To: All DWD Staff, Vendors/Contractors, and Service Providers

From: Indiana Department of Workforce Development (DWD)

Date: April 24, 2023

Subject: DWD Policy 2021-10, Change 1
Safeguarding Protected Information and DWD User Accounts Management

Purpose

This policy states the guidelines and requirements for the appropriate access, use, storage, and disposal of confidential or privileged information, including sensitive and non-sensitive Personally Identifiable Information (PII; collectively "protected information")[1], maintained by the Indiana Department of Workforce Development (DWD) or any vendor or contractor providing services to DWD, as well as any entity providing services to or through DWD. This policy also outlines requirements for DWD user accounts management as part of DWD's overall protection of information strategy. This policy supplements and is not intended to displace other applicable policies, user agreements, or agency guidance[2] unless otherwise specified.

Change 1 Summary

The *Sharing, Sending, and Receiving Protected Information* section has been updated to provide guidance on the use, sharing, and discussion of protected information through social media, collaboration platforms, and the DWD Call Center.

The *Accessing State Facilities* section has been updated to also require contractors and visitors to wear state issued badges when visiting state facilities.

The *Photographs and Video Recordings* section has been updated to specify that all photos and videos should be reviewed to ensure that they do not contain protected information before being shared or used.

Rescission

- 2021-10 *Safeguarding Protected Information and DWD User Accounts Management*

References

See **Attachment A**

[1] Confidential or privileged information, including sensitive and non-sensitive Personally Identifiable Information (PII) will be referred to as "protected information" throughout this policy.
[2] Examples include but are not limited to DWD Memorandum 2020-15, agency contracts, and systems-related agreements such as the ICC User Agreement.

Definitions

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 (UIQ) responses, Internal Revenue Service Federal Tax Information (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.

Personally Identifiable Information (PII) – Personally identifiable information (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]

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, FTI, 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. Examples include, but are not limited to, first and last names, general education, credentials, gender, or race. However, depending on the circumstances, a combination of non-sensitive PII could potentially be categorized as sensitive PII.[4]

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.

[3] TEGL 39-11 https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=7872.
[4] TEGL 39-11 page 2.

State Property – All information, including but not limited to documents, software, files, data, faxes, phone call recordings, and emails created, accessed, transmitted, or stored electronically or in paper form, related to the nature of the contractual relationship while employed by, or partnered in, a contractual relationship with the State of Indiana or any of its subcontracted entities shall be considered the exclusive property of the State of Indiana.

Content

All individuals and organizations with authorized access to protected information are obligated to ensure the protection and appropriate use of the information. State employees and those who have a business relationship[5] with DWD are subject to State and Federal requirements for safeguarding protected information, which applies to any entity, organization, or individual providing services connected to or through DWD or the WorkOne American Job Center (WorkOne/AJC) workforce system. Those subject to the State and Federal safeguards are prohibited from divulging or benefitting from, or permitting any person to benefit from, protected information.[6]

Universal Requirements for DWD Staff, Vendors/Contractors, and/or Service Providers

Accessing Protected Information
DWD staff, vendors/contractors, and service providers may only access protected information to the extent they have permission or authority. The individual accessing the data must have a bona fide business reason at the time the data is accessed.

The accessing, processing, or storing of any protected information on personally owned equipment, at an off-site location (e.g., an employee's home), or on non-grantee managed IT service is strictly prohibited unless submitted to PrivacyandSecurityOfficers@dwd.in.gov and approved by DWD.

Sharing, Sending, and Receiving Protected Information
All exchanges of protected information require an Information Exchange Agreement (IEA)[7] that includes content on safeguarding protected information.

Protected information sourced from one entity cannot be shared without the express approval of the entity that provided the protected information. Please refer to the bulleted list below for guidance on sharing, sending, and receiving protected information through relevant communication mediums.

- **Social Media and Networking Platforms**
  - This includes Facebook, Twitter, LinkedIn, and all other platforms in which the identity of participating individuals and/or entities is unknown and cannot be verified.
  - DWD staff are prohibited from sharing protected information (including PII and non-public DWD operations information) through posting, messaging, or any other means on any social media or social networking platform.

