

Privacy Impact Assessment MS O365 Multi-Tenant

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: March 10, 2022
- Prepared for: USDA OCIO-Privacy Office





Privacy Impact Assessment for the Microsoft - Office 365 Multi-Tenant & Supporting Services

March 10, 2022

Contact Point

**Phil Rendina
Director, OCIO-CEC-IOD
(816) 926-6948**

Reviewing Official

**Nancy Herbert
OCIO-CEC-GSD-SCSB, ISSPM
United States Department of Agriculture
(816) 926-6948**

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

MS-O365MT is a multi-tenant cloud computing-based subscription service offering from Microsoft that provides CEC customers with cloud versions of Exchange Online (EXO) for email service, SharePoint Online (SPO) for creating sites to share documents and information (including Project Online, Visio Online, and OneDrive for Business), and Lync Online (Lync) that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

Hosted on Azure's PaaS product, which has a FedRAMP P-ATO (Provisional approval). In this case, the service is run on Azure virtual machines. O365 MT is responsible for the child OS protections; Azure is responsible for parent OS protections. Network layer protections are implemented by Azure and are managed in coordination with Azure. For details on Azure's network, parent OS, and physical security refer to the Azure SSP.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Name, Address, E-mail address, Photographic images, Protected Health Information

1.2 What are the sources of the information in the system?

“MS O365 MT will be providing Exchange and SharePoint Access for its customers, which may include PII. Records may be obtained from USDA personnel, interns, contractors, and cooperators who may provide relevant information on a suspected or confirmed disease or illness, or the prevention of such disease or illness, which is the subject of a declared public health emergency. Information may also be sourced from personnel at medical facilities, or from existing systems of records. Individual Customer Agencies using Exchange and SharePoint are the data owners and responsible to follow USDA Privacy guidance.”

1.3 Why is the information being collected, used, disseminated, or maintained?

To provide full featured e-mail capabilities. PHI is being collected to capture records necessary and relevant to Department activities responding to and mitigating COVID-19, other high consequence public health threats, or diseases and illnesses relating to a public health emergency.

1.4 How is the information collected?

Information about the system users comes from the individuals or from internal USDA systems. The information in the content of the email or in documents and records contained within the collaboration portals/repositories may come from a variety of sources, including individuals or entities outside of USDA who correspond using email or provide information to any of the USDA program offices in the normal course of business.

1.5 How will the information be checked for accuracy?

USDA has a high degree of confidence in the accuracy of the user information because USDA receives the information directly from the employees or contractors. In most

cases, employees have direct control over their information and may edit it to maintain its accuracy at any time. Other information contained in the various components of Office 365 may be checked for accuracy outside of the system or presumed accurate based on its source. The individual user within the system will need to determine accuracy based on business knowledge and need. Moreover, the collaborative nature of Office 365 provides opportunities for those working together on a document, for example, to make changes to address any inaccuracies concurrently

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Collection of information by USDA personnel will be governed by the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to OMB Circular No. A-130 and NIST SP-800-30, Risk Management Guide for Information Technology Systems. With regards to the PHI identified in Section 1.1, there are several employment laws that govern the collection, dissemination, and retention of employee medical information. These employment laws include the Americans with Disability Act (ADA), the Rehabilitation Act of 1973 (Rehab Act), and the Occupational Safety and Health Act of 1970 (OSH Act). Generally, under federal employment laws, medical information pertaining to employees is confidential and may be obtained by an employer only for certain reasons and only at certain points in the employment relationship

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that the information in the system may not be accurate. This risk cannot be fully mitigated by Office 365 and is primarily dependent on end users in the program offices who have responsibility for their content. The collaborative nature of the system and its applications naturally provides a platform where those collaborating on a project can address any inaccuracies. With respect to user information, the risk of inaccuracy is mitigated primarily via controls that may limit or guide how the user technically enters the information. In addition, employees are routinely reminded to update information about themselves in the Global Address Book within the Outlook program

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Information collected by the MS O365 MT – Cloud Services system will be used solely for the purposes of providing services for USDA. The information collected will be used to populate Enterprise Active Directory (EAD) to name and identify all users of the system. This is done to provide audit and accountability functionality to the USDA and to provide general user management. “MS O365 will be providing Exchange and SharePoint Access for its customers, which may include PII.

The PHI will be used for Department activities responding to and mitigating COVID-19 and other high-consequence public health threats, and diseases or illnesses relating to a public health emergency

2.2 What types of tools are used to analyze data and what type of data may be produced?

No tools will be used to analyze the privacy data collected by the system; the data will only be used to manage the service. See Table above in Section 1.1, ‘Safeguards’ column. “MS O365 MT will be providing Exchange and SharePoint Access for its customers which may include PII. Individual Customer Agencies using Exchange and SharePoint are the data owners and responsible to safeguard their data.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

No commercial or publicly available data will be used unless the USDA makes this same information public on their own accord. It will not be provided publicly unless authorized by the USDA.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access controls are in place to protect the information system and its components. All systems will be segmented from the public and secured or hardened following Microsoft and NIST SP 800-53, Revision 4 guidance. See Table above in Section 1.1, ‘Safeguards’ column.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Generally, information will be maintained as long as users are actively using the system. Retentions are set for seven years. Data is deleted automatically after seven years if not already done by the data owner.

