

Date of Approval: **May 05, 2020**

PIA ID Number: **4848**

## **SYSTEM DESCRIPTION**

*Enter the full name and acronym for the system, project, application and/or database.*

SharePoint Platform, SP

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym and milestone of the most recent PCLIA?*

SharePoint (#2946)

*What is the approval date of the most recent PCLIA?*

12/20/2017

*Changes that occurred to require this update:*

Significant System Management Changes

Expiring PCLIA

*Were there other system changes not listed above?*

Yes

*What were those changes?*

The AvePoint and Nintex product suites have been installed and integrated with SharePoint. Nintex Forms provides users the ability to create web based forms as an alternative to InfoPath. Nintex Workflow provides business process automation capability as an alternative to SharePoint Designer workflows. AvePoint DocAve is a content realignment and system administration tool; AvePoint Governance Automation manages the approval and execution of Site Creation/Deletion/Recertification requests; AvePoint Compliance Guardian scans content for patterns which could identify PII/SBU or 508 problems; AvePoint Records provides electronic records management.

*What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.*

SharePoint reports to the Infrastructure Executive Steering Committee (ESC)

*Current ELC (Enterprise Life Cycle) Milestones:*

Operations & Maintenance (i.e. system is currently operational)

*Is this a Federal Information Security Management Act (FISMA) reportable system?*

No

## **GENERAL BUSINESS PURPOSE**

*What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.*

The purpose of the SharePoint software is to provide a backbone for team collaboration sites is to store, maintain, and share information as it correlates to the objectives and goals of the Internal Revenue Service (IRS) Business Units. It provides the tools to maintain and manage the IRS SharePoint platform, technical documentation, plans, policies, standard operating procedures, and allows users to leverage built-in tools for manipulating data and presentations. It will also house day-to-day materials to assist the teams with tracking progress including meeting minutes, agenda and internal knowledge documentation that assist in storing key internal knowledge for customers looking to create a SharePoint collection. SharePoint will host functionality such as collaboration on documents, document management, and structured data storage. Information owners are responsible for the data they share through the system and will complete a separate SharePoint Privacy Impact Assessment (SP PIA) as needed for any site collections storing Sensitive But Unclassified (SBU) or Personally Identifiable Information (PII) data.

## **PII DETAILS**

*Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?*

Yes

*Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?*

No

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

Yes

*Specify the PII Elements:*

Name

Mailing address

Phone Numbers

E-mail Address

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

Yes

*Specify the types of SBU from the SBU Types List*

Procurement sensitive data    Contract proposals, bids, etc.

Protected Information    Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Physical Security Information    Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

*Are there other types of SBU/PII used in the system?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Technical documentation, plans, policies, standard operating procedures, and presentations. It will also house day-to-day materials including meeting minutes, agenda and internal knowledge documentation that assist in storing key internal knowledge for customers looking to create a SharePoint collection. While the SharePoint core platform uses only limited PII (Name, SEID, work contact information, workstation information), individual sites may store PII/SBU information. Sites which will store PII/SBU are responsible for documenting how they will handle PII/SBU as part of obtaining a PCLIA for their site.

*Cite the authority for collecting SBU/PII (including SSN if relevant)*

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

PII for personnel administration is 5 USC

*Has the authority been verified with the system owner?*

Yes

## **BUSINESS NEEDS AND ACCURACY**

*Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.*

Standard Employee Identifier (SEID), Login Account, Name, Phone E-mail are used to grant access to SharePoint and specific Site Collections and may also be used by the SharePoint Services organization to contact users as part of the oversight and management of the SharePoint platform. IP Addresses and workstation information is recorded as part of system logging. Procurement and security information is only used for high-level executive communication and tracking; it is restricted to only those users. All other uses of SBU/PII will be documented in Site Collection specific PIAs.

*How is the SBU/PII verified for accuracy, timeliness and completion?*

SharePoint user information is obtained via a daily automatic synchronization with the IRS Active Directory (AD). Any corrections to the data should be handled per standard processes for updating the IRS AD. Procedures for verifying the accuracy, timeliness, and completeness of SBU/PII will be documented in Site Collection specific PIAs.

