SOP 22-02
Safeguarding Protected Information and DWD User Accounts Management
Standard Operating Procedures
Grow Southwest Indiana Workforce Region 11
Approval Date: 05/20/2022

Purpose

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

Rescission

DWD Policy 2013-03 Requirements Pertaining to Confidential and Privileged Information
DWD Policy 2007-46 Guidance on the Proper Handling of Social Security Numbers
DWD Policy 2003-17 Computer Use Policy

References

See Attachment B

Action

DWD Policy 2021-10 Safeguarding Protected Information and DWD User Accounts Management will be implemented in Region 11 as SOP 22-01.

CONTENT

All individuals, organizations, business entities, and Department staff with access to confidential and/or privileged information have an obligation to ensure the protection and appropriate business use of the information. State employees and those who have a business relationship with the 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 these safeguards are prohibited from benefiting from, or permitting any other person to benefit from, information confidential in nature and from divulging confidential information. A complete copy of the Indiana Code of Ethics may be found at https://www.in.gov/ig/ethics-code/ and IAC 1-5-10 and 11.

Definitions

Confidential information is 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, storge, disposal, and appropriate use of the information for official lawful purposes. Information and records of DWD relating to the unemployment tax, or the payment of unemployment insurance benefits, SSA Unemployment Insurance Inquiry (UIQ) responses, IRS Federal tax information (FTI), student educational data, medical records, as well an information that 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 is available only to authorized persons. Authorization is determined 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 grant 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 should be handled properly.

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Both confidential information and privileged information may contain PII. PII can be further delineated as Sensitive PII (or Protected PII) and Non-Sensitive PII. See Training and Employment Guidance Letter (TEGL) No. 39-11.

Sensitive PII, or Protected PII, is 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 names, 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 those items could potentially be categorized as Protected or Sensitive PII.

Information that has been properly aggregated and suppressed 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 account of fewer that 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 DWD's Data Officer.

State Property- All information including but not limited to documents, software, files, data, faxes, phone call recordings, and e-mails 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 while employed by or partnered in contractual relationships with the State of Indiana or any of its subcontracted entities shall be considered the exclusive property of the State of Indiana.

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

Accessing Protected Information

- DWD staff, vendors/contractors, and services 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 approved by DWD.

Sharing, Retention, and Destruction of Protected Information

- All exchanges of protected information require an Information Exchange Agreement (IEA) that includes content on safeguarding protected information.
- The sharing of protected information requires appropriate approvals by both the sending and receiving parties, which is done via a Data Sharing Agreement (DSA).
- Protected information sources from one entity cannot be shared without the express approval of the entity that provided the protected information.
- If protected information is unexpectedly received, encountered, or sent to an unintended recipient by DWD staff, vendors/contractors, or services providers, the incident is to be reported to your direct supervisor the DWD Chief Information Officer (CIO), and the DWD General Counsel.

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 is use. Additionally, all work computers, laptops, cellphones, and other devices must be locked when unattended in accordance with the IOT IRUS 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 information transmitted via file transfer protocol, voice, email, or stored, CD, DWD, USB storage devices, or any other mobile or portable storage, 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 to any person or entity.
- 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). Indiana Code 5-15-5.1-13 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.
- Records, printouts, notes, and documents, which have reached the end of their required retention period and are not 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 videos, by DWD staff, vendors/contractors, or service providers is prohibited while on WorkOne/AJC, DWD, or remote work premises.
- Cameras that are used for business reasons or to document special occasions, such as retirement, birthday, or award celebrations, must only be used with the immediate supervisor's approval and all photographs or video recordings must be limited to the subject area.

Social Media

- DWD staff and vendors/contractors, and service providers are prohibited from posting any protected information on any social media platform.

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 following:
  - Security safeguards set forth in this DWD agency policy, and
  - All IOT and DWD policies and procedures as published within Archer, the State's governance, risk, and compliance tracking system.
- 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.

