SWIS Data Management Operational Guide

(Processing, Access, Storage and Security)

REVISION HISTORY

Date	Version	Description	Author
	0.1	First Draft	

TABLE of CONTENTS

PART III: PROCESS

TABLES

PART I: SUMMARY

1. SUMMARY

1.1 SWIS Overview

The States Wage Interchange System (SWIS) is a medium via which participating states collaborate in an effort to streamline the exchange of interstate wage data, efficiently and securely. The system facilitates the exchange of wage information in a manner that minimizes the burden to state unemployment insurance programs associated with responding to requests for wage data ensures the security of the transactions involving individual wage data and produces the data in an efficient, effective manner. Each state has two primary parties involved in SWIS transactions:

> 1.1.1 A **State Unemployment Insurance Agency (SUIA)**, the *supplier* of wage information; and
> 1.2.2 A **Performance Accountability and Customer Information Agency (PACIA)**, the *consumer* of wage information and the entity identified by the Governor as being responsible for performance accountability and eligible training provider certification.

The SWIS Data Sharing Agreement (DSA) has three (3) PACIAs that signed the agreement and are responsible for submitting SWIS requests for their agency for Federal Reporting: Workforce, Education and Vocational Rehabilitation.

As described in the SWIS Guidelines, requests for wage data made to the SWIS are transmitted through the SWIS Clearinghouse, a computerized network operated by the SWIS Operations Contractor. Conduent, Inc. (Conduent) currently serves as the SWIS Operations Contractor. Conduent assists states with the design and installation of necessary computer hardware and software to operate the system, handles the day-to-day transfer of wage data from state to state, and provides ongoing technical support to the participating states. Overall, administration of the SWIS Clearinghouse is the responsibility of the National Association of State Workforce Agencies (NASWA), a not-for-profit organization with an extensive background in the operation of state unemployment insurance and employment service programs.

The SWIS is categorized as a sensitive system due to the nature of the data being transmitted, to include social security numbers (SSN) and other personal identifiable information (PII). It is to this effect that it is a U.S. Department of Labor (USDOL) regulation for all participants to conform to guidelines set forth to include handling such sensitive data with acceptable level of security, in order to maintain the confidentiality, integrity and availability of such data. SWIS users are required to sign an acknowledgment form after reading the SWIS standards and guidelines document before being granted access to systems used for SWIS data processing and storage or viewing any such data.

1.2 Objective

This document is intended to capture _____ processes and policies as it relates to the SWIS data management, by way of documenting the personnel roles, security polices and technical details pertaining to the wage request and transmission process.

2. ROLES AND RESPONSIBILITIES

Table 1 - Roles and Responsibilities

Roles	Personnel	Responsibilities
Oversight (System Owner)		Primary Contact representing the Agency as it relates to SWIS administration and signed agreements
Oversight (Information Technology)		Information Technology direction and management
Oversight (Compliance)		Compliance and Independent Assessment
Information Security		Information Security review, recommendation and documentation
Program Support (Agency)		SWIS System and Server Administration
Program Support (Contractor)		
Vendors	→ →	Data Maintenance and Case management Mainframe or network application hosting and system administration, network connection to SWIS Clearinghouse and data security

PART II: POLICY

3. SECURITY OBJECTIVES

The SWIS data processing and storage system implementation at ______ utilizes Server and Mainframe components. As determined by utilizing National Institute of Standards and Technology (NIST) Federal Processing Standards-199 (FIPS-199) system categorization standards, the SWIS Security Categorization (the security category for the SWIS data processing and storage system) is: [(Confidentiality, Medium), (Integrity, Medium), (Availability, Medium)], resulting in an overall "Medium" system and sensitivity. As a result, it is essential that SWIS data processing and storage policy, procedures, and controls are established and maintained to support due care, due diligence, and adequate security posture.

