DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

August 31, 2016
Control #: **PGLD-10-0816-0005**
Affected IRM: **10.5.1**
Expiration Date: August 31, 2018

MEMORANDUM FOR DISTRIBUTION

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

Frances W. Kleckley
Digitally signed by Frances W. Kleckley
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Internal Revenue Service, ou=People, serialNumber=379408, cn=Frances W. Kleckley
Date: 2016.08.31 15:48:35 -04'00'

SUBJECT: **Shared Drives**

This Interim Guidance (IG) memorandum is to issue IG PGLD-10-0816-0005, guidance on **Shared Drives**.

Purpose: The interim guidance (IG) provides specific policy regarding methods for protecting privacy when shared drives contain Sensitive But Unclassified (SBU) data, including tax information and Personally Identifiable Information (PII).

Distribute this guidance to all personnel responsible for protecting SBU data, including tax information and PII. The policy applies to all employees, contractors, and vendors of the Service who are acting as site owners.

Background/Sources of Authority: IRM 10.5.1 is issued under the authority of the Privacy Act of 1974, the Internal Revenue Code, 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 laws relevant to this IRM section, refer to Exhibit 10.5.1-2, *References*. The IRS shared network drives (such as I drive, S drive, home directories, or other shared resources) are governed in part by the section SC-28 Protection of Information at Rest in IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance*.

Procedural Change: The following procedural changes apply when shared drives contain SBU data, including tax information and PII.

This IG amends IRM 10.5.1.6.16.1 (06-15-2016):

10.5.1.6.16.1 (MM-DD-YYYY) Shared Drives

(1) The IRS shared network drives (such as I drive, S drive, home directories, or other shared resources) are governed in part by the section SC-28 Protection of Information at Rest and the section Internal Collaborative Technology and Systems in IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance*. This policy makes it clear that the site owner must ensure that only those with a need-to-know should have access to SBU data on shared drives, with controls in place to limit access. Because of these controls, encryption is not required.

(2) To protect the privacy of employee and tax information, the law and IRS policy requires a Privacy and Civil Liberties Impact Assessment (PCLIA) when an agency uses PII in Information Technology to ensure examination and mitigation of privacy risks, with few exceptions.

(3) When a shared drive contains SBU data (such as PII, tax, or employee information), site owners must submit a PCLIA through the Privacy Impact Assessment Management System (PIAMS):

http://pipds.web.irs.gov/PIAMS/PIAMSHome.aspx

a. Use the PIAMS SharePoint PCLIA questionnaire because of the similar collaborative data use.

b. Prepare the PCLIA at the highest shared drive level (such as \\<server>\<share>\<department>), not the individual file or folder level. Indicate whether the SBU data is housed on a shared drive or SharePoint site and also note whether database(s) are included and what type.

c. Correctly align employee access to the shared drives and create a process for documenting access approvals.

d. Meet requirements outlined in IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance*, in the Access to Sensitive Information section. When automated checks can't be performed, business units are expected to perform due diligence and develop the appropriate awareness training, operational instructions, and job aids (e.g., banners, standard operating procedures, or handouts) to aid employees in self-reporting.

(4) For databases (unsupported by IT) on shared drives (i.e., Access databases):

a. Identify databases with SBU data.

b. Review shared drive content. Delete databases no longer needed or consolidate to shared drive(s) with SBU data.

Note: Prior to the deletion of unwanted databases/shared drives, owners must ensure adherence to appropriate records retention policies. For any databases or shared drives that contain federal records, it is good practice to fill out Form 11671: http://core.publish.no.irs.gov/forms/internal/pdf/f11671--2009-03-00.pdf

c. For databases remaining on shared drives, site owners must ensure compliance with one of the following options:

   - Complete a PCLIA for the shared drives with SBU data. Use the PIAMS SharePoint PCLIA questionnaire because of the similar collaborative data use.

     Note: These PCLIAs are valid for three years. Within three years of the approved PCLIA, the site owner must ensure deletion of the database from the shared drive or migration of the data to SharePoint (along with an updated PCLIA).

   - Move the data to move to an IT supported platform (such as SharePoint) and complete a SharePoint PCLIA at the site collection level.

   - Complete a system PCLIA on the individual application/database.

d. For more information on databases unsupported by IT, refer to the Enterprise Architecture: https://organization.ds.irsnet.gov/sites/eao/framework/content/main.htm

(5) For more information on PCLIAs, refer to IRM 10.5.2, *Privacy Compliance and Assurance*.

Effect on Other Documents: PGLD will incorporate this guidance into IRM 10.5.1, *Privacy and Information Protection, Privacy Policy,* no later than August 31, 2018.

Effective Date: Immediately

Contact: If you have any questions, please contact me, or a member of your staff may contact Greg Ricketts, Associate Director, Privacy Policy and Knowledge Management, at 901-546-3078, or Gregory.T.Ricketts@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 of Staff
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Communications and Liaison
Chief Counsel
Chief, Criminal Investigation
Chief Financial Officer
Chief, Planning, Programming & Audit Oversight
Chief, Risk Officer
Chief Technology Officer
Director, Affordable Care Act Office Director, Office of Compliance Analytics Director, Office of Online Services
Director, Office of Professional Responsibility Director, Office of Research, Analysis and Statistics Director, Privacy, Governmental Liaison and Disclosure Director, Return Preparer Office
Director, Whistleblower Office
Executive Director, Equity, Diversity and Inclusion
IRS Human Capital Officer
National Taxpayer Advocate
Treasury Inspector General for Tax Administration (TIGTA) Associate Chief Information Officer, Cybersecurity
www.irs.gov