and uses of PII/SBU. Each site collection covered by the overarching PIA must refer to the name of the overarching PIA in the new site collection creation or re-certification process.

Data Access Limited

(5) Balance the collaborative nature of SharePoint with the critical privacy protections required for PII/SBU data. When tax account information moves to a collaborative environment, privacy risks increase. To use this platform safely, strong controls must be put in place.

(6) Limit access to all PII/SBU data on a need to know basis, with access only by authorized individuals who require the information for the performance of official duties. The site collection owner will manage access to all content within their site collection. Follow security rules in IRM 10.8.1, Security Policy and Guidance, related to Collaborative Technology and Systems, and the IRS Privacy Principles.

(7) Restrict 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 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 (such as password protection).

(8) If IRC § 6103, Privacy Act, Title 18, Bank Secrecy Act, or other SBU data must be placed on SharePoint, strongly consider password-protecting the document(s) within the SharePoint site collection, again with strictly limited access. Share the password(s) only with those who have a need to access the documents while working the accounts.

(9) Upon review of a SharePoint PIA, the PGLD Office of Privacy Compliance may require password protection, or other privacy risk mitigations, for certain site collections.

(10) This PIA policy does not apply to limited PII/SBU that normally appears on the SharePoint site collections, such as names and contact information about site members.

Compliance Monitored

(11) The PGLD Office of Privacy Compliance will monitor SharePoint site collections to ensure compliance with this policy and the use of PII/SBU as stated in that site collection's PIA.

(12) It is essential that SharePoint site collection administrators also monitor their site collections for compliance with this policy and apply the appropriate security and access controls to protect the PII/SBU data, per IRM 10.8.1, Security Policy and Guidance, related to Collaborative Technology and Systems, and the IRS Privacy Principles.

(13) Ultimately, it is the burden of the parent organization or Business Operating Division and their programs to adhere to IRS PII/SBU data protection standards for SharePoint site collections as specified in this policy.

(14) If PII/SBU data is found on a SharePoint site collection that does not have a current or accurate PIA, that SharePoint site collection will be considered by the Office of Privacy Compliance to be non-compliant, and the site collection administrator will be notified. Upon notification, the site collection administrator (ideally via Business Systems Planning representatives or SharePoint Stakeholders) will have 20 business days to submit a SharePoint PIA to *Privacy. Failure to respond puts the SharePoint site collection at risk for suspension from use until a SharePoint PIA is submitted and approved.

Effect on Other Documents: This guidance will be incorporated into IRM 10.5.1, *Privacy, Information Protection & Data Security,* dated May 5, 2010, no later than September 13, 2014.

Effective Date: Immediately

Contact: If you have any questions, please contact me, or a member of your staff may contact Joseph P. Lynem, Associate Director, Office of Privacy Compliance, (202) 622-0162, or joseph.p.lynem@irs.gov.

Distribution
Commissioner of Internal Revenue
Deputy Commissioner for Operations Support
Deputy Commissioner for Services & Enforcement
Commissioner, Large Business and International Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax-Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Criminal Investigation
Chief Financial Officer
Chief Technology Officer
IRS Human Capital Officer
National Taxpayer Advocate
Executive Director, Equity, Diversity and Inclusion
Director, Affordable Care Act Office
Director, Office of Online Services
Director, Office of Professional Responsibility
Director, Privacy, Governmental Liaison and Disclosure
Director, Research, Analysis and Statistics
Director, Return Preparer Office
Director, Whistleblower Office
Associate Chief Information Officer, Cybersecurity
Chief Counsel
Chief of Staff