☒ Mandatory
☐ Informational
☐ Best Practice
☐ Other

TECHNICAL ASSISTANCE

Date: May 9, 2023

Contact: policy@dwd.in.gov

Program: Indiana Department of Workforce Development (DWD)

Subject: DWD Technical Assistance 2022-13
DWD Microsoft TEAMS User Guidance on Safeguarding Protected Information

Purpose

DWD uses the Microsoft TEAMS application to securely communicate, collaborate, and share information. This technical assistance provides guidance for all DWD staff, vendors/contractors, and service providers on how to handle protected information in accordance with federal and state data security requirements when working within TEAMS.

This guidance is intended to supplement DWD Policy 2021-10, Change 1 *Safeguarding Protected Information and DWD User Accounts Management.*

References

DWD Policy 2021-10, Change 1 *Safeguarding Protected Information and DWD User Accounts Management*[1]

Definitions

TEAMS, spelled in all capital letters, refers to the Microsoft TEAMS application comprising multiple components/functions that include Team(s), Chat, and Calls through which users can communicate and collaborate. This application, including all components, functions, recordings, and files, is subject to this guidance, DWD Policy 2021-10 Change 1, and federal data security guidance.

- A **Team** is an enclosed environment in which defined members can securely collaborate, communicate, and store data. TEAMS enables real-time (like phone calls and meetings) and non-real-time (like posting messages) communication and collaboration between multiple users, and information sharing and storage via posting, screen sharing, files sharing, and audio/video meetings.

[1] Active DWD policies can be accessed at https://www.in.gov/dwd/compliance-policy/policy/active/.

- **Chat** enables real-time and non-real-time communication and collaboration between multiple users, and information sharing and storage via posting, screen sharing, file sharing and audio/video meetings.
- **Calls** enable real-time communication and collaboration between two users via audio/video meetings and screen sharing. Users shall be aware that the written communications and file sharing capabilities within Calls is completed through Chat.

A TEAMS **"User"** is required to adhere to the provisions of this policy and includes anyone that has been given access to participate in a Teams meeting, chat, or call.

A TEAMS **"Authorized User"** is a user that is required to adhere to the provisions of this policy, the Information Resources Use Agreement (IRUA), and has a legitimate business need to have access to protected information that has been authorized by DWD management.

Protected Information[2] - Includes the following:

- *Confidential Information* - Information that has been so designated by statute, promulgated rule, or regulation, based on statutory authority which does not permit public access to, or requires the protection, storage, disposal, and appropriate use of the information for official lawful purposes; and
- *Privileged Information* - Privileged information[3] is available only to authorized persons. Privileged information is not confidential pursuant to the law but is sensitive in nature and is subject to the same restrictions and requirements as confidential information for purposes of this guidance; and
- *Personally Identifiable Information (PII)* - PII is any information that can be used to distinguish or trace an individual's identity, either by itself or when combined with other PII, that is linked or is linkable to an individual.
    - *Sensitive or protected PII* includes any information that, if disclosed, could result in harm to the individual whose name or identity is linked to that information.
    - *Non-sensitive PII* is information that, if disclosed by itself, could not reasonably be expected to result in personal harm to the individual whose name or identity is linked to that information. However, depending on the circumstances, a combination of non-sensitive PII could potentially be categorized as sensitive PII.

NOTE: Confidential or privileged information, including sensitive and non-sensitive PII and non-public DWD operations information will be referred to as "protected information" throughout this guidance.

Content

IOT requires a request to be submitted through the State of Indiana WorkSmart 365 website to have a Team set up in the TEAMS application. Prior to completing the required form,[4] staff requesting a Team should complete the following:

---

[2] See DWD Policy 2021-10 Change 1 *Safeguarding Protected Information and DWD User Accounts Management* for additional guidance.

[3] Including non-public DWD operations information.

[4] The form can be accessed at https://ingov.sharepoint.com/sites/WorkSmart365/Lists/Office365GroupRequestForm/MyRequests.aspx.

- IRUA required training.[5]
- Recommended TEAMS training, *Get set up for calls and meetings.*[6]

It is the responsibility of **all** TEAMS users to safeguard protected information in accordance with this guidance, DWD Policy 2021-10, Change 1, and the IRUA when working within TEAMS.

User Type Details

TEAMS users fall into the following groups:

- DWD Staff users that are authorized to access Social Security Administration Unemployment Insurance Inquiry (UIQ) responses and Internal Revenue Service Federal Tax Information (FTI).
- DWD Staff users that are **not** authorized to access FTI/UIQ information but **are** authorized to access other types of protected information.
- External users include, but are not limited to, any vendor or contractor providing services to DWD, as well as any entity providing services to or through DWD, other state agencies, and the federal government. These users may or may not be authorized to access protected information.

NOTE: DWD staff that initiate a meeting (including chat and call) must be aware of the level of authorized access for the attendee(s) and the type of information that will be discussed/shared during the meeting to ensure information is being shared only with authorized users.

