Federal Trade Commission
Privacy Impact Assessment

Microsoft SharePoint

May 2018

PIA Template Version 1.51 – July 2017

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC or Commission) is an independent federal government law enforcement and regulatory agency with authority to promote consumer protection and competition through prevention of unfair, deceptive and anticompetitive business practices; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish these missions without unduly burdening legitimate business activity.

Microsoft SharePoint (SharePoint) is a commercial off-the-shelf web-based application that integrates with Microsoft Office to provide enhanced communication and collaboration features. SharePoint is an application that falls within a larger information system: the FTC Data Center General Support System (Data Center or Data Center GSS).[1] Both SharePoint and the Data Center are managed through the FTC's Office of the Chief Information Officer (OCIO).

SharePoint improves document sharing, collaborative editing, document management, and administrative efficiency. The FTC makes use of SharePoint to more efficiently and effectively complete its law enforcement and other missions. For example, through SharePoint, FTC staff can more easily share documents, collaboratively edit documents, and create document libraries. SharePoint also offers other administrative management features, such as a calendar feature. SharePoint sites can be set up and customized for individual FTC organizations and for particular business processes undertaken by those teams.

This Privacy Impact Assessment (PIA) discusses specific examples of offices' use of SharePoint, but such discussion is intended to be illustrative and not exhaustive. In the event of significant changes to FTC SharePoint use, such changes will be reflected in an updated PIA.

Specific offices and groups at the FTC use SharePoint to accomplish their individual purposes and goals. For example, the FTC Privacy Office uses SharePoint to edit PIAs collaboratively with stakeholders across different offices, including OCIO, Office of General Counsel (OGC), Records and Information Management (RIM), and others. The FTC Privacy Office has also used SharePoint to maintain an inventory of FTC systems containing PII and to manage the Social Media, Applications, and Websites (SAW) database. The Workplace Flexibility Taskforce and the Certificates of Public Advantage (COPA) Working Group use

[1]The Data Center is the primary IT infrastructure used by the FTC to host information systems, platforms, and applications that collect, process, disseminate, and store information in support of the Commission's mission. The Data Center supports the major administrative and mission functions of the Commission and provides for the internal and external transmission and storage of FTC data. For more information, see the FTC's Privacy Impact Assessment for the Data Center GSS. At times, the FTC Privacy Office exercises its discretion to conduct PIAs to assess privacy risks of technologies that are encompassed by one or more pre-existing PIAs. The Privacy Office is doing so for SharePoint, which is subject to privacy and security controls outlined in the Data Center PIA, for several reasons, including improving transparency about PII holdings in this application and clarifying that the FTC is not using particular advanced file sharing capabilities of SharePoint.

SharePoint to facilitate interoffice teamwork. The Financial Management Office (FMO) uses SharePoint for agency-wide risk management initiatives, such as audit findings or internal controls tracking, as well as for individual project documentation. OGC uses SharePoint to process FOIA appeals and to manage litigation holds. OCIO uses SharePoint to manage responses and artifact collection for Federal Information Security Modernization Act (FISMA) compliance activities.

FTC staff members upload into SharePoint data that has been created or obtained in connection with the Commission's law enforcement, policy and other activities. For example, such information may be obtained from public resources on the internet, non-public investigatory databases, other law enforcement agencies, and commercial databases such as Lexis/Nexis. Due to the diverse needs and uses of the groups within the FTC that use SharePoint, varied kinds of data are maintained in SharePoint. Further information about personally identifiable information (PII) and other information maintained in SharePoint is available in Sections 2.1 and 2.2, below.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in the FTC Data Center General Support System (GSS), on which the SharePoint application sits, is collected, maintained, and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C.§§ 41-58 and other laws and regulations the Commission enforces.[2] For more information, refer to the Data Center PIA.