The following subsections contain the agency's system-specific security controls as it relates to any components used to process and store SWIS data, to include personnel and technology. The SWIS security controls provide system-specific direction for ensuring compliance with the medium security control baseline prescribed in NIST SP 800-53, as well meet and/or exceed USDOL requirements per the SWIS data sharing agreement.

SWIS data processing and storage systems rely on ______ and IT agency policy and procedures. All systems shall comply with applicable controls prescribed in the medium security control baseline set forth in NIST SP 800-53, Revision 4, as well as any applicable _______ Defined Values for a medium security baseline and best practices.

The Information Security and Compliance oversight shall ensure SWIS data processing and storage policy and procedures are reviewed annually and updated at least biennially, or with any significant changes to the overall system and/or process.

****Reference _____ IT Security Policies →   and _______ Policies → ****

3.1 Access Control Policy (NIST security control *AC-1, AC-5, AC-6, CM-5, PE-1)*

Logical and physical access to SWIS data processing and storage systems shall be granted to individuals based on a valid need-to-know basis that is determined by the System Owner and satisfies all personnel security criteria and intended system usage. Remote access for privileged functions shall be formally authorized by the System Owner on a case-by-case basis and only for compelling operational needs.

Individuals approved for access to SWIS data processing and storage systems shall not be granted access to the system until they have reviewed the SWIS standards and Guidelines documents, signed the SWIS PACIA and SUIA access forms(as relevant), and received appropriate training. Access authorizations shall comply with roles-based information access and permissions to ensure least privilege and the separation of duties to eliminate conflicts of interest in the responsibilities and duties of individuals.

***For details on access request and approval process, refer to Appendix B

3.1.1 Account Management (NIST security control AC-2)

SWIS data processing and storage System Support Staff responsible for administering access shall create, activate, modify, disable, and archive user accounts in accordance with the _____ and _____ Access Request and Approval Process.

3.1.2 Account, Physical Access, and User Activity Review

System administrators/custodians shall review user activity audit logs with respect to the enforcement and usage of security access controls on a monthly basis (and bi-weekly for users with significant roles and responsibilities) and upon personnel termination, transfers, or reassignments. The custodian(s) shall document, investigate, and report suspicious activities or anomalies identified during his/her review of user accounts and user activity in coordination with the ISO. With regard to physical access to data center(s), the Contractor Information Security Personnel shall review the SWIS physical access list and authorization credentials for contractor facilities on a quarterly basis and upon personnel termination, transfers, or reassignments, reporting any suspicious activities or anomalies identified during his/her review.

3.1.3 **Auditing Policy** *(*NIST security control

Auditable events within any SWIS data processing and storage systems shall be reviewed annually or upon significant changes to the system.

3.1.4 Security-Related Events and Audit Record Content (NIST security control)

The SWIS data processing and storage systems shall generate audit records for the following security-related (e.g. access control, identification and authentication, configuration settings, etc.) events:

- User account management activities:
  - Addition and deletion of user accounts
  - Changes in security attributes such as access levels, privileges, roles, etc.
  - User account suspensions and activations
- Successful and failed logon/logoff events

SWIS data processing and storage system components (e.g. operating system, database, network, etc.) shall generate audit records for the following security-related events: user logons, both successful and failed; failed access attempts; any attempts to move outside permitted activities; configuration changes; account and permission modifications; successful accesses to security-critical objects (i.e., operating system files); changes to the system security configuration; modification of system-supplied software; and creation and deletion of objects.

All (application and system) audit records generated for SWIS data security-related events shall include the following information: event type and sub-type; timestamp of the event; Message; Success or failure of event; IP address of the client; and user ID triggering the event.

3.1.5 Audit Failure Events (NIST security control)

SWIS data processing and storage systems shall provide a real-time alert when the following audit failure events occur: Software/hardware errors; data corruption, data transmission failures, and failures in the audit capturing mechanisms.

