

SSP ATTACHMENT 4 –

FedRAMP Privacy Impact Assessment (PIA)



Microsoft


Office 365 FedRAMP Environments

Version 7.0


July 30, 2021

Controlled Unclassified Information

Prepared by

First Information Technology Services, Inc.		
	Street Address	1 Microsoft Way
	Suite/Room/Building	Building 31
	City, State, ZIP	Redmond, WA 98052

Prepared for

Microsoft Corporation		
	Street Address	1 Microsoft Way
	Suite/Room/Building	Building 31
	City, State, ZIP	Redmond, WA 98052

Revision History

Detail specific changes in the table below

Date	Version	Page(s)	Description	Author
5/2/2012	1.0	N/a	Document Publication	FedRAMP Office
12/19/2012	1.1	N/a	First draft in FedRAMP Template	A.J. Schwab
1/15/2013	1.2	N/a	Second draft in FedRAMP Template	A.J. Schwab
2/23/2013	1.3	N/a	Final draft in FedRAMP Template	A.J. Schwab
2/26/2013	1.4	N/a	Final for Publication	A.J. Schwab
4/11/2014	1.5	N/a	Annual Review	A.J. Schwab
8/10/2015	1.6	N/a	Reviewed for compliance	Microsoft
12/14/2015	1.7	N/a	System version update	Microsoft
1/31/2017	2.0	All	Annual review and update to current FedRAMP template	Microsoft
8/16/2018	3.0	N/a	Annual review	Microsoft
7/26/2019	4.0 (GCCH) 4.0 (DoD) 5.0 (MT)	N/a	Annual review	Microsoft
7/24/2020	6.0 (All)	N/a	Annual review, environment consolidation	Microsoft
7/30/2021	7.0	N/a	Annual review	Microsoft

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact info@fedramp.gov

For more information about the FedRAMP project, see www.fedramp.gov

Table of Contents

1	PRIVACY OVERVIEW AND Point of Contact (POC).....	1
1.1	Applicable Laws and Regulations.....	1
1.2	Personally Identifiable Information (PII).....	2
2	Privacy Designation.....	3
3	Privacy Impact Assessment Talking Points	3
3.1	PII Mapping of Components (SE-1, DM-1).....	4
3.2	Prospective PII Use.....	7
3.3	Sources of PII and Purpose	8
3.4	Access to PII and Sharing.....	9
3.5	PII Safeguards and Liabilities.....	10
3.6	Contracts, Agreements, and Ownership	12
3.7	Accuracy of the PII and Redress.....	13
3.8	Maintenance and Administrative Controls.....	13
3.9	Business Processes and Technology.....	15
3.10	Privacy Policy	15
3.11	SIGNATURES.....	16
4	ACRONYMS.....	16

List of Tables

Table 1-1	Office 365 Privacy POC.....	1
Table 1-2	Office 365 Laws and Regulations	1
Table 3-1	PII Mapped to Components.....	4

1 PRIVACY OVERVIEW AND POINT OF CONTACT (POC)

The Table 1-1 - Office 365 Privacy POC individual is identified as the Office 365 Privacy Officer and POC for privacy at Microsoft.

Table 1-1 Office 365 Privacy POC

Name	Greg Roberts
Title	Microsoft Office 365 Principal Group Program Manager
CSP / Organization	Microsoft / Office 365
Address	1 Microsoft Way, Redmond, WA 98052
Phone Number	425-882-8080
Email Address	O365PrivacyQuestions@microsoft.com

1.1 APPLICABLE LAWS AND REGULATIONS

The FedRAMP Laws and Regulations can be found on: www.fedramp.gov

Table 1-2 Office 365 Laws and Regulations include additional laws and regulations specific to Office 365. These will include law and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 1-2 Office 365 Laws and Regulations

Identification Number	Title	Date	Link
5 USC 552a	Title 5 Government Organization and Employees; Chapter 5 Administrative Procedure; Section 552a Records maintained on individuals (Privacy Act of 1974 as amended)	January 2014	5 USC 552A
OMB Circular A-130	Managing Information as a Strategic Resource	July 2016	OMBA-130
OMB M-03-22	OMB Guidance for Implementing the Privacy Provisions	September 2003	OMB M-03-22
OMB M-07-16	Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)	May 2007	OMB M-07-16
OMB M-10-23	Guidance for Agency Use of Third-Party Websites	June 2010	OMB M-10-23
OMB M-99-18	Privacy Policies on Federal Web Sites	June 1999	OMB M-99-18

