WORKFORCE PROGRAM PRIVACY

Department of Labor and Regulation (DLR) staff or other personnel with access to confidential information received by DLR are advised of the confidential nature of the information, the safeguards to protect the information, and the civil and criminal sanctions for noncompliance with such safeguards. Personnel must acknowledge their understanding of these compliance requirements and their liability for improper disclosure. This policy covers the handling of confidential information, including but not limited to private information a customer shares with DLR staff about their situation, and personally identifiable information (PII) collected from DLR staff or SDWORKS system during utilization of DLR services. DLR may amend this policy as necessary.

PERSONALLY IDENTIFIABLE INFORMATION

The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

1. Protected PII – information that, if disclosed, could result in harm to the individual whose name or identity is linked to the information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, biometric identifiers (fingerprints, iris scans, etc.), medical history, financial information and computer passwords.
2. Non-sensitive PII – information that, if disclosed, by itself could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

Information collected by DLR includes, but is not limited to names, addresses, telephone numbers, citizenship, gender, race, Social Security Number, Federal Employer Identification Number, State Employer Identification Number, age, work history, educational outcomes, individual's program and service eligibility, information necessary for program enrollment and reporting for the purpose of required program reporting and performance.

Handling of PII

The U.S. Department of Labor Employment and Training Administration (ETA) has established the following requirements for the handling of PII:

- Data must be processed in a manner to protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records. PII data must be stored in an area physically safe from access by unauthorized persons at all times.
- All PII and other sensitive data transmitted via email or stored CDs, DVDs, thumb drives, etc. must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Both Classic and New Outlook provide an option to encrypt an email to an outside entity, i.e. not within the state.sd.us domain, utilizing the email option button and choosing 'Encrypt' to send PII outside of the state system. PII may also be transmitted through secure methods such as Microsoft Form and Adobe Sign.

- DLR may use SharePoint, OneDrive, or SDWORKS document management to store PII. Accessing, processing, and storing of ETA grant PII data on personally owned equipment is prohibited. Paper documents are discouraged, but, when necessary, they must be stored in a locked cabinet and appropriate methods for destroying are required, such as shredding.
- Data may not be obtained or used for any purpose other than those required by the programs. Access to data is restricted to only those individuals who need it in their official capacity to perform duties in connection with the scope of work.

Back to Table of Contents

SDWORKS

The SDWORKS website allows job seekers, employers, and the general public to use labor exchange functions and find labor market information about South Dakota. SDWORKS collects PII during account registration, during use of SDWORKS, and any time personal information is requested during use of the website. This information is gathered to fulfill workforce reporting and program performance requirements to ensure program integrity and future improvements. In addition, information is used to create a personal profile or job listing to post in the SDWORKS searchable database servers.

SDWORKS users may create an electronic resume or job listing to be stored online. In the Account Settings, registered SDWORKS users have the option to make a resume open to public viewing by employers, this includes any information in the resume such as address, phone, email, etc. When information is sent to an employer or recruiter, DLR is not responsible for the retention, use or privacy practices of the employer or recruiter. Voluntarily disclosing PII, usernames, e-mail addresses, or messages from SDWORKS may result in unsolicited messages from other individuals or third parties. Such activities are beyond the control of the SDWORKS system and DLR.

IP addresses and website usage information is automatically collected when a user visits the SDWORKS website. This information helps to evaluate visitor behavior on an aggregate basis, including the number and frequency of visitors to each page and the length of time each page is viewed.

Cookies may be passed to a user’s computer. Cookies are information files a web browser places on the hard drive of a computer or temporarily in a computer's memory during internet browsing. Cookies cannot damage user files or read information from a hard drive. SDWORKS cookies are used to maintain a user’s session as they move through pages within the website. SDWORKS will set an identifying cookie to customize the website to best meet the needs of the user.

Email addresses of SDWORKS users, specifically out-of-state residents, may be used for the purpose of market research and outreach. Such information supports the efforts of workers recruitment programs, such as Dakota Roots. This could result in unsolicited direct mail, email blasts, etc.

Webpage visits, time spent on a webpage, visits to a job order, and job searches are gathered to learn more about customer usage and webpage performance.

The aggregate data may be provided to third parties to assist DLR in enhancing workforce development efforts. The SDWORKS error logging system will collect usernames related to any website errors as a means to help our technical staff understand the error.

The SDWORKS website provides links to navigate a user to other websites which may have their own information collection practices, privacy policies and security measure. Visitors to other websites from SDWORKS should review the privacy policies and information collection practices of those websites.

Management information systems, such as SDWORKS, contain confidential information that can only be used by assigned staff with permission and for authorized purposes only. The available screens are not to be printed, duplicated, or disseminated in any unauthorized manner.

SDWORKS Access

To ensure the security and integrity of the SDWORKS system, the following measures are in place:

- **Physical Security:** Access to database servers is restricted to authorized personnel only.
- **Electronic Security:** Data is protected using SSL encryption to prevent unauthorized interception and ensure secure communication.
- **Individual Account Protection:** Each user must use their own password to access their SDWORKS account. Passwords should never be shared.
- **Session Security:** Users should log off and close their web browser after each session to prevent unauthorized access.
- **Data Usage Restrictions:** Information accessed through the system may only be used for purposes directly related to the authorized programs. Unauthorized use or distribution of data is strictly prohibited.