[5] The definition of "business relationship" in IC 4-2-6-1(a)(5) includes the dealings a person has with an agency seeking, obtaining, establishing, maintaining, or implementing a pecuniary interest in a contract (including a grant agreement) with an agency.
[6] Indiana State Code of Ethics https://www.in.gov/ig/ethics-code/ and IAC 1-5-1 0 and 11.
[7] Generally, IEA are required for data extracts and are not required for normal business exchanges.

- **Collaboration Platforms**
  - This includes, but is not limited to, Microsoft Teams, Zoom, and audio/video conferencing, including audio/video equipment within DWD and partner conference rooms.
  - Only the "call" (telephone-like) functionality may be used to verbally discuss protected information.[8]
    - DWD staff, contractors, vendors, and service providers are prohibited from recording calls during which protected information is discussed.
    - "Calls" involving FTI or UIQ information may only involve participants that are authorized to access FTI/UIQ information.
  - The use of "Chat", where content is typed or uploaded, may NOT be used to share protected information with an unauthorized user.[9] Participant identity must be verified to ensure they are authorized to access protected information.
    - "Chat" activity is retained, which poses a data security risk if protected information is discussed with unauthorized users.
  - SDLC documentation tools or knowledge bases including but not limited to Atlassian Confluence must not be used to share or contain protected information with unauthorized users.
  - Exceptions can be requested through the DWD Data Privacy and Security Officers.[10]
- **DWD Contact Center**
  - This includes "calls" via the Genesys PureConnect or Genesys Cloud systems.
  - Calls are recorded and stored within the secured Genesys systems.
  - Prior to discussing protected information with a caller, the DWD representative must verify the caller's identity per DWD department procedures.

If protected information is unexpectedly received, encountered, or sent to an unintended recipient by DWD staff, vendors/contractors, or service providers, the incident is to be reported to the individual's direct supervisor, the DWD Chief Information Officer (CIO) and the DWD General Counsel.[11]

Storage, Retention, and Destruction of Protected Information

DWD staff, vendors/contractors, and service providers are responsible for ensuring that protected information is properly filed and stored when their workspace is unattended. Documents containing this type of information must never be left unattended and must be stored in a secure location when not in use. Additionally, all work computers, laptops, cellphones, and other devices must be locked when unattended in accordance with the IOT IRUA to prevent unauthorized access.

It is not permissible to email, fax, copy, print, export, store, discuss over the phone, dispose of, or electronically transfer protected information without proper permission or authority from your supervisor. Additionally, upon approval, all protected information containing personally identifiable

---

[8] 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.

[9] Authorized User – a user that is required to adhere to the requirements of this policy, the Information Resources Use Agreement (IRUA), and/or has a legitimate business need to have access to protected information that has been authorized by DWD.

[10] Send requests to PrivacyandSecurityOfficers@dwd.in.gov.

[11] See the *Security Breach* section of this policy for contact information for the CIO and General Counsel.

information transmitted via file transfer protocol, voice,[12] email, or stored on CDs, DVDs, USB storage devices, or any other mobile or portable storage devices, must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. However, staff are prohibited from emailing unencrypted protected information that contains sensitive personally identifiable information to any person or entity.[13]

The storage of non-business-related content or unapproved software on State-issued devices is not permitted.

DWD staff must use the secure email process made available by State of Indiana IOT or other encrypted email methods to send emails that contain protected information.

All protected information must be retained and destroyed in accordance with the Record Retention schedule administered by the Indiana Archives and Records Administration (IARA).[14] Indiana Code 5-15-5.1-13,[15] requires that confidential records must be destroyed in such a manner that they cannot be "read, interpreted, or reconstructed." Large retention and/or record destruction requests must be made according to IARA standards.[16]

Records, printouts, notes, and documents that have reached the end of their required retention period and are no longer needed and that contain protected information must be securely shredded. Electronic media and hardware must be disposed of according to IARA and IOT procedures.

Photographs and Video Recordings

The unauthorized use of cameras, including cell phone cameras or video cameras, by DWD staff, vendors/contractors, or service providers is prohibited while on WorkOne/AJC, DWD, or remote work premises. Photographs and video recordings that are used for business reasons or to document special occasions, such as retirement, birthday, or award celebrations must only be used or shared after being reviewed to ensure they do not contain protected information.

Required Staff Training

DWD staff and vendors/contractors that use State of Indiana technology tools and resources are required to complete IOT's Information Resources Use Agreement (IRUA) when they are hired or receive their vendor or State contractor account and then every two (2) years thereafter.

