Affects Members Of the Public? Mark if Applicable w/ an X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	10/16/2024
Departmental Element & Site	Office of the Chief Information Officer (OCIO); Department of Energy (DOE) Headquarters - IM-60.
Name of Information System or IT Project	Microsoft 365 (M365)
Exhibit Project UID	019-000001955
New PIA ☐ **Update** X	This is an updated PIA to the signed copy dated 4/16/2024. Replaced Azure AD with Entra ID. Updated response to question 30.

	Name, Title	Contact Information Phone, Email
System Owner	Damon Bragg System Owner	301-903-0015 Damon.Bragg@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

	Infrastructure Operations Office (IM-61), OCIO U.S. Department of Energy	
Local Privacy Act Officer	Deputy Chief Privacy Officer and Director of Privacy Management and Compliance Office of the Chief Information Officer	privacy@hq.doe.gov
Cyber Security Expert reviewing this document (e.g.ISSM,CSSM,ISSO,etc)	Michael Okoro Information System Security Officer (ISSO) Security and Compliance Office, IM-63 U.S. Department of Energy	915-702-3696 Michael.Okoro@hq.doe.gov
Person Completing this Document	Gregory Huber Messaging Engineer, IM-61 U.S. Department of Energy	301-903-9925 Gregory.Huber@hq.doe.gov
Purpose of Information System or IT Project	Microsoft 365 is Software as a Service (SaaS) hosted by Microsoft that runs on a Windows Server cloud-based infrastructure and is part of the Microsoft Office line of products. DOE accesses M365 through Microsoft's Government Cloud Community Cloud (Gov Cloud) as a SaaS platform. SaaS provides system users with online versions of MS Office Suite (Office Web Apps) along with SharePoint Online, Exchange Online, OneDrive for Business, Teams, Office Online, Intune, Planner, Edge, Microsoft Bookings, Forms, Application Programming Interface, Azure Rights Management, Stream Entra ID, Entra ID Connect, Power Platform, Dynamics 365, To Do, Lists, Whiteboard, Planner, Delve and Visio and these services are considered Cloud Clients. M365 is hosted on Azure Infrastructure as a Service (IaaS) – Platform as a Service (PaaS), Azure implements network and network layer protections and servers are located in Azure Continental US (CONUS) data centers. The purpose of M365 is to ensure full functionality and ease of use of Microsoft 365 Cloud Clients, such as Exchange Online. M365 is a SaaS hosted by Microsoft, which runs on a Windows server cloud-based infrastructure and is part of the Microsoft Office line of products. **It is currently possible for PII type information to be stored in M365 in various applications including Exchange, Teams, SharePoint, OneDrive, OneNote, Power Platform, etc."**	

MODULE I – PRIVACY NEEDS ASSESSMENT

DOE has implemented the following M365 Cloud Services:

OneDrive for Business – Cloud based storage repository that facilitates creation, storage, sharing, and collaborative work for all types of electronic files which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information and other confidential information. The files in OneDrive for Business (ODfB) are private by default and can only be viewed by the file creator. Files may be made searchable by the file creator, and by system administrators for authorized purposes such as eDiscovery. However, the users can alter permissions for their files, and the file rights can be further delineated to view only, view and comment, or view, comment, and edit. ODfB allows staff to share information with business colleagues (internal and external to EITS) as needed and edit Office documents together in real time with Office Online. External sharing is limited by an allowed domains list which includes other DOE organizations and select .gov domains. It can also sync files to a local computer using the ODfB sync application. Due to the nature of ODfB, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents.

Office Online – Web browser version including Word, PowerPoint, Excel, and OneNote. Office Online opens Word, Excel, OneNote, and PowerPoint documents in a web browser, and makes it easier to work and share Office files from any location with an Internet connection, from almost any device, and provides M365 customers with the capability to view, create, and edit files.

Microsoft Exchange Online – Microsoft Exchange Online is a hosted messaging application that provides organizations with access to the full-featured version of Exchange Server. It includes access to e-mail, calendar, contacts, and tasks for endpoint devices.