Microsoft's data retention standards are explained in the Office 365 Trust Center (<http://www.microsoft.com/en-gb/office365/trust-center.aspx>). costs. If you Depending on the nature and type of record within the components of Office 365, various NARA-approved records schedules will apply. In particular, email records and the persistent chat records are governed by GRS 6.1 Capstone E-mail Retention.

General Records Schedule (GRS) 2.7, Items 010, 070 or 080, and NARA records retention schedules DAA– GRS2017–0010–0001, DAA–GRS2017–0010–0012, and DAA–GRS2017–0010–0013, to the extent applicable.

PHI will be maintained in accordance with NARA General Records Schedule (GRS) 2.7, Items 010, 070 or 080, and NARA records retention schedules DAA– GRS2017–0010–0001, DAA–GRS2017–0010–0012, and DAA–GRS2017–0010–0013, to the extent applicable.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Per USDA, this system does not qualify as an electronic records keeping system. Records will be maintained in accordance with guidance defined by the Client (US Government Agency that contracts for the use of the system). Agencies are not required to notify Microsoft if they intend to populate Office 365 with PII. Microsoft assumes that customers will populate address book 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 Moderate rating into Office 365.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.



There is a risk that the information in Office 365 may be accessed by unauthorized users or by authorized users for an unauthorized purpose.

This risk is mitigated by requiring all users to have an USDA system account and PIV card. Prior to receiving access to USDA network, all users must agree to the USDA Rules of Behavior, which includes the consent to monitoring and restrictions on data usage. The systems are monitored for misuse and unauthorized activity and access can be removed at any time by the system administrator.

This risk is also mitigated by providing training and guidance to end users who are the subject matter experts regarding, e.g., access controls within their purview to provide information and invitations to collaborative meetings only to those who have a need-to-know.

In addition, USDA uses a combination of technical and operational controls to reduce risk in the Office 365 environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, Office 365 undergoes regular reviews of its security controls

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

All USDA Agencies.

4.2 How is the information transmitted or disclosed?

At this time USDA MS O365MT is not federated with anyone else. If information contained in Office 365 is shared outside of USDA it is consistent with applicable laws and policy.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Policies and procedures designed to protect the privacy of PII are defined in sections PS-1, AT-1, and AU-1 in the SSP. The System Owner is responsible for the implementation of the policies and procedures. The same moderate impact NIST 800-53, Revision 4 security controls will be used for all components that hold data within the CEC accreditation boundary.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Microsoft personnel are prohibited from viewing customer data and PII in any service component except as required to support the service, or in providing service notifications.

When an agency shares address book information with Microsoft, that agency makes this decision to support e-mail functionality.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

While OCIO-CEC has no System of Records, many of the client organizations that OCIO-CEC support have business functions that require a System of Records. Mere maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to trigger the conduct of a privacy impact assessment (PIA). To trigger the SORN requirements of the Privacy Act, information must actually be retrieved by a personal identifier.

The information that is shared ,MS O365 MT – Cloud Services is compatible with the intent of the original collection — to create/maintain user accounts, in accordance with the contractual Statement of Work. Use an Interconnection Security Agreements (ISA) to share data between interconnected systems. Refer to the processes and procedures defined in NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, or its replacement.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The connection from MS O365 MT – Cloud Services for archiving is encrypted and the moderate impact NIST 800-53, security controls are implemented and documented within each System Security Plan (SSP). Microsoft personnel are prohibited from viewing customer data and PII in any service component except as required to support the service, or in providing service notifications.

Regarding the PHI, all or a portion of the records or information collected may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances

or for the purposes described in the associated SORN.

When an agency shares address book information with Microsoft, that agency makes this decision to support e-mail functionality.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

By having data transmitted to and stored at an additional facility the risk is increased, however the use of encryption decreases the potential compromise of data. This risk may be further reduced by limiting the private information that gets stored and using file level encryption for sensitive data. Microsoft personnel are prohibited from viewing customer data and PII in any service component except as required to support the service, or in providing service notifications.