DWD staff, vendors/contractors, and service providers are required to adhere to the security safeguards set forth in this DWD agency policy.

Additionally, all DWD staff are required to adhere to the State Employee Handbook and must complete all IOT's monthly cyber security training modules by the specified deadline.

---

[12] The term "voice" includes voicemail and other unencrypted digital, electronic, and analog recordings.
[13] TEGL 39-11 https://wdr.doleta.gov/directives/corr_doc.cfm?DOCN=7872.
[14] IARA Record Retention Schedules for DWD https://www.in.gov/iara/3276.htm.
[15] Indiana Code 2020 Session IC 5-15-5.1-13 http://iga.in.gov/legislative/laws/2019/ic/titles/005#5-15.
[16] IARA Destroying Records https://www.in.gov/iara/3210.htm, IARA Policy 20-01, Electronic Records Retention and Disposition https://www.in.gov/iara/files/policy-20-01-erecords-retentionanddisposition.pdf, and Electronic Records Technical Standards IARA Policy 20-02 https://www.in.gov/iara/files/policy-20-02-erecords-technicalstandards.pdf.

Accessing State Facilities[17]

- All DWD staff, contractors, and visitors are required to wear State ID badges visibly, on their person.
- When entering a secure area via the scanning of your badge, do not allow others without a visible, valid badge to enter (piggyback) immediately behind you. Notify security and/or the DWD Director of Facilities if this happens.
    - For the Indiana Government Center, notify State's Security Control:
        - (317) 234-4838 (unless it becomes an emergency, which would then be 911)
    - For other locations:
        - Please follow the location's standard procedures
- Visitors to DWD offices in state facilities must sign in and be given a visitor's badge (where available). Visitors must be escorted within state facilities.

Access to the State Network Outside of the U.S.[18]

- State devices that can connect to the State network via a wired, wireless, or remote VPN connection are not permitted to be taken outside the United States.
- DWD staff and vendors/contractors are **not** permitted to access the State network from outside the United States via non-State issued devices.

Security Breach

A security breach is the unauthorized acquisition of protected information that compromises the security, confidentiality, or integrity of that information. 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;
- The DWD Chief Information Officer (CIO), (317) 234-8371; and
- The DWD General Counsel, (317) 234-8451.

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.

Violation of Data Security Requirements

DWD staff, vendors/contractors, and service providers who fail to abide by the security requirements and appropriate use standards for protected information contained herein may be subject to disciplinary action up to and including termination of employment.

DWD staff, vendors/contractors, and service providers who access or use protected information beyond the scope of authority granted to them or without a legitimate business purpose will be subject to disciplinary action up to and including termination of employment.

A person who knowingly or intentionally exerts unauthorized control over the property of another commits criminal conversion, a Class A misdemeanor under Indiana Code 35-43-4-3(a).[19] Therefore,

---

[17] This does not include local area American Job Center/WorkOne offices, which may have their own badge policies.

[18] Exceptions may apply but will require the approval of the DWD IT CIO and/or the DWD Security Officer, PrivacyandSecurityOfficers@dwd.in.gov, and will be limited in duration.

[19] Indiana Code 2020 Session IC 35-43-4-3(a) http://iga.in.gov/legislative/laws/2019/ic/titles/035#35-43-4-3.

DWD staff, vendors/contractors, and service providers who use State property, including documents, records, or data for personal reasons and without a legitimate business reason can be charged with criminal conversion. Additionally, the unauthorized use of data related to a federal program can be subject to additional federal criminal prosecution and civil enforcement actions that may result in a fine and/or imprisonment.

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 can have their employment or contract terminated, be prosecuted where applicable, and face fines/imprisonment if found guilty.

Additional DWD Staff-Specific Requirements

DWD Staff Account Access
DWD supervisors are required to submit a request to the DWD Service Desk[20] whenever:

- A subordinate needs access to a computer, network, server, directory folder, application, or database, that processes or stores protected information.
- Creating, modifying, disabling, or deleting an account (network/application/database).
    - Requests to disable/terminate account access for staff that will no longer be working for the agency must be submitted in a timely manner.
- Supervisors are also required to ensure staff have the appropriate level of training on safeguarding protected information before submitting an access-related account request.

