

**PEE DEE INSTRUCTION NUMBER:**

**WIA-14-002**

**TO:**

**Pee Dee Local Workforce Development Area Grantees**

**SUBJECT:**

**Confidentiality Statement**

**ISSUANCE DATE:**

**June 17, 2015**

**EFFECTIVE DATE:**

**July 1, 2015**

---

**Purpose:** The purpose of this instruction is to transmit the LWDA's policy regarding the confidentiality of customer's personally identifiable information. The Confidentiality Agreement between the Pee Dee Local Workforce Development Area (LWDA) and SC Department of Employment and Workforce (SCDEW), the SCDEW Personal Identification Information (PII) Handling and Confidentiality Policy, and the Confidentiality Statement for all WIOA-funded employees are attached for reference. This instruction supersedes WIA Instruction #04-003.

**Background:** Releasing information improperly is a serious offense and carries with it penalties under the law. In acknowledgement of this fact, the Pee Dee Workforce Investment Area released an instruction regarding confidentiality in Program Year 2004. That instruction requires that information obtained by WIA-funded staff in the course of their work with an individual be held confidential and prescribed specific (and limited) instances in which information could be released. Recently, the LWDA has entered into agreement with SCDEW to ensure that individuals with access to SCDEW Workforce Information Portal have signed and agreed to confidentiality. In the process of the determination of eligibility for Workforce Innovation and Opportunity Act (WIOA) programs and in the delivery of WIOA program services, LWDA staff, as well as LWDA grantee staff, may have access to individuals' Confidential Information from the SCDEW portal and other Personally Identifiable information (PII). SCDEW requires that the LWDA:

- Instruct all personnel having access to the disclosed information about confidentiality requirements, the requirements of this Agreement, and the sanctions specified by South Carolina law for unauthorized disclosure of confidential information;
- Instruct all personnel, including contractors and service providers having access to the disclosed information to sign a statement of Agreement that they will adhere to DEW's confidentiality requirements and procedures; and
- Instruct all personnel to dispose of information disclosed or obtained, and any copies thereof made by the recipient agency, entity, or contractor, after the purpose for which the information is disclosed is served, except for disclosed information possessed by any court. Disposal means the return of the information to DEW or destruction of the information, as instructed and approved by DEW. If destruction of the information is requested by DEW, LWDA will destroy the information within an approved timeframe. LWDA will provide a certificate of destruction.

The requirements under the LWDA's agreement with DEW will apply to all personally identifiable information obtained in the course of providing a service or administering a program under the Workforce Innovation and Opportunity Act (WIOA).

**Action:** All Pee Dee LWIA grantee staff funded with WIOA funds must agree to and sign the attached Confidentiality Statement. The signed statement must be submitted to the Pee Dee LWDA by July 7, 2015.

**Inquiries:** Questions regarding this instruction should be directed at Joette Dukes at (843) 669-3138.

  
\_\_\_\_\_  
Joette Dukes  
Workforce Development Director

Attachment

## **PEE DEE WORKFORCE DEVELOPMENT AREA (LWDA) CONFIDENTIALITY AGREEMENT**

I understand that the Local Workforce Development Area (LWDA) has received and will continue to receive confidential information from the South Carolina Department of Employment and Workforce ("DEW") pursuant to the attached Agreement between the LWDA and DEW and that DEW has a policy regarding Personal Identification Information (PII).

Information obtained from any employing unit or individual in the course of administering policies and procedures of the Workforce Innovation and Opportunity Act (WIOA) by an employee of the Pee Dee LWDA, adult, dislocated worker or youth programs shall be held confidential. This means that all facts learned in the course of administering WIOA services have been entrusted to the LWDA's WIOA programs and shall not be disclosed or open to the public in any manner.

I have reviewed the terms of the Agreement and the PII Policy and agree to:

- use confidential information only as authorized;
- safeguard all confidential information in accordance with this agreement and DEW's confidentiality rules, including DEW's PII policy and applicable federal and state laws and regulations; and
- not disclose this information without prior written authorization.