[2] See https://www.ftc.gov/enforcement/statutes for additional statutes enforced or administrated by the Commission.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[3] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This list may not be exhaustive		
☒ Full Name	☒ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☒ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Alias	☒ Geolocation Information	☒ Investigation Report or Database
☒ Sex	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☐ Other *(Please Specify)*
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

SharePoint stores Commission documents containing various types of PII. Any information that can be stored on the shared network space also can be stored in SharePoint. (See Data Center PIA for more information.) This includes names, addresses, telephone and fax numbers, e-mail addresses, financial information such as bank account information, credit card information and Social Security numbers (SSNs) of individual defendants or respondents, witnesses, consumers or other non-FTC individuals. PII collected by the audit log is limited to login ID. User information profiles in SharePoint may include FTC employee or contractor data such as name, username, work e-mail, and department within the agency. Since SharePoint is a collaboration tool that is used by FTC staff to perform the Commission's law enforcement and other activities, the PII maintained in the system will depend on the particular business processes for which a SharePoint site is set up and is subject to change based on Commission needs.

For instance, the FOIA office maintains PII in SharePoint relating to communications with FOIA appellants, materials responsive to FOIA requests, appeal memos, and determination letters:

[3] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- Communications with Appellant: Communications (e.g., letters, e-mails and facsimiles) to and from the appellant, including the original request letter and the appeal letter. PII captured here can include, but is not limited to, names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the appellant or the person appealing on behalf of the appellant. Documents (such as an original FOIA request) may also contain SSNs.

- Responsive Materials: During the processing of the original request, the FOIA attorney or government information specialist assigned to the request retrieves copies of materials responsive to the request from other FTC offices. These documents consist of legal, investigatory, administrative, or similar nonpublic agency records, some of which may contain PII about investigatory targets or other individuals (e.g., witnesses, complaints, FTC staff, other consumers, or the requester) depending on the type and nature of the record. For example, such PII can include names, addresses, telephone numbers, or other information about an individual (e.g., a complaint by a consumer or description of an alleged violation by the subject of the investigation). During the appeal process, the FOIA attorney or government information specialist who processed the original request uploads these materials in PDF format to the SharePoint site so that the attorney assigned to the appeal can review the materials to determine whether the documents were properly released or withheld pursuant to the statutory standards.

- Appeal Memo and Determination Letter: Once the attorney assigned to the appeal has reviewed the original request and determination, the responsive materials, and the appeal letter, the attorney drafts a memorandum of law and fact for the General Counsel recommending the approval or denial of the appeal as well as a proposed determination letter addressed to the appellant. These documents are saved to SharePoint for review by the managing attorney and the Assistant General Counsel for FOIA. PII captured here can include, but is not limited to, names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the appellant or the person appealing on behalf of the appellant.[4]

Other offices house various types of PII in SharePoint depending on their needs. For instance, the COPA Working Group uses SharePoint to maintain contact lists for FTC staff members that include staff members' names and FTC contact information. This group also uses SharePoint to maintain contact lists for industry stakeholders. Likewise, OGC uses SharePoint to manage litigation holds. This includes regular emails to staff reminding them of their litigation hold obligations for matters in active litigation and the collection of information indicating whether staff have documents responsive to the litigation hold request.

SharePoint maintains a log of FTC user actions within the program. In general, this log is only available to select FTC employees and contractors in OCIO. Log data may be provided

[4] Some FOIA processing data is already maintained and managed by the FTC in itsFOIAExpress System , which has its own PIA on ftc.gov.

to other authorized entities, such as the Office of the Inspector General (OIG), for auditing purposes, if approved by OCIO. The log contains both PII and non-PII information about FTC SharePoint users, such as login ID and actions within a site. The purpose of this log is to allow oversight of SharePoint use and allow for investigation and accountability in the event of inappropriate use of SharePoint.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The FTC also houses a variety of non-PII information in SharePoint depending on the needs and purposes of the offices that use this software. (See the Data Center PIA for more information on the types of non-PII information collected and maintained.)

