Office of Government Ethics

Microsoft 365
Privacy Impact Assessment

December 2024
Information Technology Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for Microsoft 365

Provide electronic copies of the signed PIA to OGE's Chief Information & Cybersecurity Officer and Privacy Officer.

Name of Project/System: Microsoft 365 (M365)
Office: Information Technology Division

I. EXECUTIVE SUMMARY

The Office of Government Ethics (OGE), Information Technology Division (ITD) is deploying Microsoft 365, a cloud-based Software as a Service (SaaS) solution, in order to stand up and deploy a communications and collaboration suite of applications for OGE in the cloud. M365 provides a robust and standardized enterprise-wide suite of collaboration, communication, and office productivity tools for OGE employees and contractors that will also allow OGE to manage, access, and protect information, and provide scalability.

M365 is used by all OGE employees, contractors and program offices for collaboration. Within their collaborative workspaces, OGE employees can use the tools of M365 to produce deliverables, which may include Word documents, spreadsheets, presentations, dashboards, and other products, and collaborate with others via video conferencing, telephone and shared documents. Content access is controlled by approved role-based groups. Only OGE employees and authorized contractors may have system user accounts or access to OGE collaboration accounts.

Users access Office 365 via a Uniform Resource Locator (URL), or web address. In accordance with recommended best practices, OGE's Office 365 uses Active Directory Federation Services (ADFS) to connect users. The site interfaces with OGE's Active Directory to ensure that only personal identity verification (PIV) authenticated users can access the applications. This also provides a Single Sign On (SSO) capability for the OGE user community. This suite of tools enhances OGE's ability to store, archive, and retain discoverable data in place across the Office 365 platform. Additionally, ITD staff and other appropriate offices, to include the OGE Privacy Team, will be able to monitor and investigate actions taken on data, identify risks, and contain and respond to threats.

M365 is a subscription-based service which provides access to numerous Microsoft services and software. This Privacy Impact Assessment (PIA) evaluates the privacy implications of the M365/Teams applications listed below. This PIA will be updated to address privacy risks as other service products are implemented.

A. Outlook

Outlook is a hosted messaging solution that delivers the capabilities of Microsoft Exchange Server as a cloud-based service. The solution provides users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. Exchange Online integrates fully

with Active Directory, enabling administrators to use group policies, as well as other administrative tools, to manage Outlook features across the environment.

B. Office Desktop Applications

M365 provides the latest version of the Office desktop applications that OGE personnel are familiar with, such as Word, Excel, Planner, List and PowerPoint. The M365 desktop applications are installed on individual Virtual Machines (VMs) and may also be accessible via the web in emergency situations when the OGE network (OGEN) is down and VMs are inaccessible.

C. Microsoft Teams

Microsoft Teams is a persistent collaboration platform that enables document sharing, document revision tracking, online meetings, and other useful features for business communications. Authorized OGE business communications include: online audio and video calling; video conferencing with screen and file sharing; and document sharing. Teams enables OGE employees to communicate and collaborate with colleagues via Teams Channels (standard and private). In Team Channels, OGE employees may share and store artifacts that they generate; access multiple collaboration tools, such as Outlook and Calendar; and participate in meetings, accessing collaboration tools and content as needed. OGE is not opening Teams to guest users. Only authenticated OGE users can participate in Teams Channel activities. However, non-OGE employees may participate in Teams meetings (video and audio), and will be captured on meeting chats. OGE does not authorize the recording of meetings, with very limited exceptions for authorized programs.

D. OneDrive

OneDrive is a document, file and synchronization service, and serves as OGE's integrated storage, backup, and collaboration tool. With OneDrive, OGE employees can control how they store, share and update their files, choosing between the following options as needed:

- Storing and accessing some files only on their virtual machine (VM);
- Maintaining some files only on the cloud to share files for real-time collaboration with colleagues; and
- Backing up files, stored on one's VM, to the cloud and synchronizing them, so that changes can be retained in both places and allowing for download for personnel to work offline should they not have internet access available.

OneDrive also provides the capability for OGE employees to create files directly in the cloud, using the standard suite of Office applications such as Word, Excel, and PowerPoint.

E. Microsoft Purview

Microsoft Purview provides eDiscovery solutions. It can be used to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Viva Engage teams. It allows users to create eDiscovery cases to identify, hold, and

export content found in mailboxes and sites. With the Premium E5 license that OGE holds, users can also manage custodians and analyze content.

F. M365 for the Web

M365 for the Web provides web-based access to OGE employees for most of the same communication and collaboration tools and services that are available through VMs on the OGE Network.