I understand the confidentiality terms of the Agreement survive the duration of the Agreement.

I further understand that unauthorized disclosure of confidential information could subject me to the penalties provided under S.C. Code Ann. § 41-29-150, in addition to other penalties and/or fines under state and/or federal law and regulations.

By my signature below, I certify I have read the attached Confidentiality Agreement and the PII Policy and will abide by their terms.

Employee Name (Typed)\_\_\_\_\_ Date\_\_\_\_\_

Signature\_\_\_\_\_ Date\_\_\_\_\_

## **CONFIDENTIALITY AGREEMENT**

### **BETWEEN**

**THE SOUTH CAROLINA DEPARTMENT OF EMPLOYMENT AND WORKFORCE**

### **AND**

**PEE DEE WORKFORCE DEVELOPMENT AREA**

This Confidentiality Agreement is entered into as of June 1, 2015, by and between the South Carolina Department of Employment and Workforce (DEW) and Pee Dee Workforce Development Area ("LWDA").

**PURPOSE:** The purpose of this Agreement is to address the confidentiality requirements for LWDA's to use the DEW Workforce Information Portal in order to have limited access to unemployment insurance (UI) claimant data that will be used to determine an individual's potential eligibility for training and employment services programs under the Workforce Investment Act ("WIA") and the Workforce Innovation and Opportunity Act ("WIOA"), effective July 1, 2015, and for LWDA outreach for employment and training opportunities.

## **ARTICLE I**

### **DURATION OF AGREEMENT**

This Agreement shall take effect upon the signatures of both parties and shall terminate at the end of the third program year, June 30, 2018. This agreement may be renewed as permitted by federal and state law. The confidentiality requirements of this Agreement shall survive the term of this Agreement.

This Agreement may be amended in the event of changes in federal or state law, including but not limited to changes regarding the confidentiality of Unemployment Compensation (UC) information.

## **ARTICLE II**

### **APPLICABLE CONFIDENTIALITY LAWS AND REGULATIONS**

The parties agree to comply with all applicable federal and state laws, regulations, and guidance, including but not limited to:

1. The Privacy Act of 1974, 5 U.S.C. §552a;
2. The Family Privacy Protection Act, S.C. Code Ann. §§ 30-2-10, *et. seq.*;
3. The South Carolina Department of Employment and Workforce law, S.C. Code Ann. §41-27-10, *et seq.*, including §§ 41-29-150 through 170;
4. Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information, 20 C.F.R. Part 603;

5. Tax Information Security Guidelines for Federal, State and Local Agencies, IRS Publication 1075;
6. Office of Management and Budget M-07-16; and
7. SC Department of Employment and Workforce Personal Identification Information (PII) Handling and Confidentiality Policy.

## **ARTICLE III**

### **DEFINITIONS**

#### **1. CONFIDENTIAL INFORMATION**

Confidential information includes information in DEW's records that pertain to the administration of UI benefits, including wage reports. See 20 C.F.R. Part 603.2. The types of data include, but are not limited to, an individual's and/or employing unit's:

1. Name, Address, Email, and Phone Number;
2. Last four digits of Social Security Number;
3. Whether an individual is receiving Unemployment Insurance;
4. Most recent employer;
5. Any identifying particulars that in combination with publicly accessible information would identify the individual or employing unit.

#### **2. PERSONALLY IDENTIFIABLE INFORMATION**

**Personally identifiable information (PII) is the information that can be used to uniquely identify, contact, or locate specific individuals. Examples of PII elements include: name, address, date of birth, race, gender, telephone number, official government issued identification numbers, Social Security benefit data, tax data, and financial, medical and employment information.**

## **ARTICLE IV**

### **INFORMATION DISCLOSED PURSUANT TO THIS AGREEMENT**

This Agreement is limited to the disclosure of information that is received by LWDA for the purposes outlined in this Agreement only.