3.1.6 Audit Monitoring (NIST security control)

_____ Security/Audit Administrator and Security Analyst, shall conduct an on-going review and analysis of the Mainframe or network systems components (including application, operating system, database and network) audit records for indications of inappropriate or unusual activity; and investigate, report, and take appropriate actions with regard to identified suspicious activity or suspected violations in accordance with procedures in Section 4.2 of ____ Mainframe or Network Audit Policy

The ISO shall recommend increasing the level of audit monitoring when there is an indication of increased risk to ______ operations, assets, or individuals based on law enforcement information, federal government-issued alerts or other credible sources of information. The ISO shall communicate this increased level of audit monitoring to support personnel, requiring appropriate actions, including increasing the audit log monitoring frequency to twice a day where applicable.

Security personnel shall be sent an alert of the following inappropriate or unusual activities with security implications: audit failure events, network device or server failures, intrusion attempts, denial of service attacks, malicious code detection, and other attacks on the system.

3.1.7 Audit Record Retention (*NIST security control)*

SWIS data processing and storage system audit records shall be retained for a minimum of five (5) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

3.2 Configuration Management Policy *(*NIST security control *)*

All SWIS data processing and storage System Support Staff shall adhere to the agency’s Configuration Management Plan, which provides systems configuration change control process and configuration management policy.

SWIS data processing and storage systems shall be configured to the most restrictive mode. All components shall be hardened against the current Computer Institute of Standards-specified hardening guidance. Information Technology oversight shall review relevant systems quarterly to identify and coordinate appropriately the elimination of unnecessary functions, ports, protocols, and/or services.

3.3 Contingency Planning Policy (NIST security control *)*

SWIS data processing and storage System Support Staff shall test backup data to verify media reliability and information integrity at least quarterly

3.4 Continuous Monitoring Policy (NIST security control *)*

SWIS data processing and storage System Support Staff shall monitor the security controls on an ongoing basis in accordance with _____ policy and guidance

The ISO shall suggest an increase in the level of monitoring when there is an indication of increased risk to ____ operations, assets, or individuals based on law enforcement information, federal government-issued alerts, ____ Computer Security alerts, or other credible sources of information. The ISO shall communicate this increased level of audit monitoring to support personnel, requiring appropriate actions.

3.4.1 Configuration Management, Control, and Monitoring (*NIST security control)*

Refer to the ____ and ____ portals referenced above for policy pertaining to the management, control, and monitoring of changes to the information system, including conducting impact analyses.

3.4.2 Ongoing Assessment of Security Controls

SWIS data security and storage systems security controls shall be assessed on an ongoing basis with a rigor commensurate with the system’s ______ "Medium" security category. Compliance oversight shall coordinate independent assessment of all SWIS data security and storage systems security controls on an annual basis.

3.4.3 Security Alerts and Advisories *(NIST security control)*

The Security/Audit Administrator and/or Security Analyst will receive and reviews the United States Computer Emergency Readiness Team (US-CERT) notification for the latest security alerts and bulletins (_____). The _____ Primary ISO or ____ Office of Information Technology (OIT) designee shall receive, review, and track vendor-issued alerts with regard to corresponding product vulnerabilities and issues as they are issued. The Primary ISO or _____ OIT designee shall issue alerts/advisories to appropriate personnel and take appropriate actions.

3.4.4 Vulnerability Scanning *(NIST security control)*

All systems should be scanned for vulnerabilities on a quarterly basis or after a major system modification or any modification that affects the security posture of the system, using approved tools and techniques.

3.4.5 Status Reporting

____ and ISO shall provide security status briefings for SWIS data security and storage systems to the _____ CIO on an as needed basis. With regard to issues of a high criticality identified during continuous monitoring activities, ____ Information Security point of contact shall report these items immediately to the _____ ISO, CIO and System Owner. Moderate risks shall be reported within five (5) business days, and a low risk shall be reported within 10 business days.