SharePoint Online – It provides online collaborative sites that are visible to personnel within the EITS domain and can be used to share any information, some of which may contain personally identifiable information (PII), in the form of reports, contact information, and others. SharePoint Online can help staff share information, organize projects and teams, and discover people and information. Allows staff to share information with business colleagues (internal and external to EITS) as needed and edit Office documents together in real time with Office Online. External sharing is limited by an allowed domains list which includes other DOE organizations and select .gov domains.

MODULE I – PRIVACY NEEDS ASSESSMENT

	Microsoft Teams – It is a collaboration platform and provides instant messaging, audio and video calls, online meetings, availability (presence) information, and screen sharing capabilities within the Teams application. Teams allows staff to connect with co-workers, both inside and outside of EITS. External collaboration is limited by an allowed domains list which includes other DOE organizations and select .gov domains. and leverages multiple devices to reach stakeholders through an enterprise-grade, secure, Information Technology (IT) managed platform. Part of the implementation will include Enterprise Mobility + Security Suite (EMSS), a comprehensive solution designed to help manage and protect users, devices, apps, and Data. EMMS provides the following: **Entra ID**– Manages identity with hybrid integration to protect application access from identity attack. Entra ID is the management portal for identity and access control and Azure Information Protection for data protection. **Microsoft Intune** – Intune is the component of Enterprise Mobility + Security (EMS) that manages mobile devices and apps. **Microsoft Planner** – It is a planning application within M365 platform. The application is available to premium, business, and educational subscribers to M365. Planner enables users and teams to create plans, assemble and assign tasks, share files, communicate, and collaborate with other users, and receive progress updates via various means on the M365 platform. **Microsoft Bookings** - It is a web-based booking calendar that integrates with Outlook. The Bookings app in Teams lets schedulers handle their main tasks and change some settings. **Microsoft Stream** - Enterprise Video service where users can upload, view, and share videos securely. Also, a secure video service so you can manage who views your video content and determine how widely to share within your organization. Secure application access is enabled by Entra ID, a recognized leader in identity management systems, to protect sensitive corporate content. **Microsoft Forms** - A simple, lightweight app that lets you easily create quizzes, polls, and collect information. It is used to collect customer feedback, measure employee satisfaction, improve product/business, or organize events. **Application Programming Interface (API) -** It is a source code -based specification intended to be used as an interface by software components to

MODULE I – PRIVACY NEEDS ASSESSMENT

	communicate with each other. An API may include specifications for routines, data structure's, object classes, and variables. **To Do** - Microsoft To Do is a cloud-based task management application. It allows users to manage their tasks from a smartphone, tablet, and computer. **Lists** - Microsoft Lists, which is also known as Lists is a system designed to help a user track information and organize work in "simple, smart, and flexible" ways. This can include tracking company assets like laptops, tracking contracts, inventory (ex. office supplies), or a daily routine. Microsoft Lists is an interface upgrade to SharePoint lists, separated out into its own app. **Whiteboard** - Microsoft Whiteboard is an application for business and educational collaboration through the use of images, text, drawings, and hypertext links. Digital ink is written to the whiteboard through the use of a Surface Hub pen, touch screen, or mouse and keyboard. Changes to a board are viewed in real-time by invited participants. If enabled by the organization's administrator, whiteboards can be created and shared in Microsoft Teams, exported to OneNote, and saved to the Azure cloud. Delve - Office Delve allows M365 users to search and manage their emails, meetings, contacts, social networks, and documents stored on OneDrive or Sites in M365. Delve uses machine learning and artificial intelligence to try to show the most relevant people and content. Delve is based on Office Graph. **Visio -** Visio in Microsoft 365 allows customers to create, view, edit, and share diagrams either in Visio for the web or directly in Microsoft Teams.
Type of Information Collected or Maintained by the System:	Due to the nature of M365, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in M365. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose. ☐ Social Security Number (Possible)