FTI and UIQ Response Requirements
The following applies to specific DWD staff that have a business reason to access FTI and UIQ response data:

- DWD staff having access to FTI are required to complete the following:
    - Annual Treasury Offset Program Security (TOPS) role training modules; and
    - DWD's specific FTI handling role training module.
- Security Background Checks
    - DWD staff having authorized access or potential access to FTI are required to be fingerprinted and submit to an enhanced background check by the FBI.
- It is not permissible to email, fax, copy, screenshot, print, or save FTI or UIQ response data to any storage media, other than within designated storage within the Uplink and/or Contact Center applications.
    - If FTI and/or UIQ response data is inadvertently mishandled, individuals must contact their direct supervisor, the DWD Chief Information Officer (CIO) and the DWD General Counsel.[21]
- DWD supervisors and Account Control administrators are required to adhere to DWD Policy 2017-08, Change 1 *Suitability Standards for Department of Workforce Development Employee and Contractor Access to Federal Taxpayer Information* when requesting, authorizing, and granting access to FTI.

[20] Send requests to https://www.in.gov/dwd/intranet/dwd-service-desk/.
[21] See the *Security Breach* section of this policy for contact information for the CIO and General Counsel.

- If FTI is inadvertently printed, it must be shredded and logged. To log the incident, please notify the DWD Security Officer.[22]

Universal Acknowledgement Requirement

All DWD staff, vendors/contractors, and service providers shall read, acknowledge, and abide by this and all applicable agency policies, state and federal regulations, and state and federal statutes governing the access, use, and distribution of protected information.[23] All DWD staff, vendors/contractors, and service providers shall agree to access protected information for authorized business purposes only and to abide by all other requirements and terms contained therein. This policy supplements and is not intended to displace other applicable policies, user agreements, or agency guidance unless otherwise specified.

Action

All DWD staff, vendors/contractors, and service providers shall be made aware of and agree to adhere to the requirements of this policy. Contents of this policy will be part of routine DWD monitoring.

Effective Date

Immediately.

Ending Date

Upon rescission.

Attachments

Attachment A - References
Attachment B - DWD User Accounts Management

Additional Information

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

[22] Notifications are to be sent via email to PrivacyandSecurityOfficers@dwd.in.gov.
[23] Examples include but are not limited to IC 4-1-6, TEGL 39-11, this policy, DWD Memorandum 2020-15, and all systems-related agreements such as ICC's User Agreement, and IOT's IRUA.

Attachment A
References

- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, 34 CFR 99
- Federal Information Security Management Act of 2002 (FISMA)
- Privacy Act of 1974
- Social Security Act of 1935
- Computer Security Act of 1987
- 26 U.S.C. § 3304(a)(16) and 6103
- 29 U.S.C. § 3341
- 42 U.S.C. § 503 and 654a(d)(1)-(5)
- 20 CFR 603
- I.C 4-1-6
- I.C. 4-1-8
- I.C. 4-1-10
- I.C. 4-1-11
- I.C. 4-3-26
- I.C. 5-14-3-6.5
- I.C. 22-4-19-6
- I.C. 24-4.9
- TEGL 39-11 *Guidance on the Handling and Protection of Personally Identifiable Information (PII)*
- Internal Revenue Service Publication 1075
- NIST Special Publication (SP) 800
- Social Security Administration Technical Systems Security Requirements (TSSR) version 8.0, 12/2017
- OMB Circular A-130 (revised) *Managing Information as a Strategic Resource*
- IARA Policy 20-01 *Electronic Records Retention and Disposition*[24]
- IARA Policy 20-02 *Electronic Records Technical Standards*[25]
- DWD Policy 2017-08, Change 1 *Suitability Standards for Department of Workforce Development Employee and Contractor Access to Federal Taxpayer Information*

[24] https://www.in.gov/iara/files/policy-20-01-erecords-retentionanddisposition.pdf.
[25] https://www.in.gov/iara/files/policy-20-02-erecords-technicalstandards.pdf.

