WORKFORCE INVESTMENT NETWORK
LOCAL WORKFORCE INVESTMENT AREA (LWIA) 13

DATE:	**January 10, 2014**
POLICY NUMBER	**2014:01**
SUBJECT:	**LWIA 13 POLICY REGARDING HANDLING AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)**
PURPOSE:	In an effort to comply with federal requirements and protect an individual's personal information against fraud and identity theft, this Policy implements reasonable and appropriate measures that WIN staff must follow to protect against the loss, misuse and alteration of personally identifiable information ("PII") and other sensitive information under LWIA 13's control.
REPLACES:	**N/A**
REVISION NUMBER:	**N/A**

I. APPLICABLE STATUTES, REGULATIONS AND GUIDANCE:

A. U.S. Employment and Training Administration Training and Employment Guidance Letter No. 39-11 (June 28, 2012);
B. Privacy Act of 1974 (the Privacy Act);
C. Federal Information Security Management Act (FISMA);
D. OMB M-06-15 *Safeguarding Personally Identifiable Information* (May 22, 2006);
E. OMB M-06-19 *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006);
F. Combating Identity Theft: A Strategic Plan (President's Task Force on Identity Theft, May 10, 2006 (www.idtheft.gov);
G. OMB M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007);
H. NIST SP 800-122 *Guide to Protecting the Confidentiality of PII* (April 2010)
I. Tennessee Identity Theft Deterrence Act of 1999, codified at Tenn. Code Ann. §47-18-2101 et seq.

II. BACKGROUND:

As part of its grant activities, LWIA 13 has business reasons to collect or handle personally identifiable information ("PII") relating to WIN and staff; subgrantee and partner organizations and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources. The State of Tennessee and the federal government have issued law and several rules, regulations and guidelines pertaining to the privacy of information.

III. SCOPE:

This Policy applies to all WIN staff, whether or not they deal directly with PII or sensitive information or are granted access to PII or sensitive information during their normal course of employment with WIN. This policy specifies proper controls to safeguard sensitive PII and what to do if sensitive PII has been compromised.

IV. DEFINITIONS:

A. *Mobile Storage Devices* means CDs, DVDs, thumb drives, flash drives, hard drives, USBs, zip drives, or other removable media.

B. *Personally Identifiable Information ("PII")* means information that can be used to directly or indirectly 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.

The State of Tennessee defines *Personal information* as an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:

(i) Social security number;
(ii) Driver license number; or
(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

C. *Sensitive Information* means any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Pursuant to the U.S. Department of Labor, there are two types of PII:

D. *Non-sensitive PII* means 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 sensitive or non-sensitive PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending upon the circumstances, a combination of these items could potentially be categorized as sensitive PII.

E. *Sensitive PII* means information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of sensitive PII include, but are not limited to, social security numbers (SSNs), driver's license number, credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (e.g., fingerprints, voiceprints, iris scans, etc.), medical history, criminal record, financial information (e.g., wage information) and computer passwords.

The differences between sensitive 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. To illustrate the connection between non-sensitive PII and sensitive PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number (or portions thereof), a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of LWIA 13 participants is so important.

V. POLICY AND REQUIREMENTS:

The use of PII at WIN should be consistent with the goals, purposes and mission of LWIA 13. Federal law, guidance and policies require that PII and other sensitive information be protected against fraud and identity theft. Sensitive PII is the most sensitive information that WIN staff may encounter in the course of their work, and it is important that such information remain protected. WIN staff should exercise due care when handling all information encountered in the course of his or her work for WIN, especially PII. Sensitive PII, however, requires special handling because of the increased risk of harm to an individual if it is compromised.

Accordingly, WIN staff shall comply with the following requirements when collecting, using, storing, transmitting and/or disposing of WIN-related PII and other sensitive information ("Sensitive PII").

A. Limit the collection and use of records containing Sensitive PII.

1. Only collect personal information that is necessary to provide the information or services requested by an individual, i.e., request Sensitive PII only when it is absolutely necessary.

2. Only access sensitive PII when you need to know that information, that is, when the need for the information relates to the performance of your official duties.
3. Refrain from browsing files containing Sensitive PII out of curiosity or for personal reasons.

B. Before collecting Sensitive PII, provide notice of the uses and purpose for collection of the personal information (see the attached Privacy Act Notice, which shall be completed by the individual).