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Medical & Health Information (Possible) ☐ Financial Information (Possible) ☐ Clearance Information (Possible) ☐ Biometric Information (Possible) ☐ Mother's Maiden Name (Possible, provided by user for security questions) ☐ DoB, Place of Birth (Possible, provided by user for security questions) ☒ Employment Information (Possible) ☐ Criminal History ☒ Name, Phone, Address (Possible) ☒ Other – All types of PII may be collected by M365. M365 contains username, work email address, work phone number, work address, title of DOE employee and contractor, and related organizational information required for system administration. MS Teams provides a contact service that allows users to maintain contact information, including phone numbers which may either be work related and/or personal contact information based on user provided information and email addresses pulled from AD/DOEInfo/Myidentity. This information is manually entered by the service user. Due to the nature of M365, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information and their documents. It is currently possible for PII type information to be stored in M365 in various applications including Exchange, Teams, SharePoint, OneDrive, OneNote, Power Platform, etc." . Information about individuals may include, but is not limited to names, email addresses, telephone numbers, SSNs, dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose.
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history*	YES

MODULE I – PRIVACY NEEDS ASSESSMENT

and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Manual Review

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	- Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. - Federal Information Security Modernization Act of 2014 - Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 27, 2011 - 44 U.S.C. Chapter 35, The Paperwork Reduction Act; - 40 U.S.C. 1401, the Clinger-Cohen Act; - 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; - Presidential Memorandum, "Systems in Cloud Computing Environments," December 8, 2011; - Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Users consent by logging on to the system. A limited amount of credentialing is pulled from Entra ID. All systems on the network display a warning banner as required by DOE O 205.1D, Department of Energy Cybersecurity Program (Pg 5), which directs that Enterprise Risk Management Implementation Plans " Must require DOE and NNSA NSS and Federal unclassified systems to display a system use notification (e.g., Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on "OK" or "I agree" button to proceed). The warning banner must cover the following in substance." The warning banner requires users to agree before proceeding.

MODULE II – PII SYSTEMS & PROJECTS

3. CONTRACTS **Are contractors involved with the design, development, and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Contractors are involved with the design, development, and maintenance of the system. M365 Suite is a Software as a Service (SaaS) offering. DOE does not maintain or administer the underlying infrastructure of the cloud provided service. The individuals provided this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Yes. Contract clauses require the contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE.

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed M365 Suite as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. M365 is a subscription service offering a shared pool of computing resources that may include a significant amount of PII. The level of risk associated with the type and sensitivity of PII is dependent on the office or program use and the safeguards implemented to mitigate the risk. Information accessible from MS Teams via business card pop-up functionality (native Microsoft feature across all Office applications) could include name, email address, work phone, work address, and title of employees, company name. The use of M365 allows some PII such as personal phone number, home phone number to be entered and stored in the system and may include other personal information such as the employee personal contact information. Due to the nature of M365, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in M365. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, SSNs, dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose. Microsoft 365 is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. M365 is rated as FISMA moderate based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Prior to granting privileged users access to the EITS M365 tenant, all users must agree and as well as acknowledging the DOE Warning Banner before accessing the system, which includes the consent to monitoring, and restrictions on data usage. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels. The contract

MODULE II – PII SYSTEMS & PROJECTS

	between EITS and M365 does not allow the service provider to review, audit, or transmit DOE data, which minimizes privacy risks from the vendor source. All EITS Microsoft 365 users must complete privacy, security and records management awareness training on an annual basis. EITS utilizes a combination of technical and operational controls to reduce risk in the M365 environment, such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies. All users must have a DOE account to access M365. Individuals and offices utilizing the M365 service are responsible for implementing adequate controls to safeguard PII used or maintained within their environment as appropriate. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the M365 environment, which will help EITS effectively maintain a good privacy and security posture for the M365 system. The M365 system security plan is reviewed annually to ensure adequacy of controls implemented to protect data. **Site and Data Owners** are responsible for the content which they upload or store to any M365 services. Controlled Unclassified Information (CUI) including PII is permitted on a moderate system. In the event of a breach of the DOE implementation of M365, there is a very low risk of unauthorized access to the documents uploaded or stored to the system duties to role-based controls that limit access to Cloud Client and to specific data in Cloud Client to certain users. Elevated privileges are restricted by separation of duties and least privilege. Privileged accounts require an enhanced validation process.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Data can be downloaded with proper permission via web browser. Yes, PII can be retrieved by an individual identifier. Information can be retrieved by Name, Location, Extension, and other personally identifiable information. **Data and site owners** would be responsible for this administration of their SORN.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	No
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	**Individual Site and Data Owners** are responsible for the individual information held in their instance of M365. Credentialing information may be obtained from DOEInfo or Myidentity. A limited amount of credentialing is pulled from Entra ID.
9. Will the information system derive new or meta data about an individual from the information collected?	Although the system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected, new data may be input into the system to support the mission of the M365 instance. Meta data associated with user credentials may be linked to a specific user to manage internal transactions, which is part of the structural design of the M365 Suite products.