For example, the FTC Privacy Office's SharePoint pages include draft PIAs and other privacy-related documents. The Office of Policy Planning (OPP) uses SharePoint to house a variety of documents created in programs such as Word and Excel; some of the information in these documents is publicly available, and some is considered work product or non-public/Controlled Unclassified Information (CUI). FMO uses SharePoint to store and manage audit and control tracking documents for Corrective Action Plans. FMO also uses SharePoint to house other project specific documents, including those relating to Contract Lifecycle Management and to strategic planning.

The examples provided above are illustrative and not exhaustive. Additional documents that could be maintained or processed in SharePoint may include a variety of law enforcement documents – e.g., compulsory process documents, hearing transcripts, briefs, etc. – internal staff memoranda, Congressional correspondence, and Federal Register notices of rulemakings.

2.3 What is the purpose for collection of the information listed above?

As outlined in the Data Center PIA, information in the SharePoint application is collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, personnel management, and other activities. Further details about how and why the FTC collects information can be found in other Privacy Impact Assessments published on www.ftc.gov.

2.4 What are the sources of the information in the system/project? How is the information collected?

FTC staff members upload into SharePoint data that has been created or obtained in connection with the Commission's law enforcement, policy and other activities. For example, such information may be obtained from public resources on the internet, non-public

investigatory databases, other law enforcement agencies, and commercial databases such as Lexis/Nexis. More specifically, staff members from OPP save public information, such as news articles and other documents available on the internet, in SharePoint. FMO staff include publicly available audit/evaluation reports, nonpublic internal control reviews, and internally generated project documentation, in SharePoint. FOIA Office staff input information from law enforcement databases, FTC investigative files, FOIAXpress, and other sources. See the Data Center PIA for more information about the sources of the information stored in the SharePoint application.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
Offices, staff members, and contractors, who use SharePoint for job functions.	FTC staff and contractors who require information in support of FTC law enforcement and other activities, and in order to respond to FOIA and other disclosure requests, will have access to SharePoint. Many offices, such as OPP, FMO, and the Privacy Office, use SharePoint to share documents or information with other offices within the agency. FTC SharePoint sites are not accessible to anyone outside of the FTC. The internal entities who will have access to the information on any particular SharePoint site is dependent on the particular business purpose of the SharePoint site and the access permissions granted for that specific site. As with all applications that reside in the FTC's Data Center, access to any SharePoint site is restricted to those staff and contractors who need to access the site to fulfill job functions, i.e., access based on a least-privilege security model as described in Section 5.2.
Contractors or staff who need to perform site administration.	A small number of designated contractors or staff can access FTC SharePoint pages and data for the purpose of site maintenance as described in Section 3.2. The SharePoint contractor has signed an appropriate Non-Disclosure Agreement (NDA).
The FTC Office of the Inspector General (OIG)	Under appropriate circumstances, data housed in SharePoint, or SharePoint log data, may be provided to the OIG for auditing or law enforcement purposes.

External entities, such as other law enforcement agencies, do not have access to the FTC's SharePoint sites. The FTC may share information housed in SharePoint with other law enforcement agencies that have agreed, in writing, to treat the information confidentially. Individuals who file a FOIA request may be provided with information that FTC staff obtains from SharePoint, unless the information is subject to a FOIA exemption. Likewise, individuals who file a Privacy Act request may be provided with information about

themselves that is in SharePoint, subject to certain exemptions. Any sharing of information contained in SharePoint involves the extraction of data from the application before it is shared securely with the non-FTC party.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Authorized FTC contractors have access to information in the various systems and programs that comprise the Data Center, including, when necessary, SharePoint. Some authorized FTC contractors have access to SharePoint simply as users, and another authorized FTC contractor (or small number of contractors) has access to SharePoint as an administrator.