Accessing State Facilities

- All DWD staff 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 other 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 them be 911)
  - For other locations:
    - Please follow the location's standard procedures
- Visitors to DWD offices in state facilities must sign and be given a visitor's badge (where available). Visitors should be escorted within state facilities.

Access to the State Network Outside of the U.S.

- 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:
  1. Their direct supervisor
  2. The DWD Chief Information Officer (CIO), (317) 234-8371, and
  3. 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 the authority granted or without legitimate business reason to do so will be subject to disciplinary action up to and including termination of employment.
- In addition, a person who knowingly or intentionally exerts unauthorized control over the property of another commits criminal conversion, which is a Class A misdemeanor under IC 35-43-4-3(a). Therefore, 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 whenever:

- A subordinate needs access to a computer, network, server, directory folder, application, or database, that processes or stores protected information.
- Creating, modifying, disability, or deleting an account (network/application/database)
  - Requests to disable/terminate account access for staff that will not 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 IRS 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 IRS 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 IRS FTI or SSA UIQ response data to any storage media, other than within the Uplink and/or Contact Center applications.
    - If IRS FTI and/or SSA UIQ response data is inadvertently mishandled, director supervisor, the DWD Chief Information Officer (CIO) and the DWD General Counsel.
- DWD supervisors and Account Control administrators are required to adhere to DWD Policy 2017-08 Suitability Standards for Department of Workforce Development Employee and Contractor Access to Federal Taxpayer Information when requesting, authorizing, and granting access to IRS FTI.
- If IRS FTI is inadvertently printed, it must be shredded and logged. To log the incident, please notify the DWD Security Officer.

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. 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 term contained therein. This policy supplements and is not intended to displace other applicable policies, user agreement, 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 – DWD User Accounts Management
Attachment B- References

Attachment A
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 applications access roles-levels such as Admin, SuperUser, TOP_INTERCEPT, ROLE_TOP_HOLD< Tas_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.
- Isolate 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 ties 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 permission maintenance requires authorization by a department manager or authorized designee.

- VPN remote access requires authorization by a department manager or authorized designee.
- Database user application account maintenance requires authorization by the DWD IT system owner.
- DWD Account Control will ensure contractor accounts do not have access to IRA FTI or SSA UIQ response data via an application account/role or file directory permissions.
- DWD DBAs will ensure contractor database accounts do not have access to IRS FTI or SSA UIQ response data.
- DWD Account Control is not permitted to initiate account maintenance without an authorizing supervisor's request and approval.
- To perform the actual account maintenance, DWD Account Control reviews a supervisor's request 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 setting may be requested and authorized by a manager:

Enable the disabling of exporting data forma 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 account monthly for inactivity and will disable to remove accounts/roles/ access, as necessary.
- Access to servers is monitored via the QRadar network activity logging tool, with access being review weekly by the DWD Security team.
- Access to SSA 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 IRS FTI database schema via Oracle accounts is logged and is reviewed weekly by the DWD Security team and the DWD lead DBA.
- Access to IRS FTI via the Uplink is logged and is reviewed weekly by the DWD Security team.
- Unauthorized access attempts to the IRS 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 or their situation. Identified workstations having malicious software are either rectified or disabled and reimaged.
- Request, 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 IRS FTI schema logs.

DWD/SPD Human Resources Oversight
Account control management of PeopleSoft Time and Labor

DWD Accounting Oversight
Account control management of PeopleSoft Financial (EnCompass).

Attachment B
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 19335
- 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)
- IRS Publication 1075
- NIST Special Publication (SP) 800
- SSA Technical Systems Security Requirement (TSSR) version 8.0, 12/2017
- OMB Circular A-130 (revised) Managing Information as a Strategic Resource
- IARA Policy 20-10 Electronic Records Retention and Disposition
- IARA Policy 20-02 Electronic Records Technical Standards
- DWD Policy 2017-08 Suitability Standards for Department of Workforce Development Employee and Contractor Access to Federal Taxpayer Information