## **PRIVACY ACT AND SYSTEM OF RECORDS**

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

*Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.*

Yes

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 36.003 General Personnel and Payroll Records

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 34.037 Audit Trail and Security Records

## **RESPONSIBLE PARTIES**

*Identify the individuals for the following system roles:*

## Official Use Only

## **INCOMING PII INTERFACES**

*Does the system receive SBU/PII from other systems or agencies?*

No

## **DISSEMINATION OF PII**

*Does this system disseminate SBU/PII?*

No

## **PRIVACY SENSITIVE TECHNOLOGY**

*Does this system use social media channels?*

No

*Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?*

No

*Does the system use cloud computing?*

No

*Does this system/application interact with the public?*

No

## **INDIVIDUAL NOTICE AND CONSENT**

*Was/is notice provided to the individual prior to collection of information?*

No

*Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.*

Notice comes through such communications as the Privacy Act notification on Human Resource Connect (HR Connect) and e-Performance, Single Entry Time Reports (SETR), and other personnel systems. Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation. SharePoint is a document management and collaboration platform. Sites will be required to document how they handle this provision as part of obtaining a PCLIA for their site.

*Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?*

Yes

*Describe the mechanism by which individuals indicate their consent choice(s):*

SharePoint is a document management and collaboration platform. Sites will be required to document how they handle this provision as part of obtaining a PCLIA for their site.

*How does the system or business process ensure 'due process' regarding information access, correction and redress?*

All corrections or errors should be handled through the IRS standard process to correct errors with the IRS Active Directory. SharePoint is a document management and collaboration platform. Sites will be required to document how they handle this provision as part of obtaining a PCLIA for their site.

## **INFORMATION PROTECTION**

*Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)*

IRS Owned and Operated

*The following people have access to the system with the specified rights:*

*IRS Employees*

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

*IRS Contractor Employees*

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

*How is access to SBU/PII determined and by whom?*

Access to SharePoint and the creation of SharePoint user records is automatic based on the user's completion of the an Online-5081 request for access to the IRS network and agreement to those terms and conditions. Procurement and security information is only used for high-level executive communication and tracking; it is restricted to only those users. SharePoint is a document management and collaboration platform. Sites will be required to document how they handle this provision as part of obtaining a PCLIA for their site. Site Collection Administrators and Site Owners are responsible for the data they share through the system and will complete a separate SharePoint Privacy Impact Assessment (SP PIA), as needed, for any SharePoint Site Collection storing SBU or PII data.

## **RECORDS RETENTION SCHEDULE**

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?*

Yes

*How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.*

SharePoint is a document management and collaboration platform. Sites will be required to document how they handle this provision as part of obtaining a PCLIA for their site. GRS 3.1 Item 011-System development records-Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use. GRS 5.1 Item 010-Administrative records maintained in any agency office. Destroy when business use ceases.

## **SA&A OR ASCA**

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

Yes

*What date was it completed?*

6/3/2019



*Describe the system's audit trail.*

Production portion of the system is part of GSS-30 and inherits applicable controls. The platform records multiple types of audit data including IIS Logs, SQL Logs, and SharePoint ULS logs. SharePoint versioning functionality has been enabled to track history of information uploaded and updated. Additional options to audit access to information are available both within the SharePoint Administrative capabilities and an add-on tool Site Administrator Reports. These enable auditing of the access, or ability to access (via permissions), sites collections which are the containers of potential PII/SBU.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

No

*Please explain why:*

System is currently in operations and maintenance.

## **SBU DATA USE**

*Does this system use, or plan to use SBU Data in Testing?*

No

## **NUMBER AND CATEGORY OF PII RECORDS**

*Identify the number of individual records in the system for each category:*

IRS Employees: More than 100,000

Contractors: More than 10,000

Members of the Public: More than 1,000,000

Other: Yes

*Identify the category of records and the number of corresponding records (to the nearest 10,000).*

SharePoint is a document management and collaboration platform. Sites which store records are responsible for documenting as part of obtaining a PCLIA for their site.

## **CIVIL LIBERTIES**

*Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?*

No

*Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*

No

*Will this system have the capability to identify, locate, and monitor individuals or groups of people?*

No

*Does computer matching occur?*

No

## **ACCOUNTING OF DISCLOSURES**

*Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?*

No