Identification Number	Title	Date	Link
PL 100-503	Consolidated Appropriations Act of 2005, Section 522	October 1988	PL100-503
PL 104-191	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	August 1996	PL 104-191
PL 104-231	Electronic Freedom of Information Act As Amended in 2002 [PL 104-231, 5 USC 552], October 2, 1996	October 1996	PL 104-231
PL 107-347	E-Government Act of 2002 - Federal Information Security Management Act (FISMA) of 2002, Title III	December 2002	PL 107-347
PL 107-347 208	E-Government Act of 2002 - Sec. 208. Privacy provisions.	December 2002	PL 107-347 208
PL 107-347 V	E-Government Act of 2002 - The Confidential Information Protection and Statistical Efficiency Act (CIPSEA), Title V	December 2002	PL 107-347 V
PL 113-187	44 U.S.C The Presidential and Federal Records Act Amendments of 2014 showing changes to NARA Statutes found below in Chapters 21, 22, 29, 31, 33, of Title 44 in PDF.	December 2014	PL 113-187
NARA	44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33 (see Public Law 113-187)	February 2008	NARA 44USC
FTC	Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices	June 2008	FTC Sec-5
ECFR	Title 36, Code of Federal Regulations, Chapter XII, Subchapter B	March 2016	e-CFR data
NCSL	State Privacy Laws	January 2016	NCSL

1.2 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information

- DNA information
- Bank account numbers
- Voice recordings

PII refers to information that can be traced back to an individual person.

2 PRIVACY DESIGNATION

Cloud Service Providers (CSPs) perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt-out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.

Federal cloud customers (data owner/system owners) are required to perform their own Privacy Impact Assessments and may share this information with the CSP if they so desire (for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII).

Threshold Analysis

Check one.

- Opt-out. This cloud will not host privacy information.
- This cloud is willing to host privacy information.

Select the cloud layers that are represented by Office 365 GCC High and DoD. Select all that apply.

- This cloud includes Software as a Service (SaaS).
- This cloud includes Platform as a Service (PaaS).
- This cloud includes Infrastructure as a Service (IaaS).

3 PRIVACY IMPACT ASSESSMENT TALKING POINTS

According to NIST SP 800-122, Appendix D,

There must be no personal data record-keeping systems whose very existence is secret.

Additionally, NIST SP 800-122, Appendix D states,

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

In light of the NIST guidance, Privacy Impact Assessment talking points have been developed for the purpose of ensuring full disclosure between stakeholders.

Identifiers in parenthesis after a section title indicate NIST SP 800-53, Appendix J privacy controls that are related to the particular talking point. These mappings to Appendix J privacy controls are not considered a replacement for Appendix J controls.

3.1 PII MAPPING OF COMPONENTS (SE-1, DM-1)

Office 365 consists of seventeen (17) key components and one (1) optional component. Each component has been analyzed to determine if any elements of that component collect and/or store PII. The type of PII collected and/or stored by Office 365 and the functions that collect it are recorded in Table 3-1. Unless otherwise noted, responses to PTA/PIA questions are for the key components of Office 365 rather than the optional components.

Table 3-1 PII Mapped to Components

Components	Does this Component Collect or Store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
Activity Feed Services (AFS)	Yes	AAD OrgID, user ID, username, email address, tenant ID, activity group, activity group item, device subscription ID	Enables collection & synchronization of a user's data across devices where their MS account is connected.	Microsoft applies controls based on a FIPS 199 High level data classification.
Bing	Yes	The platform supports several types of data storage, which may include name, address, e-mail address and phone number, Tenant ID. The service can also contain the content from the tenant's mail (i.e. Exchange Online) and conversational (i.e. Microsoft Teams) services.	Storing ground truth of data and creating search index.	Microsoft applies controls based on a FIPS 199 High level data classification.
Customer Insight and Analysis (CIA)	Yes	AAD OrgID, user ID, e-mail address, Tenant ID, username	To correlate data and provide customer facing usage reports to show how subscription is being consumed.	Microsoft applies controls based on a FIPS 199 High level data classification.
Cloud Input Intelligence (CII)	No	N/a	N/a	N/a