Information disclosed pursuant to this agreement includes information contained in the following data systems:

DEW Workforce Information Portal ("Portal").

## **ARTICLE V**

### **PURPOSES FOR REQUESTING INFORMATION**

Information that is requested or received by LWDA, pursuant to this Agreement, is limited to the information permitted by federal and state law and to the information needed by LWDA staff for determining an individual's potential eligibility in WIA or WIOA programs for training and employment services and for LWDA outreach for employment and applicable training opportunities.

## **ARTICLE VI**

### **REQUIRED SAFEGUARDS**

Both the recipient agency/entity and the individual recipient of confidential information and PII are subject to several required safeguards.

The individual recipient of any confidential information is required to:

1. Use the disclosed information only for purposes authorized by law and consistent with this Agreement;
2. Store the disclosed information in a place physically secure from access by unauthorized persons;
3. Undertake precautions to ensure that only authorized personnel have access to disclosed information in hardcopy form.
4. Store and process disclosed information maintained in electronic format in such a way that unauthorized persons cannot obtain the information by any means; and
5. Undertake precautions to ensure that only authorized personnel are given access to disclosed information stored in computer systems.
  - a. Precautions include not saving UC information and PII exported from the Portal into spreadsheets or other documents in shared folders with unauthorized personnel.

The agency/entity recipient of any confidential information and PII is required to:

1. Instruct all personnel having access to the disclosed information about confidentiality requirements, the requirements of this Agreement, and the sanctions specified by South Carolina law for unauthorized disclosure of confidential information.
2. Sign an acknowledgement that all personnel, including contractors and service providers, having access to the disclosed information have been instructed in accordance with this Agreement and will adhere to DEW's confidentiality requirements and procedures. (See Attachment A).
  - a. It is the understanding pursuant to this Agreement that the LWDA will be working on this project exclusively. Prior to any additional personnel, contractors, or service providers of the LWDA joining this project, the LWDA will notify DEW so the acknowledgement can be executed prior to any disclosure to the additional personnel.
3. Dispose of information disclosed or obtained, and any copies thereof made by the recipient agency, entity, or contractor, after the purpose for which the information is disclosed is served, except for disclosed information possessed by any court. Disposal means the return of the information to DEW or destruction of the information, as instructed and approved by

DEW. If destruction of the information is requested by DEW, LWDA will destroy the information within an approved timeframe. LWDA will provide a certificate of destruction.

4. Maintain a system sufficient to allow an audit of compliance with the requirements of this Agreement.

## ARTICLE VII

### REDISCLASURE OF CONFIDENTIAL UC INFORMATION

**LWDA is not authorized to redisclose any confidential information without prior authorization from DEW. Specifically, LWDA is not authorized to disclose the unemployment insurance status.**

Should the situation arise where LWDA seeks authorization to redisclose confidential information from the Portal, there are limited exceptions that DEW authorizes redisclosure of confidential UC information. The only exceptions are as follows:

1. To the individual or employer who is the subject of the information;
2. To an attorney or other duly authorized agent representing the individual or employer;
3. In any civil or criminal proceedings for or on behalf of a recipient agency or entity;
4. In response to a subpoena as provided in 20 C.F.R. § 603.7;
5. To an agent or contractor of a public official only if the person redisclosing is a public official, if the redisclosure is authorized by the State law, and if the public official retains responsibility for the uses of the confidential UC information by the agent or contractor;
6. From one public official to another if the redisclosure is authorized by the State law;
7. When so authorized by Section 303(e)(5), SSA, (redisclosure of wage information by a State or local child support enforcement agency to an agent under contract with such agency for purposes of carrying out child support enforcement) and by State law; or
8. When specifically authorized by a written release that meets the requirements of 20 C.F.R. § 603.5(d) (to a third party with informed consent).