C. Restrict access to Sensitive PII to only those employees who need it to perform their official duties.

1. Share Sensitive PII with another WIN employee or subgrantee only if the recipient needs the information to perform his or her official duties;
2. When sharing Sensitive PII with other companies or organizations, including subgrantees/contractors, use Confidentiality Agreements or Ensure confidentiality/nondisclosure requirements are included in contracts between WIN and the contracting agencies.
3. Refer requests for Sensitive PII from members of the public, the media or other outside entities to WIN's Media Relations Specialist.
4. Immediately remove access privileges of former WIN employees.
5. Access to servers housing databases or records containing Sensitive PII shall be restricted to permit only the access needed for the use and support of that application. The server shall be protected by a firewall and other technical security measures.
6. Access to WIN's equipment and WIN's managed IT services shall be limited to those individuals or entities that require access to perform the job duties and functions assigned to him or her.

D. Whenever possible, use the eCMATS or other management information systems' case number or other unique identifiers as a primary identifier for any person, except where the Sensitive PII is required by law and/or permitted by LWIA 13's Policy as described herein. This is recommended for all electronic and paper records used to identify, track, and service individuals.

E. Minimize the Production of Sensitive PII.

1. Do not create unnecessary or duplicative collections of Sensitive PII, such as duplicate or ancillary files.
2. If it is necessary to create duplicate files of Sensitive PII to perform a particular task or project, delete or destroy the duplicate copies pursuant to subsection (J) below as soon as they are no longer needed.
3. When printing, copying or extracting Sensitive PII from a larger dataset, target actions to obtain data on only the specific individuals and the specific data elements necessary to perform the task at hand.

F. Secure Sensitive PII from Access by Unauthorized Individuals at all times.

1. Do not put, and to the fullest extent possible, refrain from requesting Sensitive PII on documents that are widely seen by others, including but not limited to the Intake/Registration Form, file jackets, etc.

2. Never leave records containing Sensitive PII open and unattended on a desk, network printer, fax machine, copier, etc.
3. Physically secure paper records containing Sensitive PII in a locked drawer, cabinet, desk, safe or other secure enclosure when not in use or otherwise under your control.
4. Secure electronic records containing Sensitive PII through the use of access codes. Limit disclosure of the access codes to only those individuals whose official duties require access to such information.
5. Handle, process and/or discuss Sensitive PII in a manner that prevents those who do not need to know the Sensitive PII from looking over your shoulder, eavesdropping or overhearing.
6. Avoid discussing sensitive PII in person or over the telephone when you're within earshot of anyone who does not need to know the information.
7. Position your computer screen so that is minimally visible to people passing by.
8. Use a privacy screen if you regularly access Sensitive PII in an unsecured area where those without a need to know or members of the public can see your screen, e.g., reception area.
9. Lock your computer when away from your station (even if only for a few minutes).
10. Do not choose options that allow your computer to remember passwords.

G. Save, Store or Access Records Containing Sensitive PII only as authorized.

1. Save, store or access Sensitive PII only on WIN-issued or approved equipment[1], WIN-managed secure information technology (IT) services (e.g., servers and secure network drives, for example the "U" drive), and designated locations approved by WIN.
2. Store files containing Sensitive PII in shared access computer drives ("shared drives") only if access is restricted to those with a need to know by permissions settings or passwords. Such files may also be shared if PII is properly redacted or sanitized.
3. <u>Do not</u> access or take records containing Sensitive PII home or to any other offsite location, in either paper or electronic format, unless appropriately secured and otherwise approved by the WIN Executive Director.
4. As a general guideline, <u>do not</u> store, save or access records containing Sensitive PII on personally-owned equipment (e.g., personal computer), mobile storage devices or non-WIN managed IT services (e.g., Yahoo mail).
5. If Storing Sensitive PII on a Mobile Storage Device is absolutely necessary for business reasons, encrypt such information and physically secure such device at all times. Encryption is the process

[1] WIN-issued or approved equipment is already equipped with security functions (i.e., Windows Encrypting File System (EFS) and server protections).

of converting data into a format that cannot be read by others[2]. WIN's Information Technology department will be responsible for purchasing encryption software and/or devices. Please contact WIN's IT Manager for assistance with encrypting information. In cases where encryption is not possible, Sensitive PII shall not be stored on the mobile storage device.

H. Secure Records Containing Sensitive PII when in Transit.

1. When emailing records containing Sensitive PII outside of the WIN network (e.g., emailing from a WIN email address to a non-WIN email address), send the Sensitive PII within an encrypted attachment and provide the password separately (e.g., by phone or in person). As a last resort, the password can be sent in a separate email, but never in the same email containing the attachment.
2. When sending records containing Sensitive PII via a fax machine, alert the recipient prior to faxing so that the recipient can ensure that the transmission is not left unattended
3. Do not mail, share or courier records containing Sensitive PII on mobile storage devices unless the data is encrypted.
4. Do not transfer or return failed hard drives to a vendor for warranty if the device was ever used to store Sensitive PII. Instead, sanitize or destroy the media.
5. Do not leave Sensitive PII on voice mail messages.
6. Do not require an individual to send his or her Sensitive PII over the internet or by email, unless the Sensitive PII is encrypted.
7. Prior to replying or forwarding an email, remove any Sensitive PII from the email chain.