3.4.6 Documentation Updates

The ____ ISO shall support updating security components of the SWIS management and operations documents, to reflect any updates, at least annually and upon a significant change to the system.

3.5 Incident Response Policy (NIST security control)

SWIS data processing and storage System Support Staff shall adhere to ____ Incident Response plan and procedure.

In the event of a SWIS data breach, the ____ Security group must be notified immediately or within 15 minutes upon detection of such activities. OIT Security will in turn notify Conduent, a SWIS Clearinghouse contractor, the Employment and Training Administration (ETA), the Command Decisions Systems & Solutions (CDS[2]), and the SWIS Administration contractor. Please refer to the _____ Incident Response Policy and Procedure document for POC phone numbers and emails located on the _____ OIT Intranet.

3.6 Security Awareness and Training Policy (NIST security control *)*

In addition to the annual security awareness training, anyone with access to any systems containing SWIS data shall read the SWIS Standards and Guidelines documents and utilize all training materials made available. Additional training shall be provided by the _____ Office of Policy, Performance and Training.

3.7 System and Information Integrity Policy (NIST security control *)*

SWIS data processing and storage systems monitoring tools shall be configured per configuration and policy settings provided by ____.

3.8 Personnel Security (*)*

- Individuals requesting access to systems used to process or store SWIS Data must be approved by the system Owner (or Designee), as well as ____ IT oversight or Security Designee, prior to being granted access to the system.
- Individual possess appropriate clearance/background check for job function.
- Individual must complete Security Awareness Training by participating in the SWIS Online Webinar, reading the training slides, and reading the SWIS Standards and Guidelines documents. Documents will be emailed to the user as well as made available online.
- Individual must read and sign the SWIS Acknowledgment of Confidentiality Requirements and Restriction form (ANNEX 2).

User Activity will be monitored by way of auditing parameters built into the systems. Any violation and misuse of SWIS data will be reported to the OIT Security Office, which will in turn take appropriate actions as applicable to non-compliance activities, to include user access revocation and up to termination of employment.

3.9 Backup (Replication), Recovery and Media Protection (NIST Security Control)

The agency will utilize a Veritas tape backup system. All Systems will be backed up fully on a weekly basis and differentially on a daily basis. Tape Media will be tested regularly for functionality and data integrity.

All Storage media shall be properly labeled and access to such media shall be restricted to authorized System Support Staff only.

For data hosted externally, ____ will rely on ____ and contractor's security policies, which are based on industry best practices, as well as State and Federal Laws and regulations.

____ data shall be retained for at least seven (7) years and destroyed only if deemed necessary or as required by any specific regulation. Any data to be destroyed shall be done in a manner that is secured and will require approval from ____ management before such activities takes place.

3.10 Environmental Security

All ____-owned or leased facilities, where SWIS and other sensitive data are being processed or stored, shall have controlled access. Information Systems will reside in rooms/data centers with proper airconditioning and humidity control systems, visitor logs, smoke detectors and surveillance camera(s). Flooring and other building materials shall ensure maximum personnel safety.

PART III: PROCESSES

4. SWIS UI BENEFITS BATCH PROCESS

4.1 Daily Process <u>(Note: the Job names begins with SWIS, but the Program names still contains WRIS, until time allows for the names to be converted throughout the full process)</u>

Each weekday, Monday through Friday, including holidays, Conduent, the SWIS Clearinghouse, transmits via a dedicated line, job (program name), which generates a dataset in __ that triggers ____ job (program name).