The contractor (or contractors) with administrative access to SharePoint, also known as a Farm Administrator, a term used by Microsoft SharePoint guidance, is referred to as the SharePoint Administrator. A small number of staff or contractors have administrative access as Site Collection Administrators. The SharePoint Administrator can view the audit log of FTC user SharePoint activity and, if needed, can give a small number of OCIO staff permission to view the audit log. The SharePoint Administrator creates new sites and pages as needed and performs other technical tasks relating to SharePoint administration, content management, and development. The Site Collection Administrators manage SharePoint site collection features, and upon user request, can create sites within SharePoint site collections.

All FTC contractors are required to sign NDAs, complete security and privacy training prior to obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access and access to those systems.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

Contractors who access the Data Center GSS, including SharePoint, are subject to the same rules and policies as FTC staff. The SharePoint contractor is subject to the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☒ Oral)
- ☒ FTC Website Privacy Policy
- ☒ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☐ Other (*explain*):

☐ Notice is not provided (*explain*):

Wherever possible, the FTC provides timely and effective notice to the public and/or to individuals about activities that impact privacy, including the collection, use, disclosure, and disposal of information at the time the information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). The FTC's Privacy Act statements are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form. For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its Privacy Policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

The opportunity or right depends on how the information is collected and the purpose for the collection. The FTC does not use SharePoint to collect information, including PII, directly from the public. However, SharePoint may contain information, including PII, collected from the public in furtherance of the FTC's law enforcement or policy mission. (For details on the ways that the FTC collects information from the public, please read the other PIAs on the FTC's website.)

In some instances when the FTC collects information from the public, individuals are provided with the opportunity to consent, or to withhold consent, prior to the collection of their PII.[5] However, in some instances, individuals are *not* provided with the opportunity to consent (or to withhold consent) prior to the collection of their PII.[6]

[5] For instance, sometimes individuals provide information to the FTC voluntarily, such as when individuals submit comments in rulemaking proceedings or send correspondence to Congress which is then forwarded to the FTC, and when investigatory targets agree to provide information to the Commission in lieu of compulsory process, and in the case of FOIA requests and appeals.

[6] FTC staff also obtain information in response to compulsory process, such as subpoenas and civil investigatory demands, or via discovery in administrative and federal court litigation. Those who provide information pursuant to

SharePoint is used in a variety of ways for a variety of mission-related purposes throughout the FTC. Accordingly, some PII housed on SharePoint may have been initially collected after providing individuals the opportunity to give, or withhold, consent to collection or to particular uses of their information, and some of the PII housed on SharePoint may have been initially collected without doing so. Additionally, some of the information on SharePoint may not have been collected from the public at all.

SharePoint is software that operates as part of the FTC's Data Center. Accordingly, the FTC does not ask members of the public for consent before inputting PII into SharePoint, and individuals do not have the right to consent to particular uses of the information stored in SharePoint.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on Data Center GSS, including any data stored in the SharePoint application. The FTC's Privacy Policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions. In addition, there may be public information stored in SharePoint that also appears on the FTC's website and is accessible to the public there.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As specified above in Section 4.3, the FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in SharePoint.[7] The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted on the Data Center GSS, including data in SharePoint. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file FOIA requests for agency records about them (if they

---

compulsory process do not generally have a right to decline to provide the information. In addition, the SharePoint application collects information (i.e. for the audit log) from system users: FTC SharePoint users do not have the right to decline to provide this information.

[7] In some cases, FTC SharePoint users may not need to file a Privacy Act request to access or correct their own records. For example, managers may ask their employees to maintain and update SharePoint folders or documents containing the employees' emergency contact information or telework schedules. If employees have questions about the metadata that SharePoint collects about them (for instance, if they are concerned that the metadata may not be accurate), they may contact OCIO.

are not exempt from disclosure to them under those laws).[8] Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information that is collected and stored in SharePoint generally will not be systematically checked for accuracy and timeliness. However, information that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures) that are relevant to the business process for which the SharePoint site is set up.