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?	Detailed information about M365 is described and documented in the Microsoft support center at: https://support.office.com. In brief, these data elements for DOE employees consist of: Name: Name of the DOE employee composing and transmitting the email communication. Username: An identification used to access the DOE network. Work Email Address: Email address of the DOE employee composing and transmitting the email communication. Work Phone Number: Phone number of the DOE employee composing and transmitting the email communication. Department: The department in which the DOE employee reports. Office Location: The physical location of where the DOE employee reports. In brief, these data elements for non-DOE employees consist of the following forms of business contact information: Name: The name of the individual submitting and receiving an email to or from a DOE employee. Phone Number: Phone number of the individual submitting and receiving an email to or from a DOE employee. Email Address: The email address associated with the sender or recipient of an email communication with DOE.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	PII will be used to send and receive email, schedule calendar events as well as store and receive contact information on business partners. Information required for M365 is relevant to the purpose of the system. Data gathered within the MS Teams application are contact information and are used for the communication and collaboration among the DOE personnel to meet the mission of managing and operating DOE. Data stored within M365 is consistent with the purpose of the service to promote employee collaboration. PII is used to control access to the system-by-system administrators. M365 services such as MS Teams will allow users to view contact information to interact with each other within the collaborative environment. M365 is used to store documents for collaborative interaction between individuals. M365 provides a storage and collaborative environment for DOE employees' offices to interact with each other and the public. PII may be used for a variety of purposes within the M365 components at the local level by specific programs in support of a specific mission purpose. Due to the purpose of the system and the range of supported services, personal information may be present in these tools for a variety of reasons as part of the function of program office during communication, collaboration, and creation and management of records.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	Although the system does not derive new data or create previously unavailable data about an individual through aggregation from the information collected, new data may be input into the system to support the mission of the M365 instance. Meta data associated with user credentials may be linked to a user.
13. With what other agencies or entities will an individual's information be shared?	N/A
Reports	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports are generated for the administration of the system and may contain information about user accounts. Billing information may contain username and email – from Admin level for DOE financial billing and reporting. Reports are run for the site access. They can be generated about users and titles of documents. The site owner and data owner are responsible for these reports. Searches performed by general users could generate other users' names who authored documents returned by the search.
15. What will be the use of these reports?	For administration purposes the reports will be used for support of system content administration and security, such as incident response investigation. For general users search reports will be used for their job duties.
16. Who will have access to these reports?	Only authorized DOE federal and contractor personnel with elevated privileges will have access to these reports. Furthermore, only administrators whose role and function corresponds with the data contained in the report will be able to access said report. ROLES: • Global Administrator • Billing Administrator • Exchange Administrator • SharePoint Administrator • Password Administrator • MS Teams Administrator • Service Administrator • User Management Administrator • Power Platform Administrator Authorized access will be limited to **System and Site users** with a need to know.
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The use of the system is not designed to identify, locate and monitor individual employees or their activities. M365 provides audit capabilities on addition, modification, or deletion of data within the systems. The information is only available to administrative personnel. Administrator reviews of audit logs will also help prevent any unauthorized monitoring or user behaviors.
18. What kinds of information are collected as a function of the monitoring of individuals?	Individuals are not monitored.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Access is limited to authorized federal and contractor employees and is controlled by the system administrator. Site access is controlled by the site administrator. Privileged accounts and tenant accounts are heavily partitioned. Privileged accounts are Role Based. Continuous monitoring is utilized to ensure the ongoing security and privacy of the system and its contents. (using applicable NIST SP 800-53 controls).
DATA MANAGEMENT & MAINTENANCE	