I. Dispose of records containing Sensitive PII in a Secure Manner when those records no longer need to be retained pursuant to applicable document retention policies.

1. Shred printed material containing Sensitive PII. Do not recycle papers containing Sensitive PII.
2. Permanently erase or destroy Sensitive PII from mobile devices, computer drives and other electronic storage devices before re-issuing them for use.
3. Sanitize or physically destroy mobile storage devices that contain Sensitive PII in a manner that protects the confidentiality of the information.

VI. REPORTING PRIVACY INCIDENT(S):

A privacy incident is defined as the actual or potential loss of control, compromise, unauthorized disclosure, acquisition or access to Sensitive PII in physical or electronic form.

Immediately report any privacy incident, whether suspected or confirmed, to your immediate supervisor. If your immediate supervisor is unavailable, or if there is a

[2] Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.

potential conflict of interest, report the incident to the Deputy Director of Operations. Do not further compromise the information, such as forwarding compromised information (e.g., SSN, full name, birthdate, etc.) when reporting an incident. Upon receipt, the Supervisor shall immediately report such privacy incident to WIN's IT Manager and Deputy Director of Operations.

The IT Manager will take such action as he or she determines appropriate to stop such risk including but not limited to the immediate suspension of network access, access to administrative systems and/or access to the Internet.

In addition, the Deputy Director of Operations shall notify individual(s) whose information is or has been put at risk of identity theft or other harm when Sensitive PII has been acquired, or is reasonably believed to have been acquired, by an unauthorized person. Specifically, notification shall be provided when there are indications that:

1. The information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information;
2. The information has been downloaded or copied; or
3. The information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported to LWIA 13.

VII. REPORTING EMPLOYMENT TERMINATION:

Upon the cessation or termination of an individual's employment with WIN, for any reason, the appropriate Manager and/or HR liaison shall immediately inform WIN's Fiscal Representative, IT Manager and Manager of Performance and Quality Assurance of the employment change. The IT Manager and Performance and Quality Assurance Managers shall immediately disable said employee(s) access to WIN's network, administrative systems and other sites under WIN's control that contain PII (e.g., State's electronic system).

VIII. CONSEQUENCES FOR NON-COMPLIANCE:

Failure to comply with the requirements identified in this Policy, or any improper use or disclosure of Sensitive PII for an unauthorized purpose, may result in disciplinary actions, including and up to termination of employment. In addition, the employee may be subject to civil and criminal sanctions pursuant to state and federal law.

IX. EFFECTIVE DATE: This Policy shall be effective upon the date referenced above, until further notice.

X. INQUIRIES: Please contact WIN's Deputy Director of Operations with any questions or concerns regarding this Policy.

Attachment: Privacy Act Notice

WORKFORCE INVESTMENT NETWORK

PRIVACY ACT NOTICE

Federal and state laws require that you be furnished this Notice because you are being asked to provide personal identifying information about yourself, including but not limited to name, social security number (SSN), date of birth, employment information, telephone number(s), address(es), income information, information needed for identification verification, and other personal information, necessary to complete the application for services offered by WIN.

Authority: Workforce Investment Act. Sections 101, 188(a)(5) and 189(h) of the Workforce Investment Act provide that, in order to receive services pursuant to the WIA, an individual must present proof of United States citizenship (or authorization to work in the United States), age, and where applicable, Military Selective Service Registration and documentation substantiating other program eligibility criteria

Purpose: Your personal identifying information (including SSN) will be used by and disclosed to WIN personnel, partners and contractors or other agents who need the information to assist in activities related to Workforce Investment Act (WIA) services.

Routine Uses: Your SSN is used to verify your identity, and as an account number (identifier). The personal identifying information (including SSN) will be used for processing your application to determine your eligibility for WIA services. Your personal information will be disclosed to WIN contractors for purposes of administration of WIN programs, for enforcement purposes, for use in connection with audits or other investigations. Also, your SSN and other personal identifying information will be used to report services provided to you by WIN to the State of Tennessee Department of Labor and Workforce Development or other local, state and/or federal government agencies. Your personal identifying information (including SSN) will be retained for as long as is required by applicable law or regulation.

Disclosures: Your disclosure of this personal identifying information (including SSN) for this purpose is voluntary. However, your failure to provide the requested information may delay or prevent the processing of your application for WIA services.

By signing below, I certify that I have read and understand this Privacy Act Notice.

Printed Name: _____

_____

Signature Date