Delve <i>(MT Only)</i>	Yes	AAD OrgID, Tenant ID, user's outlook properties, group memberships, user photo	Delve allows customers to manage their Office 365 profile, and to discover and organize the information that's likely to be most interesting to him/her across Office 365.	Microsoft applies controls based on a FIPS 199 High level data classification.
Exchange Online (EXO)	Yes	Information contained in the tenant's mail service. Microsoft refers to this as "address book" data, which may contain name, address, e-mail address, and phone number, Tenant ID Exchange Online uses AAD OrgID to authenticate the user and Mailbox GUID to identify user's mailbox.	Provides full featured e-mail capability.	Microsoft applies controls based on a FIPS 199 High level data classification.
Fast Track Migrations	Yes	User UPN, Account Name, User SMTP, customer contacts (email addresses), Tenant ID,	PII collected provides the ability for full feature functionality, identifying mailboxes and migrating them to the proper source/target.	Microsoft applies controls based on a FIPS 199 High level data classification.
Information Protection (IP) (previously named Exchange Online Protection (EOP))	Yes	Information Protection collects Client IP, username, email address, organization address, work phone number, URLs, AAD OrgID, User/Network/Server IP Addresses, and Mailbox GUID.	Provides email, file attachment, and URL threat protection against viruses, malware, phishing, and spam.	Microsoft applies controls based on a FIPS 199 High level data classification.
Loki	Yes	AAD OrgID, Tenant ID, user's outlook properties, group memberships, user photo	Loki powers people experiences across M365 which surface various personas data.	Microsoft applies controls based on a FIPS 199 High level data classification.

Microsoft Teams (MS Teams)	Yes	MS Teams collects channel/team names, user principal name, emails/email notifications, username/display name, address book data, Tenant ID, tenant region/cloud, tenant usage data, domain name, AAD OrgID.	Supports communication between MS Teams users within a tenancy and its associates.	Microsoft applies controls based on a FIPS 199 High level data classification.
Office Intelligent Services (IS)	Yes	Machine Name, IP address, username, user ID, Device ID, Tenant ID, Session ID, email address, filenames, voice data (translation/dictation) and document content.	Providing the Office Intelligent Services to Office 365 customers, licensing purposes, and diagnostics and monitoring of these services.	Microsoft applies controls based on a FIPS 199 High level data classification.
Office Services Infrastructure (OSI)	No, OSI only stores azure metadata on the partner services.	N/a	N/a	N/a
Office 365 Remote Access Service (ORAS, previously named Security Workload Environment (SWE))	Yes	ORAS collects events of remote desktop connections made by Microsoft personnel to Office 365 systems, which may include ORAS Username, Tenant ID, client computer name or IP address, IP or name of destination address.	ORAS collects events to achieve an extremely rigorous level of auditing of all RDP connections by Microsoft personnel, including actions involving PII.	Microsoft applies controls based on a FIPS 199 High level data classification.
Query Annotation Service (QAS)	No	N/A	N/A	N/A
Search Content Services (SCS)	Yes	Tenant ID, customer documents could contain PII.	Tracking document content and indexing data.	Microsoft applies controls based on a FIPS 199 High level data classification.

Microsoft Office 365 Privacy Impact Assessment
Version 7.0 July 30, 2021

Skype for Business (SFB)	Yes	Skype for Business collects SIP URI (Session Initiation Protocol Uniform Resource Identifier), Client Mac Address, Client IP, Tenant ID, phone number, client machine FQDN, username, IP Address. SFB uses AAD OrgID to authenticate the user.	Supports communication between SFB users.	Microsoft applies controls based on a FIPS 199 High level data classification.
SharePoint Online (SPO)	Yes	SharePoint stores data from AAD (username, user display name, user outlook properties, group memberships), and any PII voluntarily entered in user documents or within a SharePoint Online site or list. SharePoint Online uses AAD OrgID to authenticate the user.	Supports document management.	Microsoft applies controls based on a FIPS 199 High level data classification.
Office 365 Suite Experience (SUE)	Yes	When a tenant admin logs into the Office 365 Suite, Azure Active Directory content for the user is transferred to Suite, which includes AAD OrgID, IP address, user photo image, phone number, mobile phone number, email address	Supports user login, and product service and usage.	Microsoft applies controls based on a FIPS 199 High level data classification.
Office Web Applications(WAC)	Yes	Office Web Apps uses AAD OrgID to authenticate the user. Email address will be collected when it is voluntarily provided by the customer via the feedback tool.	Supports rendering of documents.	Microsoft applies controls based on a FIPS 199 High level data classification.
Microsoft Support (Optional Support)	Yes	Users are responsible for the amount of information, including PII that is provided to Microsoft Support.	To resolve Service questions.	Microsoft Support is managed according to Microsoft Corporate Policies.

3.2 PROSPECTIVE PII USE

Respond to the following questions:

1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1)

See chart in section 3.1 above.

2. If PII fields are used, can individuals “opt-out” of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1)

When an organization signs up with Microsoft Office 365, it enables the transfer of data types shown in section 3.1 above. This an agency-wide decision. Microsoft does not share data with government agencies unless required by law.