Sharing Protected Information within Teams

Depending on the type of user, certain kinds of protected information may be shared within Teams, Chat, or Calls. Some examples are listed below. However, the lists are **not** exhaustive, and DWD staff are to consult with their leadership prior to sharing information if they are unsure if the information is protected and/or if there are related sharing restrictions within TEAMS.

General Restrictions

- Under no circumstance should a full Social Security Number be shared in Teams or Chat.
- Under no circumstance should FTI be shared with Contractors or co-workers not authorized to handle FTI.

Authorized DWD Users/Other Authorized Users
The types of information listed below may only be shared with other authorized users. Additionally, the information may **only** be shared **verbally**[7] within Teams. DWD staff, contractors, vendors, and service providers are prohibited from recording calls during which information is discussed. Calls involving FTI or

[5] Visit https://www.in.gov/iot/security/information-resources-use-agreement/ for additional IRUA information and training.
[6] Training can be accessed at https://www.linkedin.com/learning/microsoft-teams-essential-training-5/get-set-up-for-calls-and-meetings?autoplay=true&u=2188380. **NOTE:** this is a LinkedIn Learning module and requires a license to access. All DWD Employees have a LinkedIn Learning account provided by DWD.
[7] If the captions are not saved or recorded, live captioning may be used in calls regarding protected information. Please reach out to PrivacyandSecurityOfficers@dwd.in.gov for additional guidance on authorized accessibility options for hearing-impaired individuals.

UIQ information may only involve participants that are authorized to access said information.[8]

- Account security questions/answers;
- Driver's license or ID Numbers;
    - Including personal details that are typically listed on those documents such as height, weight, eye color, hair color, and date of birth;
- UI investigation status;
- UI Last Known Employer information;
- IRS-derived 1099 FTI information - Only authorized DWD staff;
- IRS TOP information - Only authorized DWD staff;
- IRS TOP intercept amounts - Only authorized DWD staff;
- UIQ response information - Only authorized DWD staff; and
- OCSE information.
- UI Department of Corrections status;
- UI FSSA status; and
- UI FSSA intercept amounts.

Authorized DWD Users Only and Exceptions
The types of information listed below may only be shared internally. However, the information may be shared with authorized external users if they have a signed data sharing agreement on file with DWD or the data has been shared as part of an audit (For example: OIG-DOL).

- Unemployment Insurance (UI) claimant/employer/agent ID (Uplink party-ID);
- UI wages amounts;
- UI benefit payments amounts;
- UI benefit collection amounts;
- UI Tax collected amounts;
- UI claimant/employer address; and
- UI USDOL reporting.

NOTE: Based on the type of data being accessed for daily work tasks, some divisions may choose to utilize a guidance acknowledgement form as part of their internal security practices. Although it is not required, DWD has provided an example acknowledgement template[9] as a resource.

Security Breach

A security breach is the unauthorized disclosure of protected information that compromises the security, confidentiality, or integrity of that information. DWD TEAMS users who become aware of any security breach resulting from the inadvertent or intentional disclosure of any protected information shall follow the reporting requirements as outlined in DWD Policy 2021-10, Change 1.

[8] Exception: IRS-derived 1099 FTI information, IRS TOP information, and IRS TOP intercept amounts may be shared with an external user if they have a data sharing agreement on file with DWD or the data has been shared as part of an audit.
[9] See Attachment A.

Monitoring and Auditing Teams and Chats

DWD shall audit Teams for policy violations, direct remedial activities, and pursue corrective personnel actions as necessary.

Violation of Data Security Requirements

DWD TEAMS users who fail to abide by the security requirements and appropriate use standards for protected information contained within this guidance, DWD Policy 2021-10, Change 1, and the IRUA may be subject to disciplinary action up to and including termination of employment.

Additionally, as reflected in the IRUA, agreed upon by DWD staff and vendors/contractors, anyone knowingly or intentionally accessing State of Indiana or U.S. government information resources without authorization may have their employment or contract terminated, be prosecuted where applicable, and face fines/imprisonment if found guilty.

NOTE: The TEAMS application may contain U.S. Government information. By accessing and using TEAMS, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized use of or access to TEAMS may subject you to state and federal criminal prosecution and penalties as well as civil penalties.

Attachments

Attachment A - Example Staff Acknowledgement Template

Action

All DWD staff, vendors/contractors, and service providers shall be made aware of and agree to adhere to the requirements of this technical assistance, the IRUA, and DWD Policy 2021-10, Change 1.

Additional Information

Questions regarding the content of this publication should be directed to policy@dwd.in.gov.

Attachment A
Example Staff Acknowledgement Template

Acknowledgement of Receipt of and Compliance with the
DWD Microsoft TEAMS User Guidance on Safeguarding Protected Information

I, _____, have read and understand the *DWD*
Printed name of staff member

Microsoft TEAMS User Guidance on Safeguarding Protected Information and I confirm that I will follow the provisions within this guidance.

Signature:_____

Date: _____