☒ Mandatory
☐ Informational
☐ Best Practice
☐ Other

TECHNICAL ASSISTANCE

Date: 12/18/2023

Contact: policy@dwd.in.gov

Program: Indiana Department of Workforce Development (DWD)

Subject: DWD Technical Assistance 2022-13, Change 1
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 2 *Safeguarding Protected Information and DWD User Accounts Management.*

Change 1 Summary

The following changes have been made to this technical assistance document:

- Additional clarifiers regarding FTI and UIQ have been included.
- "Protected Information" is more thoroughly defined.
- A sub-section on the "Use of Social Security Numbers (SSNs) in TEAMS" has been added.
- The types of information that can be shared with authorized DWD users and others have been updated.

Rescission

DWD TA 2022-13 *DWD Microsoft TEAMS User Guidance on Safeguarding Protected Information*

References

- TEGL 39-11 *Guidance on the Handling and Protection of Personally Identifiable Information (PII)*
- DWD Policy 2021-10, Change 2 *Safeguarding Protected Information and DWD User Accounts Management*[1]

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

Definitions

Federal Tax Information (FTI) - Any return or return information received from any secondary source which is protected by the confidentiality provisions of Internal Revenue Code. Since individuals often consent to sharing this data when interacting with DWD, IRS-FTI is the FTI that requires a greater degree of protection.

IRS-FTI - Internal Revenue Service Federal Tax Information that DWD receives from the IRS and is often used as part of the Treasury Offset Program (TOP) using tax return intercepts to recover overpayments. Only authorized individuals who have attended the IRS-FTI trainings should discuss IRS-FTI. This specifically refers to tax intercept amount and other data shared for the TOP process. This does not include general PII or Federal Taxpayer Identification data that a claimant willingly shares in interactions with DWD such as name, Social Security Number (SSN), address, last employer, etc.

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. Information and records of DWD relating to unemployment tax or the payment of unemployment insurance benefits, Social Security Administration Unemployment Insurance Inquiry (SSA-UIQ) responses, Internal Revenue Service Federal Tax Information (IRS-FTI), student educational data, medical records, as well as information which may reveal the individual's or an entity's identity, are confidential pursuant to state and federal laws and regulations governing protected information;

- Privileged Information - Privileged information is available only to authorized persons. Authorization is determined by one's position within DWD or through partnership in contractual relationships with the State of Indiana or any subcontracted entity funded in whole or in part by grants or contracts with DWD. Privileged information is not confidential pursuant to the law but is sensitive in nature. Privileged information is subject to the same restrictions and requirements as confidential information for purposes of this policy. All protected information must be handled properly. For example, privileged information may be policy or program information that is still being drafted and is not yet finalized to be published. Only authorized persons should view that information until it is published. Another example could include internal agency documents that specific departments use that are not confidential but should not be shared outside of the department.; 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. Both confidential and privileged information may contain PII. PII can be further delineated as sensitive PII (protected PII) and non-sensitive PII.[3]

[2] See DWD's *Safeguarding Protected Information and DWD User Accounts Management* policy for additional guidance.
[3] TEGL 39-11, page 2

- 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. Examples include, but are not limited to, social security numbers, IRS-FTI, SSA-UIQ response information, driver's license ID information, biological information, email/postal addresses, credit or debit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse name, educational history, medical history, financial information, and computer usernames and passwords.

- 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.

Information that has been properly aggregated and suppressed is outside the scope of this policy and is not considered "protected information." For the purposes of providing aggregated and suppressed data, no cell can have a count of fewer than ten (10). In addition to this primary suppression, cells must also be secondarily suppressed. Secondary suppression ensures that for a given set of data, it is not possible to derive the value of any cell with fewer than ten (10) cases from the aggregated data (such as subtracting the unsuppressed value from the total). Questions regarding proper aggregation and suppression procedures should be directed to DWD's Data Officer.

SSA-UIQ - Social Security Administration (SSA) Unemployment Insurance Inquiry information obtained from SSA through the UI Interstate Connection Network (ICON) hub as part of the identify validation process.

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 2, 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, file sharing, and audio/video meetings.
- **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, adhere to 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.

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:

- IRUA required training;[5] and
- 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 2, 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 (SSA-UIQ) responses that DWD receives from the SSA; and/or
    - Internal Revenue Service Federal Tax Information (IRS-FTI) that DWD receives from the IRS, mainly for the Treasury Offset Program (TOP). Only those who have attended the IRS-FTI training are in this group.

- DWD Staff users that are **not** authorized to access IRS-FTI/SSA-UIQ information but **are** authorized to access other types of protected information such as Social Security numbers, names, and addresses of individuals.

- 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.

---

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

[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.*

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.

NOTE: Under no circumstance should IRS-FTI be shared with contractors or co-workers not authorized to handle IRS-FTI.

Use of Social Security Numbers (SSNs) in TEAMS

- TEAMS **must never** be used to transmit or store IRS-FTI or SSA-UIQ.
- TEAMS is not to be used to store full SSNs in either the chat or file storage functionality. Instead, staff must use other permissible methods for transmitting data.[7] Other permissible methods include, but are not limited to, sending a secure email to a state-issued email address, or storing it in a password protected shared folder outside of TEAMS.
    - When another permissible method does not exist or cannot be created, full SSN data may be transmitted through TEAMS if it is not IRS-FTI or SSA-UIQ. The data must be deleted from TEAMS once the recipient receives it and properly stores it in the appropriate system of record.
- Full SSNs may only be verbally shared when using the call functionality of TEAMS, which also includes screen sharing when using Uplink or another application that shows the full SSN on the screen.
    - These sessions are not to be recorded in TEAMS, as they include protected information.

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 as a resource.[8]

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 2.

Monitoring and Auditing Teams and Chats

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

---

[7] See DWD's *Safeguarding Protected Information and DWD User Accounts Management* policy for additional guidance.
[8] See Attachment A.

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 2, 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 2.

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: _____