- Yes Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1)
Click here to enter explanation.
- No It is not possible to opt-out.

3.3 SOURCES OF PII AND PURPOSE

3. Does Microsoft have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

Microsoft does maintain a list of federal agencies consuming the service under an Authority To Operate (ATO) to enable ongoing continuous monitoring reports and other notifications required under FISMA.

Microsoft personnel do not have standing access to, and are prohibited from viewing, customer data and PII in any service component except as required to support the service, handle an incident, or in providing service notifications. In these cases, an elevated access request must be reviewed and approved.

4. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

When an agency shares address book / directory information with Microsoft, that agency makes this decision to support Office 365’s provided functionality.

5. Does Microsoft currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

PII stored at Microsoft is supplied/populated by the agency and supports Office 365 functionality.

6. Will any third-party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

Third-party sources are not providing agency PII to the system.

3.4 ACCESS TO PII AND SHARING

7. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

Microsoft only allows access to 3rd party suppliers who have enrolled in the Microsoft Supplier Security and Privacy Assurance (SSPA) Program with proper compliance status and have signed additional Online Customer Data (OCD) protection agenda. These suppliers must be listed on the Microsoft Online Service Subprocessor list on Microsoft Trust Center six-month prior to accessing the data.

8. What Microsoft personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for Microsoft personnel to have access to the PII. (AR-8, UL-2)

Microsoft controls access to customer data, including PII. For exact details on roles and how access is granted to customer data, please review the AC, IA, and PS controls in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

For exact details on how Microsoft monitors access to customer data, please review the AU controls in the SSPs. Microsoft recommends focusing on these controls:

- *AC-2 Access Management*
- *AC-3 Access Enforcement*
- *IA-2 Identification and Authentication (Organizational Users)*
- *PS-2 Position Categorization*
- *PS-3 Personnel Screening*

- *AU-2 Auditable Events*

9. For CSP support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

Microsoft controls access to customer data, including PII. For exact details on how access is granted to customer data, please review the AC and AT controls in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

Microsoft recommends focusing on these controls:

- *AC-5 Separation of Duties*
- *AC-6 Least Privilege*
- *AT-2 Security Awareness*
- *AT-3 Security Training*

10. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

This is customer controlled. If the customer selects any of the optional services in section 3.1 above, Microsoft shares data with the selected services.

3.5 PII SAFEGUARDS AND LIABILITIES

11. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

At Microsoft, no one has standing access to Customer Data and PII. Personnel who have access to PII for support or providing services are screened, trained, and monitored. For exact details on how access is granted to customer data, please review the PS, PL, AT, and AU in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

Microsoft recommends focusing on these controls:

- *PS-3 Personnel Screening*
- *PL-4 Rules of Behavior*

- *AT-3 Security Training*
- *AU-2 Auditable Events*

12. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

The System Owner is responsible for the implementation of the policies and procedures. Policies and procedures designed to protect the privacy of PII are defined in the following sections:

- *PS-1 Personnel Security Policy and Procedures*
- *AT-1 Security Awareness and Training Policy and Procedures*
- *AU-1 Audit and Accountability Policy and Procedures*

13. Does the Microsoft provide annual security training include privacy training? Does Microsoft require their contractors that have access to the PII to take the training? (AR-5)

Microsoft's ongoing training commitments are explained in the AT controls in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

Microsoft recommends focusing on these controls:

- *AT-2 Security Awareness*
- *AT-3 Security Training*

14. Who is privacy officer responsible for assuring safeguards for the PII? (AR-1)

Microsoft administers Office 365 to provide those access controls explained in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

The System Owner is responsible for the overall controls provided for PII.

15. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

Microsoft provides a cloud service consistent with the FIPS 199 High rating. Potential damage to the agency and its ' personnel should not exceed the criteria established by the government in its ' FIPS 199 High classification.

16. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

All Office 365 contingent staff must sign a non-disclosure agreement at the time of engagement and before being given access to Office 365. In addition, any contractors and contingent staff involved in the design or maintenance of Office 365 are subjected to the Microsoft Supplier Security and Privacy Assurance (SSPA) Program, as wells as additional Online Customer Data (OCD) protection addenda, as explained in the SA family of controls in the following SSPs:

- *Office 365 - MT*
- *Office 365 - GCC High*
- *Office 365 - DoD*

17. Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)

Microsoft does not share PII with federal agencies except as the customer directs or as required by law, which has been described in [Microsoft Online Services Data Protection Addendum](#).

