

To: Indiana's Workforce System

From: Indiana Department of Workforce Development (DWD)

Date: December 18, 2023

Subject: DWD Memorandum 2020-15, Change 1
Confidentiality Statement Required for All Non-DWD Individuals Accessing DWD Records

Purpose

To provide updates regarding the confidentiality provisions and Confidentiality Statement required for new contract and grant templates from DWD and for all individuals not employed by DWD (hereinafter "non-DWD individuals") accessing DWD records.

Change 1 Summary

This memo now references DWD's updated guidance on safeguarding information, appropriate Microsoft TEAMS usage, and suitability standards for those with access to federal taxpayer information (FTI).

References

- DWD Policy 2017-08, Change 2 *Suitability Standards for Department of Workforce Development Employees, Contractors, and Subcontractors with Access to Federal Taxpayer Information*
- DWD Policy 2021-10, Change 2 *Safeguarding Protected Information and DWD User Accounts Management*
- DWD TA 2022-13, Change 1 *DWD Microsoft TEAMS User Guidance on Safeguarding Protected Information*
- *DWD Continuity of Operations Plan*

Content

As part of the contract and grant template drafting process, DWD's Legal Division has again reviewed the confidentiality provisions and requirements for data being utilized by DWD's grantees and regional partners. These agreements were supplemented to clearly address various state and federal requirements relating to the use and security of confidential and protected data, including personally identifiable information. Additional language was included within the "Confidentiality of State Information" clause contained in many of the agreements, which relates to types of data being utilized with the contract or grant. These provisions serve to ensure appropriate handling and use of data containing confidential and protected information.

DWD also added a Confidentiality Statement as a requirement for individuals accessing DWD records, which was attached to the contract and grant templates as an exhibit. The Confidentiality Statement

serves to inform any individual handling confidential and protected data related to a contract or grant (including, but not limited to, through Indiana Career Connect (ICC)) of:

1. The requirements and confidentiality provisions associated with handling the data; and
2. Responsibilities in handling the data.

DWD has revised the Confidentiality Statement to be a standalone document and is requiring any non-DWD individuals handling individual level records within DWD's systems to read and sign the Confidentiality Statement prior to accessing or utilizing data. All non-DWD individuals who will view, or access individual level records must sign this document prior to being granted access to individual level records maintained within DWD's systems. Non-DWD individuals seeking access to FTI must also follow the procedures outlined in DWD Policy 2017-08, Change 2 *Suitability Standards for Department of Workforce Development Employees, Contractors, and Subcontractors with Access to Federal Taxpayer Information*. Each non-DWD individual accessing individual level records must sign a new Confidentiality Statement each year prior to July 1, and new hires must sign Confidentiality Statements prior to being granted access to any individual level records maintained within DWD's systems. Copies of the signed Confidentiality Statements shall be maintained on-site by contractors and grantees and be available upon request by DWD during monitoring or other reviews. Contractors and grantees are responsible for ensuring any and all subcontractors and subgrantees are aware of this requirement to obtain and maintain signed copies of the Confidentiality Statements. Copies of the Confidentiality Statements must be maintained on site and must be reviewed as a part of the subcontractor and subgrantee oversight processes.

Removing the Confidentiality Statement from the grant and contract templates and instead utilizing it as a standalone document will help to bring about better awareness of the provisions relating to handling confidential and protected data, as well as reduce the administrative burden on parties by requiring only one signed Confidentiality Statement annually per non-DWD individual requiring access to DWD records.

In the event of a data security incident, as determined by DWD, all DWD partners and grantees shall undertake appropriate mitigating actions as prescribed by applicable federal and state laws and regulations, including providing notice, where required, to the victims, state authorities, and federal authorities.

A "data security incident" occurs when there is reason to believe that there either was or may have been unauthorized access to any confidential or protected data maintained within DWD's systems, damage caused to any of that data, or theft of any of that data. DWD staff, vendors/contractors, and service providers who become aware of any security breach resulting from the inadvertent or intentional disclosure of any protected information shall immediately inform, in person or via phone, the following:

- Their direct supervisor;¹
- The DWD Chief Information Officer (CIO); and
- The DWD General Counsel.

Notification via an email or text is not sufficient but can be used as follow-up to the phone call and/or in person notification.

¹ Supervisors must follow the *DWD Continuity of Operations Plan* if approached regarding a security breach.

Action

All DWD contractors and grantees, including sub-contractors and sub-grantees, must collect executed Confidentiality Statements and retain them for review by DWD upon request. A copy of the Confidentiality Statement to be signed by non-DWD individuals accessing DWD records is attached to this memo.

Additional Information

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

CONFIDENTIALITY STATEMENT

The undersigned individual, who will be given access to DWD Data, which may contain various types of confidential information, including but not limited to confidential unemployment compensation information (“CUCI”) as defined by 20 C.F.R. 603, personally identifying information, as defined by the Family Education Rights and Privacy Act (“FERPA”), 34 C.F.R. 99, and other data that is classified as confidential by state and federal laws, regulations, rules, and policies, understands and agrees with each of the following statements:

1. DWD Data contains personally identifiable information, and as such must be handled in a secure and confidential manner to mitigate the risk associated with use and dissemination of sensitive data.
2. I understand that CUCI, as set forth in Indiana Code 22-4-19-6 and 20 C.F.R. 603, is confidential. I understand that if I recklessly violate Indiana Code 22-4-19-6, I commit a Class B misdemeanor and may be imprisoned for up to 180 days and fined up to \$1000 in accordance with Indiana Code 35-50-3-2.
3. I understand that DWD Data may contain personally identifiable information under FERPA and that the disclosure of such information may constitute an invasion of privacy of a student or former student, and I agree to ensure the confidentiality of such data and not impermissibly disclose such data to a third party.
4. With regard to DWD Data, I shall maintain and use DWD Data in compliance with the Employment and Training Administration of the U.S Department of Labor’s Training and Employment Guidance Letter No. 39-11, “Guidance on Handling Protection of Personally Identifiable Information.” See https://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11.pdf
5. I shall maintain and use DWD Data in compliance with:
 - Indiana Code 4-1-6 – Fair Information Practices; Privacy of Personal Information
 - Indiana Code 4-1-8 – State Requests for Social Security Number
 - Indiana Code 4-1-10 – Release of Social Security Number
 - Indiana Code 4-1-11- Notice of Security Breach
 - Indiana Code 5-14-3 – Access to Public Records
 - Indiana Code 22-4-19-6 – Records; inspection; reports; confidentiality; violations; processing fee
 - Indiana Code 24-4.9 – Disclosure of Security Breach

DWD Policy 2017-08, Change 2: Suitability Standards for Department of Workforce Development Employees, Contractors, and Subcontractors with Access to Federal Taxpayer Information

DWD Policy 2021-10, Change 2: Safeguarding Protected Information and DWD User Accounts Management

DWD TA 2022-13, Change 1: DWD Microsoft TEAMS User Guidance on Safeguarding Protected Information

6. I agree to ensure the confidentiality of DWD Data and not allow impermissible disclosure of DWD Data to any third party.
7. I agree that DWD Data will only be used for the limited purposes authorized by law and in a manner consistent with the requirements of the DWD Data.
8. I agree to use care to protect DWD Data from unauthorized access, misuse, theft, damage, unauthorized destruction, unauthorized modification, and unauthorized disclosure.
9. I agree to immediately report any instance of unauthorized access, misuse, theft, damage, unauthorized destruction, unauthorized modification, and unauthorized disclosure with respect to DWD Data within my knowledge to my direct supervisor so that DWD can be notified as required.

Signature

Name (printed)

Employer

Date