|  |  |
| --- | --- |
| Policy No.  | **15** |
| Effective Date | 5/23/2019 |
| Approval  | GNWDB  |

**Personally Identifiable Information Policy**

**Reference**

TEGL 39-11.

**Policy**

**Personally Identifiable Information**

The Workforce Innovation Opportunity Act (WIOA) requires that recipients of WIOA Title 1 funds provide personally identifiable information (PII) to access WIOA services. PII and other sensitive information must be protected consistent with applicable Federal, State, and local privacy and confidentiality laws. This policy addresses the security of sensitive and non-sensitive PII, for services offered through WIOA Title I.

The Department of Labor has defined two types of PII, protected PII and Non-sensitive PII. The differences between the two are primarily based on an analysis regarding the risk of harm that could result from the release of the PII.

**Protected PII**

Protected PII is 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, credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers, medical history, financial information and computer passwords.

**Non-sensitive PII**

Non-sensitive PII is information that if disclosed, by itself, could not reasonable 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. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

Examples include, but are not limited to, first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

**Data Protection**

1. 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.
2. Staff and other personnel who have access to PII 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 acknowledge their understanding of these compliance requirements and their liability for improper disclosure during their new-hire orientation.
3. PII will be stored in a secure location that is safe from access by unauthorized persons. Accessing, processing and storing participant data on personally owned equipment at off-site locations is prohibited.
4. Staff must ensure privacy of all PII obtained from participants and/or other individuals and protect such information from unauthorized disclosure. Participants will be required to sign a release of information to listed parties before any PII is shared with another person/agency.
5. 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.
6. All data transmitted electronically must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Unencrypted sensitive PII must not be emailed.

**Data Breach**

Any breach of data must be reported in writing to the administrative entity immediately upon occurrence, not to exceed 24 hours after the breach is identified.

**Data Retention**

Data will be retained for the required three years, then destroyed.

**Disclaimer**

This policy is based on Greater Nebraska’s reading of the applicable statutes, regulations, rules and guidance released by the U.S. Government and the State of Nebraska. This policy is subject to change as revised or additional statutes, regulations, rules and guidance are issued.