When an agency shares address book information with Microsoft, that agency makes this decision to support e-mail functionality.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

USDA/OSEC-01<https://www.usda.gov/home/privacy-policy/privacy-impact-assessments>

6.2 Was notice provided to the individual prior to collection of information?

The exact mechanism may be slightly different for each government client. Typically the agency employee, contractor, or stakeholder does not have the opportunity to decline to provide non-PII information. The information requested is required to assign and set up the user accounts. The user has the right to correct or update information at any time by sending an email request to the agency help desk.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

USDA users and others whose information may be contained in Office 365 generally do not have an opportunity to consent to the inclusion of their information in the system. USDA users cannot decline to provide their information to access Office 365. Individuals who are not USDA users but whose information is contained in the system may have opportunities at the point their information is collected to decline to provide it but once provided cannot decline for it to be included in Office 365. For example, those who participate in Teams meetings receive notice if a meeting is going to be recorded and can opt to leave the meeting or turn off their camera and microphone.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

.USDA users and others whose information may be contained in Office 365 generally do not have an opportunity to consent to the inclusion of their information in the system. USDA users cannot decline to provide their information to access Office 365. Individuals who are not USDA users but whose information is contained in the system may have opportunities at the point their information is collected to decline to provide it but once provided cannot decline for it to be included in Office 365. For example, those who participate in Teams meetings receive notice if a meeting is going to be recorded and can opt to leave the meeting or turn off their camera and microphone.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

For the PHI, Individuals may be notified if a record in this system of records pertains to them when the individuals request in writing and address such request to the USDA Departmental FOIA Office, ATTN: Departmental FOIA Officer, 1400 Independence Avenue, SW South Building, Room 4104, Washington, DC 20250-0706, Email: USDAFOIA@ocio.usda.gov

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Users have access in the various Office 365 systems to their information. For example, Exchange Online user data can be accessed via Outlook. Others whose information may be contained in an Office 365 application may access their information as appropriate by following the instructions in any applicable system of records notice.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Active Directory is an enterprise administrative tool; certain USDA user information hosted in Active Directory is read-only to the individual; a user has access to view the data but can only request appropriate changes and removal by contacting system owners and operators.

The Global Address Book is an aspect of Microsoft Outlook; an individual USDA user is encouraged to review their entries in the Global Address List (GAL) to make sure the information is up to date and correct. They can update certain information on USDA's Intranet site or by contacting the USDA Helpdesk to have this information corrected on the GAL.

To remove an employee from the GAL, requests must be submitted through the Help Desk. Others whose information is in the system can access and request amendment to their information as appropriate by following the instructions in any applicable system of records notice.

7.3 How are individuals notified of the procedures for correcting their information?

USDA's Office 365 implementation is not accessible to anyone outside of USDA and, therefore, does not provide notice directly to those individuals who are not USDA users whose information it contains. USDA users receive notice in the form of training, instructions, Rules of Behavior, and the USDA Warning Banner prior to accessing. More generally, all individuals receive notice about accessing and amending their records via this PIA and any applicable SORNs.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The user has the right to correct or update information at any time. Customers are responsible for the accuracy and currency of any PII that they provide.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There are no additional privacy risks associated with the redress.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Access to the system by Microsoft personnel will be limited to administrative personnel in support of the service. The MS O365 Multi-Tenant System – Cloud Services Access Control are provided by CEC-Enterprise Active Directory (EAD).

8.2 Will Department contractors have access to the system?

Yes. Personnel that have access to the system services will be established and controlled by the USDA. --- Images would be accessible to contractors whom are vetted and working on behalf of USDA

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

OCIO CEC provides security and awareness training to personnel managing the *MS O365 Multi-Tenant System*

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Attempting

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Office 365 audit logs are captured by USDA’s auditing tools and retained in the tools archive. The Office of the Chief Information Security Officer reviews for suspicious or unusual activity and suspected violations, and as necessary appropriate action is taken.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The information collected to support the use of the service is general information on users. The moderate impact NIST 800-53, Revision 4 security controls have been implemented on the system to protect the data within the CEC MS O365 Multi-Tenant Cloud Services accreditation boundary.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

MS-O365MT is a multi-tenant cloud computing-based subscription service offering from Microsoft that provides CEC customers with cloud versions of Exchange Online (EXO) for email service, SharePoint Online (SPO) for creating sites to share documents and information (including Project Online, Visio Online, and OneDrive for Business), and Lync Online (Lync) that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Microsoft provides a cloud service and does not present any unusual privacy issues.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23

“Guidance for Agency Use of Third-Party Websites and Applications”?

Yes

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security Plan (SSP).

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security Plan (SSP).

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security Plan (SSP).

10.5 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security Plan (SSP).

10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security

Plan (SSP).

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Third party sources are not providing agency PII to the system. Microsoft 0365 limits 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 Office 365 System Security Plan (SSP).

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Internally

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No

10.10 Does the system use web measurement and customization technology?

Yes, the system does use web measurement or customization technologies. Third party sources are not providing agency PII to the system.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

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 between tenant organizations unless required to support law enforcement.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites



and/or applications, discuss the privacy risks identified and how they were mitigated.

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

Responsible Officials

Phil Rendina
Director, OCIO-CEC-IOD
United States Department of Agriculture

Approval Signature

Nancy Herbert
ISSPM
OCIO-CEC-GSD-SCSB
United States Department of Agriculture