II. CONTACT INFORMATION:

A. Who is the person completing this document?

Diana J. Veilleux
Senior Agency Official for Privacy
Chief, Legal, External Affairs and Performance Branch
Program Counsel Division
Diana.veilleux@oge.gov
202-482-9211

B. Who is the system owner?

Tony Upson
Deputy Chief Information Officer for Network Operations
Information Technology Division
tupson@oge.gov
(202) 482-9272

C. Who is the system manager?

Zachary Schnur
IT Specialist (Network)
Information Technology Division
zschnur@oge.gov
(202) 482-9258

D. Who is the Chief Information Security Officer (CISO) who reviewed this document?

Ty Cooper
Chief Information & Cybersecurity Officer
jtcooper@oge.gov
(202) 482-9226

E. Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy

Chief, Legal, External Affairs and Performance Branch
Diana.veilleux@oge.gov
202-482-9203

F. Who is the Reviewing Official?

Ty Cooper
Chief Information & Cybersecurity Officer
jtcooper@oge.gov
202-482-9226

III. SYSTEM APPLICATION/GENERAL INFORMATION:

A. Does this system contain any information about individuals?

Yes. M365 potentially collects, maintains, uses, or disseminates a wide variety of information about individuals, including: names and contact information of OGE users and other individuals who communicate with OGE users via M365; email messages (including any attachments) which may contain a variety of information, to include PII about OGE employees, other Federal employees, and members of the public; message log information (including IP address of sender, date, and time); and information stored in collaboration portals/repositories (such as spreadsheets, word processing documents, and PowerPoint documents), which may contain a variety of information, to include PII about OGE employees, other Federal employees, and members of the public. The system also maintains logs of OGE user activity.

1. **Is this information identifiable to the individual?**

   Potentially, based upon the contents of a particular M365 service being used.

2. **Is the information about individual members of the public?**

   Potentially, based upon the contents of a particular M365 service being used.

3. **c. Is the information about employees?**

   Potentially, based upon the particular M365 service being used.

B. What is the purpose of the system/application?

M365 is a Software-as-a-Service (SaaS) product from Microsoft that includes Microsoft's Office Productivity Suite as well as communications and collaboration services. M365 allows OGE to simplify administration of licenses and subscriptions to services at an enterprise level and facilitate system-wide user management, password administration, and oversight of security and privacy controls. M365 provides communication and office productivity tools for OGE employees and contractors, and will allow OGE to manage, access, and protect information, and provide scalability.

C. What legal authority authorizes the purchase or development of this system/application?

5 U.S.C. section 13122.

IV. DATA in the SYSTEM:

A. What categories of individuals are covered in the system?

Potentially, OGE employees, other federal employees, and members of the public, depending on the particular M365 application or service being used.

B. What are the sources of the information in the system?

Information is collected and stored in M365 when an account is created and when the account is used to create documents using MS Office applications, and to send and receive email, Teams standard and private channel conversations and posts, files, calendars, meetings, tasks, and audit log information. The information collected includes the contents of email messages, attachments, Teams conversations and messages, Office files, and metadata such as the email address and message log information (such as internet protocol (IP) address, date of message, and time of message).

C. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

See above.

D. What federal agencies provide data for use in the system?

Not applicable.

E. What State and local agencies are providing data for use in the system?

Not applicable.

F. From what other third party sources will data be collected?

See above.

G. What information will be collected from the employee and the public?

See above. Due to the nature of M365, many types of PII could be potentially be collected, used, maintained and/or disseminated using M365.

H. Accuracy, Timeliness, Reliability, and Completeness

1. How will data collected from sources other than OGE records be verified for accuracy?

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 M365 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 M365 provides opportunities for those working together on a document, for example, to make changes to address any inaccuracies concurrently.

2. How will data be checked for completeness?

M365 is primarily dependent on OGE 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.

3. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

M365 is primarily dependent on OGE 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 outdated content.

4. Are the data elements described in detail and documented?

No. See explanation above.

V. ATTRIBUTES OF THE DATA:

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

B. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

C. Will the new data be placed in the individual's record?

Not applicable.

D. Can the system make determinations about employees/the public that would not be possible without the new data?

No.

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?

Not applicable.

G. If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Not applicable.

H. How will the data be retrieved? Does a personal identifier retrieve the data?

OGE end-users can use the search feature in Outlook, Purview, and Teams to retrieve information by OGE end-user name and can retrieve other information (such as information contained in email messages and instant messenger/IMs) by name or other identifiers using a full-text search capability. System administrators can retrieve OGE end-user account information and audit log information by end-user name or other end-user identifiers.

I. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

No reports are produced.

J. What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?

The opportunity to consent depends on how the information is collected. OGE generally does not use M365 as a main tool to collect information, including PII, directly from the public. However, OGE staff and contractors use M365 for business operations in furtherance of OGE's mission. To the extent information maintained in M365 applications incidentally includes PII, individuals will not have an opportunity to consent. To the extent that consent is required for the underlying collection, however, the OGE will obtain any consent necessary. If the information is collected through email, the individual has an opportunity to consent to a particular use in their email response.