Information redisclosed under subsections (5) & (6) above are also subject to the safeguards outlined in Article V. Required Safeguards of this Agreement.

The requirements of this Article do not apply to disclosures of UC information to a Federal agency which DEW has determined, by notice published in the Federal Register, to have in place safeguards adequate to satisfy the confidentiality requirement of Section 303(a)(1), SSA.

## ARTICLE VIII

### METHODS AND TIMING OF REQUESTS FOR INFORMATION

This Agreement must include “the methods and timing of requests for information and responses to those requests, including the format to be used.” (20 C.F.R. § 603.10(b)(1)(iii)). DEW will provide a user name and password to the authorized employees that will access the Portal.

LWDA agrees to safeguard this information as described in federal and state law, including but not limited to 20 C.F.R. §603. LWDA will instruct the designated employees, designated contractors, and designated service providers that information is provided so that the disclosure of this information is limited to the purpose of this agreement and limited to only necessary employees, contractors, and service providers. LWDA will agree to limit the access of the data to designated employees, designated contractors, and designated service providers that will sign the Confidentiality Agreement (See Attachment A).

In the event the designated employee is discharged or leaves his or her position with LWDA, LWDA insures the former employee will not have access to the information contained therein, and **LWDA will notify DEW that the former employee's user name and password should be revoked.**

Access to confidential information will only be granted through the Portal Information used from the Portal in any document and for any purpose is considered confidential and the provisions of this Agreement extend to all electronic, oral, and/or printed information. **Individuals with access to the Portal are prohibited from transferring DEW data to removable media and are prohibited from accessing the portal from personal devices.**

The confidentiality requirements of this Agreement survive the duration of this Agreement.

## **ARTICLE IX**

### **COSTS FOR FURNISHING INFORMATION**

Pursuant to 20 C.F.R. § 603.5, LWDA will not pay for the costs to DEW for furnishing information as LWDA is performing services that are part of providing workforce services to the local area.

## **ARTICLE X**

### **ON-SITE INSPECTIONS**

DEW reserves the right to conduct on-site inspections to assure that the requirements of State law and this Agreement are being met.

## **ARTICLE XI**

### **BREACH, ENFORCEMENT, TERMINATION AND MODIFICATION**

**Breach:** If any employee or agent thereof, fails to comply with any provision of this Agreement, the Agreement must be suspended, access to the Portal denied, and further disclosure of information (including any disclosure being processed) prohibited, until DEW is satisfied that corrective action has been taken and there will be no further breach. In the absence of prompt and satisfactory corrective action, the agreement must be canceled, LWDA's access to the Portal will be revoked, and LWDA must be required to surrender to DEW all confidential UC information or PII (and copies thereof) obtained under the Agreement which has not previously been returned to DEW, and any other information relevant to the Agreement, or provide a certificate of destruction at DEW's request.



Both parties agree that each party shall be liable for its own acts and omissions, and the acts and omissions of its employees, agents and officers, and nothing within this agreement shall impute or transfer liability to the other party. This provision shall survive the expiration or termination of this Agreement, regardless of the reason for termination.

**Enforcement:** Pursuant to federal and state law, DEW must hold confidential and must not publish information that reveals an individual's or employing unit's identity and/or any identifying particulars. In the event an employee or member of DEW violates a state provision, the person must be fined not less than \$20.00 or more than \$500.00 and/or imprisoned for not longer than 90 days. SC Code Ann. § 41-29-150. DEW is permitted to disclose information under limited circumstances, including an agency or entity to which disclosures are permitted by federal statute or regulation. SC Code Ann. § 41-29-170(B)(1)(c).

DEW is permitted to disclose this information with conditions as outlined by federal regulation to LWDA, as described in this agreement. The confidentiality requirements and penalties that apply to DEW staff extend to LWDA employees covered under this Agreement.