For example, with respect to FOIA and Privacy Act appeals, information about appellants has been collected from the appellants themselves (i.e., their original request letters, appeal letters, and related communications). OGC staff checks the accuracy and timeliness of this information (e.g. contact information, precise scope of the request or appeal) as necessary to allow FTC staff to respond to or contact an appellant with respect to the original request and any subsequent appeal. However, the OGC staff does not check the accuracy or timeliness of responsive documents that are uploaded to SharePoint for attorney review, including any PII that may be contained in such documents. The FTC is required under FOIA to grant or deny access to responsive records "as is," without alteration. The accuracy and timeliness of the information (including any PII) contained in such records, would be governed by other laws and authorities, if any, applicable at the time the agency compiles those records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

All information in the Data Center GSS, including the information stored in SharePoint, is also subject to appropriate information security controls, as further described below in this PIA and the Data Center PIA. These controls will ensure that sensitive information is protected from any undue risk of loss and that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the Data Center GSS.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

[8] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

There are administrative procedures, technical safeguards, and controls in place to protect and ensure proper use of data in SharePoint.

The FTC limits site collection creation rights to the SharePoint Administrator. To create a new SharePoint site collection—for instance, a top-level site for a new office or group within the agency—a user must contact the FTC's SharePoint Administrator, who will create this site collection. Upon request from SharePoint users, the SharePoint Administrator or Site Collection Administrators can create sites within site collections (provided that the SharePoint Farm Administrator or Site Collection Administrator has "full control" access to that site collection). Full control users of a site, which may include the SharePoint Farm Administrator or Site Collection Administrator, can create sites/subsites within that site.

FTC SharePoint sites are not accessible to anyone outside the FTC. The only staff members within the agency who can access a given SharePoint site are those who have been granted access by the SharePoint Administrator, Site Collection Administrator, or another current member with full control. This process also applies to staff members/contractors who need access for IT administration purposes. See section 3.1 and 3.2 for more details on SharePoint access and privileges for IT staff and contractors. Any users who have not been given permission to access any given site will not be able to access that site. Additionally, SharePoint users (including administrators) can only search within sites to which they have been given access.

When the SharePoint Administrator receives a request from a staff member who wants access to a particular SharePoint site, the SharePoint Administrator confirms with a site member with full control or with the requestor's supervisor to ensure that it is appropriate for the requesting staff member to access the particular site before granting access. This is done to conform to a least-privilege security model for SharePoint access at the FTC.

In accordance with FTC policies and procedures, other full control members of site collections, sites, or subsites must only grant access to staff members/contractors with a legitimate business need for access, which also allows the FTC to follow the principle of least-privilege regarding access to SharePoint.

The specific procedures for granting access using the least-privilege principle vary somewhat by office of group. For instance, the Bureau of Consumer Protection has a small group of staff members who oversee and perform many SharePoint access control functions for the entire bureau. In the FOIA office in OGC, the managing attorney for the FOIA Appeals SharePoint site grants site permissions only to those persons working on a particular appeal, and then only to those documents each individual needs to access. The FOIA government information specialist or attorney that processed the original request will be provided with access in order to upload and save the original request and determination letters and the responsive documents to the site. However, the FOIA government information specialist or attorney that processed the original request will not have access to the appeal memorandum of law and fact and the appeal determination letter. Access to these appeal documents will be limited to the attorney assigned to the matter, the managing attorney, the Assistant General Counsel for FOIA, and the General Counsel or Acting General Counsel. Moreover, staff in

other sections of OGC, and of the FTC generally, do not have access permission to the SharePoint site for FOIA appeals. Administrator rights are limited to the managing attorney and his or her administrative assistant, who will create new folders within the site as necessary and provide appropriate access permissions to those staff working on a particular appeal. FTC OCIO professionals have access as necessary to administer and support FOIA appeal processing.

The FTC also employs other SharePoint-specific controls to promote oversight. For example, for each site, site members with full control privileges can view a list of the employees who have access to that site, as well as the level of access they have (for instance, which other employees have full control privileges). This function can allow site members to notice and fix situations in which site members who no longer need access to a site continue to have access, for instance. Also, SharePoint maintains a log of FTC user actions within the program, as described in section 2.1 above.