Information in M365 pertaining to OGE staff is collected to authenticate end-users and manage administrative business functions, including personnel security, human resources, emergency notifications, etc. All OGE staff are required to have a M365 account. Staff do not have an opportunity to consent to the use of the log information for the user accounts.

VI. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

A. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Not applicable.

B. Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

Information in M365 is maintained and/or destroyed in accordance with applicable OGE records disposition schedules and General Records Schedules (GRS) that are approved by the National Archives and Records Administration (NARA). OGE staff are informed of their recordkeeping responsibilities through training and meetings. Any information that is scheduled for disposal is destroyed in accordance with applicable records schedules, OMB, NARA, and NIST requirements.

C. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

OGE records in M356 are managed according to their content in accordance with NARA approved disposition authorities.

D. Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

E. How does the use of this technology affect public/employee privacy?

The impact on privacy depends on the particular M365 service being used. Depending on the content and how it is retrieved, information maintained in M365 may be covered by a number of OGE or government-wide System of Records Notices (SORNs). Links to all published OGE SORNs are available at www.oge.gov/privacy. Information maintained, discussed, or shared in Teams Channels or during web meetings generally will not contain PII apart from participants' names. If an OGE program needs to use those tools to maintain, discuss, or share additional PII, the program must first submit a Privacy Threshold Analysis (PTA) for the particular use and comply with any additional restrictions set forth in the approved PTA.

F. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

G. What kinds of information are collected as a function of the monitoring of individuals?

Not applicable.

H. What controls will be used to prevent unauthorized monitoring?

Not applicable.

I. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Records contained in the email content and attachments and within collaboration portals/repositories are subject to various OGE or governmentwide system of records notices. OGE internal and governmentwide SORNs are available at oge.gov/privacy.

J. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No.

VII. ACCESS TO DATA:

A. Who will have access to the data in the system?

All OGE employees and contractors have access to M365. User access to individual services/application is managed by OGE's ITD through the OGE Account Access Request Form (AARF) approval process, which authorizes ITD to create, modify and disable network account, including access to OGE applications. AARF requests must be signed by the employee/user, their supervisor and the CIO before a request is approved to be implemented by ITD. Only approved OGE users are allowed to use M365 applications and services.

When individuals are included in a Teams meeting or Channel, it is the responsibility of the OGE user who initiates the meeting or Channel to determine that both OGE and non-OGE individuals who are invited to participate have a need-to-know and that it is otherwise permissible to provide access to all meeting or Channel content, to include the subject under discussion as well as any shared documents. If the discussion or shared documents may contain PII and other sensitive or nonpublic information, the program must submit a PTA for that particular use and comply with any further restrictions set forth in the approved PTA.

B. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

See above. User access to data in M365 will be limited based on the information in a particular application and the user's need to know. For example, access to information in collaborative tools, such as Teams Channel, will be limited based on the topic of the Channel and the type of information shared, i.e. whether the information is public or contains sensitive information or PII, in which case a separate PTA is required.

C. Will users have access to all data on the system or will the user's access be restricted? Explain.

No. See above. User access to data in M365 is limited based on the information in a particular application and the user's need to know, and is subject to approval under the AARF process.

D. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Only approved OGE users are allowed to use M365 applications and services. Therefore, unauthorized users do not have access. In addition, authorized OGE users have been advised that the agency policy prohibits them from unauthorized browsing of data and they have been instructed not to engage in such activities.

E. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes. In addition, all contractors involved with the deployment of M365 as utilized by OGE sere required to sign appropriate Privacy Act and non-disclosure agreements.

F. Do other systems share data or have access to the data in the system? If yes, explain.

No.

G. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Not applicable.

H. Will other agencies share data or have access to the data in this system (Federal, State, or Local)?

No.

I. How will the data be used by the other agency?

Not applicable.

J. Who is responsible for assuring proper use of the data?

Each authorized user is responsible for assuring proper use of the data collected via applications in M365.

The Following Officials Have Approved the PIA for Office 365:

1) System Owner

Electronic Signature: LEONARD UPSON

Digitally signed by LEONARD UPSON
Date: 2024.12.18 21:50:43 -05'00'

Name: Tony Upson
Title: Deputy Chief Information Officer for Network Operations

2) Chief Information & Cybersecurity Officer

Electronic Signature: JAMES COOPER

Digitally signed by JAMES COOPER
Date: 2024.12.19 13:03:43 -05'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

3) Senior Agency Official for Privacy

Electronic Signature: DIANA VEILLEUX

Digitally signed by DIANA VEILLEUX
Date: 2024.12.19 12:55:29 -05'00'

Name: Diana Veilleux
Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Privacy