**Termination and Modification:** This Agreement may be terminated by either party upon written notice, or immediately due to a breach or change in federal or state law. Should either party terminate this Agreement, LWDA employees shall no longer have access to confidential information from the DEW Workforce Information Portal and will be required, at DEW's discretion, to return or destroy any printed information and/or electronic files to the Office of General Counsel for DEW or provide a certificate of destruction, at DEW's request.

In the event there is a change in federal and or state law that nullifies any portion of this Agreement, the Agreement is immediately terminated and a new Agreement under the current law may be executed.

In addition, this Agreement is immediately terminable by DEW if it determines that the safeguards in the agreement are not adhered to by LWDA.

DEW reserves the right to deny access to an area or to individual employees of an area in the event of an investigation of a potential breach of this Agreement.

No amendments, modifications, changes, additions or deletions of the Agreement shall be valid unless in writing, signed by both parties and attached to this Agreement.

**SUCCESSORS AND ASSIGNS:** DEW and LWDA each binds itself, its successors, executors, administrators, and assigns to the other party with respect to these requirements, and also agrees that no party shall assign, sublet, or transfer its interest in the Agreement without the written consent of the other parties.

**ENTIRE AGREEMENT:** This Agreement constitutes the entire Agreement between the parties. The contract is to be interpreted under the laws of the State of South Carolina.

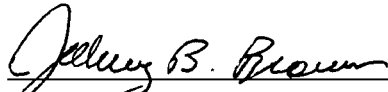
The signatories hereunder warrant and declare that they are duly authorized to execute this Agreement by virtue of their position and title.

South Carolina Department of  
Employment and Workforce

\_\_\_\_\_  
Cheryl M. Stanton, Executive Director

\_\_\_\_\_  
Date

Pee Dee LWDA

  
\_\_\_\_\_  
Johnny B. Brown, Executive Director

6/4/2015  
\_\_\_\_\_  
Date



## **SC Department of Employment and Workforce Personal Identification Information (PII) Handling and Confidentiality Policy**

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### **1.0 Overview**

The South Carolina Department of Employment and Workforce (DEW) Personal Identification Information (PII) Handling Policy was developed to ensure a secure, reliable, and sustainable work environment for conducting agency business. All Internal Systems, Internet, Intranet and Extranet-related systems; including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web (WWW) browsing, Secure File Transfer Protocol (SFTP), and File Transfer Protocol (FTP) are the property of DEW. These systems are to be used for normal business purposes in serving the interests of the Agency, its customers and its partners. The Division of Information Technology (DoIT) is committed to protecting DEW systems from illegal or damaging actions from individuals who knowingly or unknowingly commit such actions.

Accordingly, DEW and DoIT will protect the confidentiality of, and restrict access to, personal information and social security numbers of employees, contractors, claimants and other individuals to only those who have a legitimate business reason to access documents containing PII data.

Effective security is a team effort involving the participation and support of every individual who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

### **2.0 Purpose**

The purpose of this document is to define the PII Handling Policy. The PII Handling Policy addresses the protection of sensitive information from disparate sources. Violation of, or noncompliance with, this policy exposes DEW and partner agencies to the risk of exposure or theft of confidential agency-owned data. DoIT is committed to protecting all DEW owned or supported systems and the confidential data contained on these systems.

### **3.0 Scope**

This policy applies to full-time equivalent (FTE), temporary grant, hourly employees, contractors, consultants, and all other workers at DEW with access to DEW networks and/or information.

### **4.0 Definitions**

- **PII** - Personally identifiable information (PII) is the information that can be used to uniquely identify, contact, or locate specific individuals. Examples of PII elements include: name, address, date of birth, race, gender, telephone number, official government issued identification numbers, Social Security benefit data, tax data, and financial, medical and employment information.
- **SSN** – Social Security Number
- **SSA** - Social Security Administration
- **IRS** - Internal Revenue Service
- **DOL** - Department of Labor
- **DHHS** - Department of Health and Human Services
- **OCSE** - Office of Child Support Enforcement
- **DSS** - Department of Social Services
- **DOR** - Department of Revenue
- **DMV** - Department of Motor Vehicles

### **5.0 Compliance**

DoIT will monitor and report all violations of the PII Handling Policy. All violations will be promptly reported to the user and DEW management to address on a case-by-case basis. In the case of a violation that includes Federal Information, DEW is required to report the incident to the appropriate Federal Agencies.