MODULE II – PII SYSTEMS & PROJECTS	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	M365 contains a set of tools that promote communication and employee collaboration. Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of each user to ensure accuracy of data used in terms of their network profile, which is stored by Active Directory, to ensure continuous access to M365 through the EITS network. M365 is updated immediately upon a change in an employee's status, which will automatically update access to the system as only active and authorized employees will have access. When a user account is disabled or terminated, all access will be denied since the user will no longer have the ability to log onto or authenticate to the application. User contact information will be removed once the user account is deleted within the organization. M365 allows users to add individual contact information or have the user contact information be generated from an organizational directory or group. Within the organization, users have the ability to enter their own information and to ensure that it is current. M365 data owners are responsible for verifying and updating the information relevant to the service to which they subscribe. System administrators ensure completeness of user information for access control and authentication with the AD service and will not ensure data created or entered by end users to complete. M365 account request process does attempt to match the email address provided by the user in their application to the email address that is on file for that user.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The M365 Suite is a cloud-based product, software-as-a-service (SaaS) solution or cloud solution and is being implemented for the use of DOE EITS customers. The M365 system provides a single repository containing all system information and the rules, controls, and procedures that govern access to the system will be applied consistently, regardless from which site the system is accessed from.
Records Management	
22. Identify the record(s).	Records within M365 are directly linked to the **System and Site Owner** DOE missions. The Data and Site Owners are responsible for the data contained in their instance of M365. Therefore, these site records may be subject to applicable site records schedules.

MODULE II – PII SYSTEMS & PROJECTS

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □Unscheduled ■Scheduled *(cite NARA authority(ies) below)* Disposition of records: These records are temporary records. National Archives and Records Administration Records Schedule Number: DAA-0434-2018-0001 M365 and similar information technology service solutions may include, but may not be limited to, the employee/requester full name, contact phone number, business email, office of assignment, and office location. Disposition Instruction: TEMPORARY. Cut off in year the system is terminated, defunded, or decommissioned. Destroy three (3) years after cutoff, but longer retention is authorized for business use. Input • GRS 5.2 item 020 recommended, but IM-60 to review and verify applicability for use retention and disposition use. Output • GRS 5.2 item 020 recommended, but IM-60 to review and verify applicability for use retention and disposition use. Documentation • GRS 3.1 item 051 recommended, but IM-60 to review and verify applicability for use retention and disposition use.
24. Records Contact	Jared Bellman Office of the Chief Information Officer IT Service Management and Customer Advocacy Office (IM-64) U.S. Department of Energy 301-903-1713 jared.bellman@hq.doe.gov

ACCESS, SAFEGUARDS & SECURITY

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification, or use?	security and privacy controls are in place to prevent the misuse of data by individuals with access. These access controls are part of the M365 System Security Plan (SSP). All system team members (federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing and the Annual Privacy Training as a requirement for access to the system. Administrative controls include separation of duties, so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system. System administrators have limited access to information, including PII, contained on the site. Site administrators and users may upload information, containing PII, to the site. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. The technical controls include restricted access via unique user-id and password with access/functional privileges to M365 commensurate with the user's job responsibilities.
26. Who will have access to PII data?	DOE federal and contractor personnel will have access to data in the system. Authorized access will be limited to users with a need-to-know basis and separation of duties between system administrators who have limited access to PII and site administrators and users who may upload PII.
27. How is access to PII data determined?	Access to data is determined by evaluation of personnel job roles and responsibilities and organization. Based on the evaluation, the user is assigned permissions that are applied using system access control lists.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. M365 shares information with DOE Active Directory.
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	Where required, there are Memorandums of Understanding/Agreements (ISA/MOUs) between DOE EITS and other sites utilizing the EITS M365 instance.

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	EITS M365 System Owner, as identified in the System Security Plan. Site and Data Owners are responsible for the information contained in their instances of M365.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	Damon Bragg **(Print Name)** DAMON BRAGG Digitally signed by DAMON BRAGG Date: 2025.01.22 12:24:17 -05'00' **(Signature)**	
Local Privacy Act Officer	**(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2025.01.22 15:22:03 -05'00' **(Signature)**	
Chief Privacy Officer	**(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2025.01.21 14:17:28 -05'00' **(Signature)**	