Attachment B
DWD User Accounts Management

DWD Account Access Types

Types of access accounts requiring security compliance oversight (described further below), include but are not limited to:

- State network account access for individuals
- Contractor account
- Temporary account (temps, interns, vendors, service providers, …)
- Elevated privileged administrator accounts
- Service accounts

Types of access privileges to State resources requiring security compliance oversight (described further below), include but are not limited to:

- State applications such as Email, PeopleSoft, remote VPN, RightFax, SharePoint, …
- DWD applications such as Uplink, COMPAS, Bomgar, ICC, CRM, …
- DWD application access roles/levels such as Admin, SuperUser, TOP_INTERCEPT, ROLE_TOP_HOLD, Tax_Clearance,
- Individual's home directory access
- Shared directory access
- Remote access

DWD Account Access Maintenance Security Safeguards

To create, modify, disable, or remove account access to State resources, by employees, contractors, temps, interns, vendors or service providers, staff are required to adhere to the following security safeguards:

- "New Hire" employee/contractor/temp/intern computer/network account creations require authorization by the hiring manager.
- Temporary network account creations for short term technical support by a vendor/contractor/service provider require authorization by the system owner.
- Isolated elevated privileged account creations solely for administrator duties requires authorization by the system owner.
- Service accounts creations require authorization by the system owner.
- Intra-agency position transfers require authorization by department managers.
- Modifying, disabling, or removing a computer/network account of a voluntary or involuntary terminated employee requires authorization by a department manager.
- Reassignment/disablement/removal of objects tied to an account (email, home directory, application work items, …) require authorization by a department manager or authorized designee.
- Application account role/level access maintenance requires authorization by a department manager or authorized designee.

- File directory permissions maintenance requires authorization by a department manager or authorized designee.
- VPN remote access requires authorization by a department manager or authorized designee.
- Database user account maintenance requires authorization by a DWD IT manager.
- Database application account maintenance requires authorization by the DWD IT system owner.
- DWD Account Control will ensure contractor accounts do not have access to FTI or UIQ response data via an application account/role or file directory permissions.
- DWD DBAs will ensure contractor database accounts do not have access to FTI or UIQ response data.
- DWD Account Control is not permitted to initiate account maintenance without an authorizing supervisor's request and approval.[26]
- To perform the actual account maintenance, DWD Account Control reviews a supervisor's request[27] for security compliance and then submits a ticket request to IOT to execute the account maintenance.
- IOT staff are not permitted to initiate account maintenance without DWD Account Control's authorizing ticket request.
- Exemptions to the following default settings may be requested[28] and authorized by a manager:
  - Enable the disabling of exporting data from a State workstation's USB port.
  - Enable a DWD worker access to a prohibited internet site.
  - Enable a DWD IT administrator to install non-whitelisted software on a State device
  - Enable storage to a 3rd party storage service provider (e.g., GoogleDrive, DropBox, …).

DWD Account Access Monitoring/Logging Oversight

- DWD Account Control reviews the status of accounts monthly for inactivity and will disable or remove accounts/roles/access as necessary.
- Access to servers is monitored via the QRadar network activity logging tool, with access being reviewed weekly by the DWD Security team.
- Access to UIQ response information via the Uplink application is logged and is reviewed weekly by the DWD Benefits Payment and/or DWD Security teams.
- Access to the FTI database schema via Oracle accounts is logged and is reviewed weekly by the DWD Security team and the DWD lead DBA.
- Access to FTI via the Uplink application is logged and is reviewed weekly by the DWD Security team.
- Unauthorized access attempts to the FTI database schema are systematically captured and reported immediately to the DWD IT security officer and appropriate IT management and are immediately investigated.
- State workstations and servers are scanned every 6 hours for software vulnerabilities and reported to a central collector. Other devices are scanned monthly. Owners of the most vulnerable workstations and servers are notified periodically of their situation. Identified workstations having malicious software are either rectified or disabled and reimaged.

[26] Requests are to be emailed to DWDServiceDesk@dwd.in.gov.
[27] Requests are to be emailed to DWDServiceDesk@dwd.in.gov.
[28] Requests are to be emailed to DWDServiceDesk@dwd.in.gov.

- Requests, approvals, and maintenance related to account access maintenance are retained for at least 7 years, both by DWD's Service Desk Ticketing application and IOT's vFire HelpDesk ticketing tracking system.
- DWD DBAs ensure DWD contractors do not have access to FTI schema logs.

DWD/SPD Human Resources Oversight

- Account control management of PeopleSoft Time and Labor.

DWD Accounting Oversight

- Account control management of PeopleSoft Financials (EnCompass).