### **6.0 Responsibility**

Working with and protecting PII is an essential part of every job function within DEW. PII comes from many different sources including, but not limited to, Banks, the IRS, DOL, SSA, DHHS, DMV, DSS, OCSE, DOR, employers, employees and claimants.

PII also includes Unemployment Compensation information which reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with other publicly available information to reveal any such particulars. *See* 20 CFR § 603.

In addition to the applicable laws governing PII, there are regulatory requirements on how this data is handled, protected, disposed of, and transmitted. Violation of the laws governing the protection of this data exposes the violator to criminal and civil liability, including penalties of fines and imprisonment.

It is the responsibility of management and the Division of Information Technology to:

- Train users in the handling, protection and disposal of PII. Please see the Security Training policy for more information.
- Control access to PII and the systems on which it resides.
- Protect the network and servers of DEW involved in the use and handling of PII.
- Report on the digital access, disposal, or loss of this data.

It is the responsibility of DEW staff, contractors, and partners to:

- Completely read, understand and follow the guidelines in agency policies and all provided training materials regarding PII.
- Report any witnessed violations of this or other policies, breach of security or loss of data to an appropriate level supervisor, manager, or security officer within the agency.

## **7.0 PII handling**

### **Physical PII**

- All locations where sensitive data is stored should be secured physically. Office spaces, storage closets, and file cabinets should all be locked with a key possessed only by DEW staff or partners.
- PII should not be left plainly visible on desks, printers, or fax machines. Printed documents with PII should never be freely accessible and/or unattended.
- A cover sheet should always be used when transmitting PII via fax. This cover sheet should include the intended recipient, contact instructions if the fax is received by someone other than the intended recipient, and a prominent warning such as the following:
  - “PERSONAL INFORMATION – If you are not the intended recipient of this fax you are prohibited from sharing, copying, or otherwise using or disclosing its contents. If you received this fax in error, please notify the sender immediately and destroy this fax and any attachments without reading, forwarding, saving or disclosing them.”
- Hard copies of files containing PII that are mailed or sent via courier should always use sealed, privacy guarded envelopes.

### **Electronic PII**

- PII must only be used and stored on equipment approved by DoIT.
- All computers must be running operating systems and antivirus software that are approved by DoIT and up to date.
- All agency printers, scanners, copiers, and fax machines will be configured not to store any documents after they have been printed or scanned.
- All mobile data storage devices must be encrypted with approved encryption software. Please see the Mobile Device and Laptop Security Policies for more information.
- All computer monitors must be obscured from public view.



- Physical access to computer equipment must be restricted from the public as much as possible.

#### E-mail and Transmission

- PII should never be sent to third party file hosting, transfer services or social networking sites. **Never use your personal email or other accounts to transmit PII.**
- PII should never be transmitted via email or File Transfer Protocol (FTP) without being encrypted. The preferred method of sending PII data to authorized recipients is the Agency Secure File Transfer Protocol (SFTP) server. More information can be found on iConnect, [http://iconnect/index.php?title=Office\\_of\\_Information\\_Security#FAQ](http://iconnect/index.php?title=Office_of_Information_Security#FAQ)
- All FTP transmissions of PII leaving the agency must be encrypted point to point with a Virtual Private Network (VPN) tunnel or SFTP.