Back to Table of Contents

SOCIAL SECURITY NUMBERS

All DLR staff have a responsibility to keep Social Security Numbers (SSNs) of job seekers and other individuals secure.

DLR prohibits the disclosure of SSNs to unauthorized persons or entities. DLR staff will not knowingly display, disclose, transfer, or unlawfully use the SSN of any employee, student, or other individual in any manner that violates the Social Security Protection Act of 2004 or the Privacy Act of 1974.

SSNs should only be collected where required by federal or state law. If a unique personal identifier is needed, a substitute for the Social Security Number shall be used in its place.

Documents, materials, or computer screens displaying SSNs shall be kept out of public view at all times.

Documents containing SSNs shall only be sent where permitted by state and federal law. An SSN may be included in a mailed document where:

- It is sent as part of an application or enrollment process initiated by the individual.
- It is sent to establish, confirm the status of, service, amend or terminate an account, contract, employee or health insurance benefit – or to confirm the accuracy of a Social Security Number of an individual who has an account, contract, policy, or employee or health insurance benefit.
- It is sent for the purpose of compliance with proper administration of the Reemployment Assistance (RA) program.
- It is contained in a public record and is mailed in compliance with the Freedom of Information Act. Otherwise, the Social Security Number shall be redacted.
- It is mailed by, or at the request of, an individual whose Social Security Number appears in the document or information of his or her parent or legal guardian.
- The number shall not be revealed through the envelope window or be visible from the outside of the envelope.

Full SSNs should be avoided being sent through email. Instead, the individual's first and last name and last four digits of his/her Social Security Number should be sent through email, if necessary. However, when it is necessary to provide a full SSN to an entity outside of the state domain, state.sd.us, email encryption shall be utilized.

DLR staff shall not disclose any SSN over the telephone or leave a voice mail message disclosing any SSN. If an SSN must be faxed, the fax message shall be accompanied by a transmittal sheet which includes a "Confidential Notice" stating the

information included is intended to be privileged and confidential and it is only intended for the use of the individual or entity named on the transmittal sheet.

All documents or files containing SSNs shall be stored in a physically secure manner. SSNs shall not be stored on computers or other electronic devices not secured against unauthorized access. When erasing Social Security Numbers from a laptop or desktop computer, staff shall ensure the number was erased completely, including from the recycle bin.

Use of SSNs

SSN will ONLY be used for the following reasons:

1. Determination of program eligibility or in such cases of payment of wages and allowances, even though at intake it may not be possible to determine the form of payment, if any, the applicant will receive; and

Individuals seeking Reemployment Assistance benefits, Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), and Work Opportunity Tax Credit (WOTC) must provide their SSN for eligibility. Title XI of the Social Security Act, Section 1137(a)(1) provides:

> *"the State shall require as a condition of eligibility for [the programs listed in the first sentence of this paragraph] that the claimant furnish the State with the individual's Social Security Account Number and the State shall utilize such number in the administration of the programs specified."*

Individuals taking part in a paid work experience must provide an SSN so the Department can accurately report wages and issue a W-2.

2. Tracking RA wage records for the calculation of program performance measure outcomes.

Pseudo SSNs

In accordance with 20 CFR §666.150 an SSN must be requested at intake or during online registration in SDWORKS. However, a customer is not required to provide their SSN. If a customer does not wish to share their SSN, a pseudo-SSN can be generated. When requesting a customer's SSN, the use and the privacy and security of the SDWORKS system must be explained.

In accordance with Section 7 of the Privacy Act of 1974 (5 U.S.C. Section 552a Note (Disclosure of Social Security Number), unless the disclosure is required by Federal statute, applicants may not be denied any right, benefit or privilege provided by law because of the individual's refusal to disclose their Social Security Number (SSN). With the exception of the items identified in #1 above, a service will not be denied for failure to disclose an SSN.

Back to Table of Contents

RELEASE OF INFORMATION

DLR staff should not release information regarding an individual's situation or PII without written authorization in Release of Information Form 1.

An individual may refuse to sign any or all three of the intake forms. Depending on the situation, refusal to sign may result in limited availability of services to the individual. If an individual refuses to sign Equal Opportunity Form 2 or One-Stop Services Form 3, the refusal will be noted in SDWORKS. The individual may still receive the full range of services available at the One-Stop Center.

Information requests made by law enforcement or requests made by subpoenas must be directed to the Division Director and DLR's legal team. Information shared should protect confidentiality.

When federal agencies make onsite inspections or audits, DLR must make information available; contact the Division Director for assistance. Individuals who gain access to confidential information must first sign a confidentiality agreement.

20 CFR §666.150
TEGLs 5-08, 39-11, 10-24
Section 7 of the Privacy Act of 1974 (5 U.S.C. Section 552a Note (Disclosure of Social Security Number))
Title XI of the Social Security Act, Section 1137(a)(1)
Federal Information Processing Standards 140-2 c
Social Security Protection Act of 2004 or the Privacy Act of 1974
Freedom of Information Act

Back to Table of Contents