Other procedures, technical safeguards, and controls that protect data in SharePoint pertain to the Data Center in which SharePoint is housed, as well as to the FTC's security procedures more broadly.

All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access any application in the Data Center GSS, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. Categories of employees deemed to be higher risk – such as interns and International Fellows – may have restricted access to network and physical space.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

FTC staff is responsible for minimizing PII and disposing of it when the PII is no longer needed and in accordance with the FTC records disposition schedule. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security and Privacy Awareness training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

A more thorough discussion of the Data Center's administrative procedures, technical safeguards, and other controls are available in the Data Center PIA.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

SharePoint is hosted within the FTC Data Center GSS. A risk assessment was completed as part of the Security Assessment and Authorization. The FTC follows all applicable FISMA requirements and other applicable federal guidance to secure the Data Center GSS. The Data Center GSS is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The Data Center GSS received an authority to operate in October 2017.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ **Not Applicable**

The FTC does not use PII to conduct testing, training, or research in SharePoint.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Information in the Data Center (of which SharePoint is a component), including information, if any, that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with applicable FTC policies and procedures, as well as with the FTC records disposition schedule and General Records Schedules approved by the National Archives and Records Administration (NARA). FTC staff receive training and reminders about their records and destruction obligations. Deleted information is securely and irreversibly destroyed within thirty days in accordance with applicable FTC policies and procedures, OMB, NARA, and NIST regulations and guidelines. There are no additional security risks posed by the deletion of information in SharePoint.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

No. The FTC's SharePoint configuration is an intranet site accessible through the FTC network, and only FTC staff and contractors have access to it. The FTC's SharePoint uses session and persistent cookies to keep SharePoint from "timing out" while a user is logged

into it, but these cookies are used for internal purposes only. SharePoint is not accessible via an external website or portal and it does not collect information directly from the public.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Information contained in SharePoint may be inaccurate or incomplete.	See Section 5.1 of this PIA.
Individuals who have access to PII on SharePoint could exceed their authority and use the data for unofficial/unauthorized purposes.	SharePoint maintains a log of FTC user actions within the program. See section 2.1 for details.
FTC employees who are not authorized to access particular SharePoint pages with sensitive information could gain access to such pages.	See Section 5.2 for details on how the FTC implements least-privilege access principles in SharePoint.
Staff members could overlook files relevant to FOIA and Privacy Act requests that are stored in SharePoint.	When responding to FOIA/PA requests, staff members confirm via a "FOIA Request for Documents" checklist that they have searched SharePoint for responsive documents.
SharePoint's advanced sharing features could be used to share information with unauthorized parties.	SharePoint does have certain features that would present new privacy risks if enabled, but these features are not enabled for the FTC configuration. For example, SharePoint can be configured such that SharePoint sites and any documents saved to the sites can be accessed from any web browser as well as certain mobile devices. This feature is not available to FTC users. In order to access SharePoint sites, FTC users need to be working within the FTC network, connecting to the system from within an FTC building or through the FTC's secure web-based connection, SAFE. Likewise, SharePoint can be configured to allow users to broadcast PowerPoint presentations on the web, publish Excel documents on the web or to extranet sites, and publish Access databases on the web or to extranet sites. However, these features are not available to FTC users. FTC users are restricted to publishing