## 8.0 Prohibited Practices

Employees who have access to PII are prohibited from:

- Publicly displaying or otherwise unlawfully disclosing any person's PII.
- Using PII as a primary account number or printing PII on any identification badge, membership card, permit, or license.
- Mailing documents containing PII where the number is visible on or from outside the envelope or packaging.
- Including more than four sequential digits of a social security number on any document mailed unless it is specifically permitted by law, regulation or court order; or is sent as part of an application or enrollment process; or is sent to establish, confirm, amend, or terminate an account or benefit policy.
- Transmitting PII over the Internet or a computer system or network unless the connection is secure, or the transmitted data is encrypted.
- Requiring an individual to use or transmit all or more than 4 sequential digits of his or her SSN to gain access to an internet website or a computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal ID number or other authentication device is also required to gain access.
- Utilizing their SSNs as passwords for access to computer systems.

## 9.0 Disposal of PII

Documents that contain SSNs or any other PII must be properly destroyed when those documents no longer need to be retained to conduct DEW business. Paper documents containing PII should be shredded by using shredders that use crosscutting (both horizontal and vertical shedding/cutting). Electronic storage devices such as hard drives, flash drives or phones must be wiped with agency-approved software and then sent to an approved disposal facility.

## 10.0 Confidentiality

DEW employees and contractors are required to keep all data belonging to the Federal Government, DEW, and its partners secure. Data handled in the course of job duties may not be disclosed or discussed with anyone who is not authorized to receive the information. This data should also never be accessed, used, stored, or transmitted for personal purposes or on personal devices or services. All DEW employees and contractors are responsible for the security and protection of this data.

## 11.0 Enforcement

Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including termination. Additionally, noncompliance will be reported to law enforcement, as appropriate, and may result in criminal prosecution, civil litigation, restitution, fines, and/or penalties.

Alleged or suspected violations of the PII Handling Policy should be reported to DoIT or to the Internal Audit Fraud, Abuse and Waste hotline. Please see the Internal Audit and Quality Control page on iConnect for methods to contact the hotline. All alleged or suspected violations will be formally reviewed. Note that all violations involving PII obtained from a Federal Government Agency must be reported by DEW to the appropriate Federal Agencies.

Any employee who abuses the DEW's computing, information, or communications resources may also be subject to civil action and/or criminal prosecution. **DEW will pursue criminal and civil prosecution of violators when appropriate.** Individuals will also be responsible for any financial loss to the DEW that results from inappropriate use of information technology resources.

***The "PII Handling Policy" is agreed to and abided by as consideration for continued employment at DEW. Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including termination, may involve civil or criminal litigation, and may involve restitution, fines, and/or penalties.***



South Carolina Department of Employment and Workforce  
Personal Identification Information (PII) Handling and Confidentiality Policy  
Technology Access Rights and Obligations  
User Agreement Acknowledgement

As a user of the South Carolina Department of Employment and Workforce (DEW) data and resources, I agree to abide by the Personal Identification Information (PII) Handling and Confidentiality Policy and the following terms and guidelines as they relate to the policy established:

1. I will protect DEW confidential data, facilities and systems against unauthorized disclosure and/or use.
2. I will maintain all computer access codes in the strictest of confidence and immediately change them if I suspect their secrecy has been compromised.
3. I will be accountable for all transactions performed using my computer access codes.
4. I will not disclose any confidential information other than to persons authorized to access such information as identified by my section supervisor.
5. I will not access any DEW confidential data for personal use.
6. I will report activity that is contrary to the provisions of this agreement to my supervisor and DoIT.
7. I agree to report to DoIT any suspicious network activity or security breach.

***Privacy Expectations***

DEW actively monitors network services and resources, including, but not limited to, real time monitoring. Users should have no expectation of privacy. These communications are considered to be DEW property and may be examined by management for any reason including, but not limited to, security and/or employee conduct.

I acknowledge that I must adhere to this policy as a condition for receiving access to DEW data and resources.

I understand the violation or disregard of any of these guidelines, statutes or policies may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with DEW, and any other appropriate legal action, including possible criminal prosecution under State and Federal statutes.