3.6 CONTRACTS, AGREEMENTS, AND OWNERSHIP

18. NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this accountability described in contracts with customers? Why or why not? (AR-3)

Yes, it is described in [Microsoft Online Services Data Protection Addendum](#) that customers sign with Microsoft.

19. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

Agencies retain ownership of their data when it is stored in Office 365, as described in the [Microsoft Online Services Data Protection Addendum](#).

20. Do contracts with customers require that customers notify Microsoft if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

Agencies are not required to notify Microsoft if they intend to populate Office 365 with PII. Microsoft assumes that customers will populate address book / directory data into Office 365 as a standard part of business. Any other use of Office 365 for the transmission, storage, or processing of PII is subject to Agency-specific Rules of Behavior. Agencies should not populate data above a FIPS 199 High rating into Office 365.

21. Do Microsoft contracts with customers establish record retention responsibilities for both the customer and Microsoft? (AR-2, AR-3)

Office 365's data retention standard is explained in [Microsoft Online Service Terms](#) and [Microsoft Online Services Data Protection Addendum](#) that customers sign with Microsoft, which shows the data retention standard as:

Data Retention and Deletion

At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section.

22. Is the degree to which Microsoft will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

Liability for the CSP is clearly defined in the [Microsoft Online Services Data Protection Addendum](#).

3.7 ACCURACY OF THE PII AND REDRESS

23. Is the PII collected verified for accuracy? Why or why not? (DI-1)

Agencies are responsible for the accuracy and currency of any PII that they provide while using Office 365.

24. Is the PII current? How is this determined? (DI-1)

Agencies are responsible for the accuracy and currency of any PII that they provide while using Office 365.

25. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

Yes, agencies are responsible for the accuracy of any PII that they provide while using Office 365. Agencies can make corrections through various capabilities provided to tenant administrators with Office 365.

3.8 MAINTENANCE AND ADMINISTRATIVE CONTROLS

26. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

Office 365 is operated from geographically diverse locations. Common controls are used across these sites and are explained in the System Security Plan.

27. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)

See Question 21 above for an explanation of data retention in Office 365.

28. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

Any of the customer's PII within Office 365 is overwritten at the end of the retention period. Information disposal is inherited by Azure, which has a FedRAMP IaaS P-ATO.

29. Is the system using new technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

Microsoft recommends that agencies use Active Directory Federation Services (ADFS) when connecting to Office 365. This provides each agency with the ability to set password complexity and multi-factor authentication sequences that are unique to that specific agency. This also ensures that any PII associated with the agency's users (e.g. biometrics in multi-factor authentication) are retained within that agency.

30. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

Office 365 moves functions (e.g. electronic mail and collaboration) traditionally housed within an agency into a CSP offering. Microsoft does not expect privacy impacts other than those defined previously in this document.

31. Is access to the PII being monitored, tracked, or recorded? (AR-4)

Each service team within Office 365 is required to maintain specific standards about the logging of access to customer data, including PII. See control AU-2d in the System Security Plan for more detail.

32. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

There is no System Of Records Notice (SORN) for Office 365 .

3.9 BUSINESS PROCESSES AND TECHNOLOGY

33. Have the talking points found herein resulted in circumstances that requires changes to business processes?

Microsoft expects agencies to educate their users on acceptable Rules of Behavior (PL-4) as part of the agency's ongoing training program (AT-2, AT-3) and to only store content at a FIPS 199 High, Moderate, or Low level as applicable.

This PIA has not resulted in business process changes at Microsoft as the system was implemented to provide a FIPS 199 High level.

34. Does the outcome of these talking points require that technology or operational changes be made to the system?

This PIA has not resulted in technology changes at Microsoft, as the system was implemented to provide a FIPS 199 High level.

3.10 PRIVACY POLICY

35. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

Yes. See the Microsoft Privacy Statement and supporting material on the Microsoft Office 365 Trust Center. The Microsoft Privacy Statement is provided as an answer to question 36 below. The Microsoft Office 365 Trust Center is located here:

<https://www.microsoft.com/en-us/trustcenter/>

36. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

Yes. <http://go.microsoft.com/fwlink/?LinkId=512132>

3.11 SIGNATURES

The information found herein has been documented by *Microsoft* and has been reviewed by the Office 365 Chief Privacy Officer for accuracy.

 Recoverable Signature

X 

Xiting Phillips
Principal Privacy Manager
Signed by: Xiting Phillips

 Recoverable Signature

X 

Greg Roberts
Chief Privacy Officer
Signed by: Greg Roberts

4 ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](#) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.