	information within the intranet SharePoint sites to which they have been given access. Furthermore, the FTC SharePoint configuration allows the sharing of links to documents (e.g., through email), but the links can only be accessed from within the FTC network.
FTC users could gather unnecessary PII and subsequently enter it into SharePoint.	The FTC has taken steps to minimize the amount of information that the agency collects and maintains about individuals. For example, the FOIA office, which uses SharePoint, only asks for the minimum amount of contact information from individual requestors necessary to communicate with them and respond to their requests and appeals as required by law.[9]
FTC staff may not dispose of documents containing PII in SharePoint in accordance with the FTC and NARA records disposition schedules.	During the FTC's annual Lighten Up! day, and through ongoing tips and training, staff are reminded to dispose of all material stored anywhere on the network (shared drive, individual drives, SharePoint) in accordance with the FTC's policies and procedures.
SharePoint saves every version of documents edited there, which runs counter NIST 800-53, App. J data minimization requirements.	In this instance, the cost in terms of data minimization is outweighed by the benefits of document preservation. Staff can collaboratively edit documents and retain an organized "paper trail" of how the document changed over time, which could be helpful in litigation hold contexts. If staff adhere to records retention requirements and participate fully in Lighten Up Day, they will delete unnecessary drafts in SharePoint at least annually.
Individual users could set up unauthorized SharePoint sites, leading to information being maintained on such sites without proper oversight and auditing.	Individual users cannot create top-level SharePoint sites (i.e. site collections) at will; they must do so via the SharePoint Administrator and/or other authorized tech personnel as described in section 5.2 above.

[9] The FOIA online request form alerts requesters not to provide sensitive PII to the agency unless necessary to authenticate a specific request. During the appeal process, only the information necessary to make a determination on the appeal is saved to the SharePoint site, and only those FTC staff who are working on the appeal (the FOIA government information specialist or attorney who processed the original request, the attorney assigned to the appeal, the managing attorney(s), the Assistant General Counsel for FOIA, and the General Counsel or Acting General Counsel) have access to the information. See also sections 3.1 and 3.2 on IT staff SharePoint access and roles.

SharePoint sits within the Data Center GSS. A fuller discussion of other privacy risks and risk mitigations associated with the Data Center is available in the Data Center PIA.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Yes, there are automated privacy controls and advanced capabilities to support privacy in the SharePoint application.

For example, the SharePoint Administrator maintains the log described in section 2.1 via the SharePoint application. Individual users cannot create top-level SharePoint sites at will; site and page creation is managed as described in section 5.2. Access to SharePoint sites is managed via least-privilege principles as described in section 5.2.

Other automated privacy controls pertain to the Data Center, of which SharePoint is a component. See the Data Center PIA for more information.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The SharePoint application , like the Data Center GSS in which it resides, is not considered a Privacy Act system of record of its own accord. SharePoint is an application that stores data from designated Privacy Act systems.

SORNs may apply to data housed in SharePoint depending on the data that various offices are uploading to SharePoint, and on the systems with which the underlying data is affiliated. For instance, with respect to the FOIA and Privacy Act SharePoint site, records pertaining to FOIA and Privacy Act appellants are covered by: V-1 – Freedom of Information Act Requests and Appeals –FTC, and V-2 –Privacy Act Requests and Appeals—FTC; records pertaining to individuals whose information may be retrieved from some responsive materials would be covered by I-1—Nonpublic Investigational and Other Nonpublic Legal Program Records—FTC, I-6 –Public Records—FTC, or other applicable FTC SORNS. Additionally, login data and other user data collected by SharePoint are covered by VII-3—Computer Systems User Identification and Access Records—FTC. A complete list and copies of these SORNs is available online at www.ftc.gov.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The SharePoint Administrator maintains a log of FTC user actions within the program as described in section 2.1. The collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy.

More generally, for the Data Center, access logs, storage logs, and firewall logs are periodically reviewed to ensure that users are complying with Data Center policies and procedures. PIAs, including this one, are reviewed routinely to ensure accuracy. In addition, all FTC staff and contractors must review and sign the FTC Rules of Behavior form and take privacy and security training on an annual basis.

9 Approval and Signature Page

Prepared By:

_____ **Date:** _____
Bruce Jennings
Assistant Director, OCIO Touch Services

Reviewed By:

_____ **Date:** _____
John Krebs
Acting Chief Privacy Officer (CPO)

_____ **Date:** _____
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date:** _____
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date:** _____
Yvonne Wilson
Records and Information Management Services

Approved By:

_____ **Date:** _____
Raghav Vajjhala
Chief Information Officer (CIO)