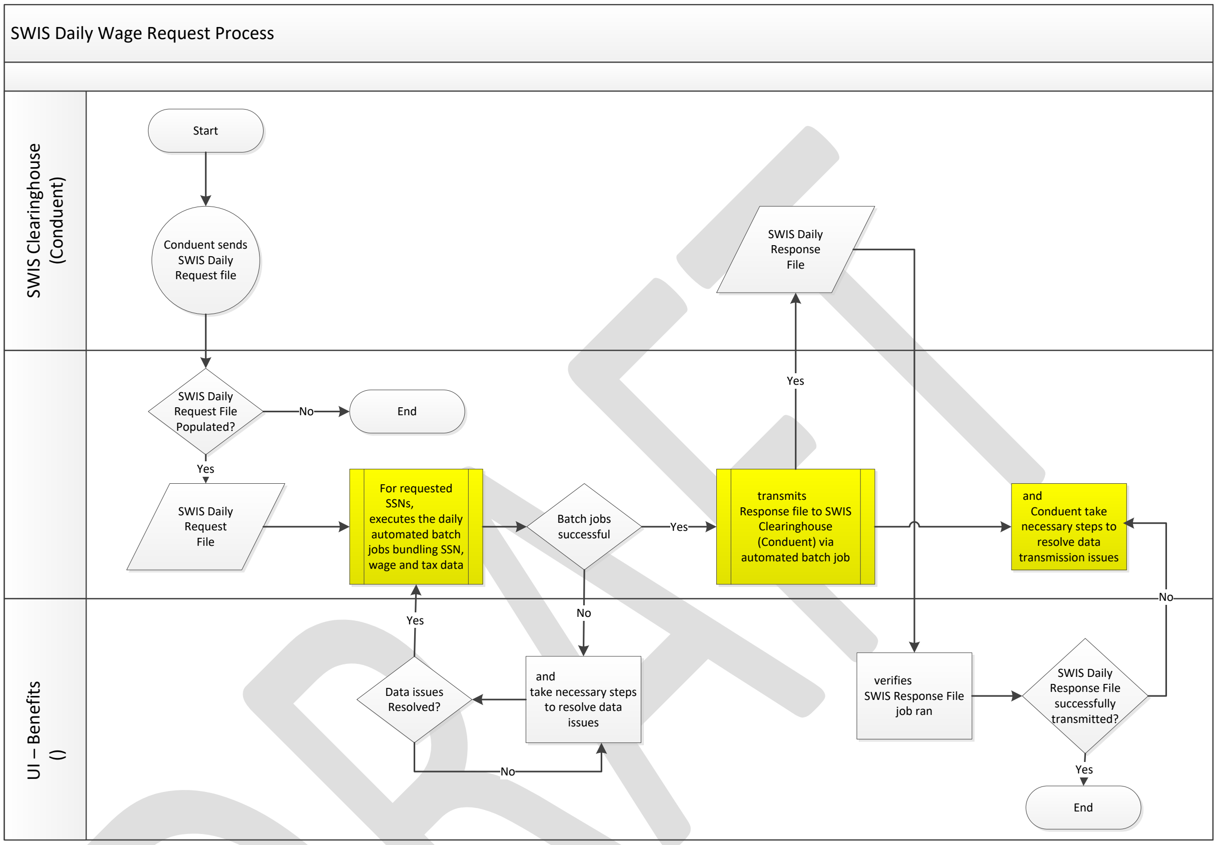
Job _____ deletes the prior request and response files; reads the requested file and if the file contains records (file is not empty); the job unbundles (program _____) the request data into individual SSNs [up to eight (8) SSNs can be included per record] based on the header record. The job then checks the unbundled file (program ______) to ensure the data is in the proper format. If the data is in the proper format, _____ uses the header record which indicates the quarter(s) being requested (up to eight (8) quarters can be requested) and generates a file (program _____) for matching against the __ Benefits Wage and __ Benefits copy of the Tax file. ______ then creates a dataset to trigger job ______.

Job _____ deletes the triggering dataset created in job SWIS010D and reads the edited file (program _____) from job _____ and searches the wage records for that SSN and the quarters requested; if a match is **not** found, the response record is populated with zeros for wages for that year and quarter and the employer data will not be populated.   If wages **are found** for that year and quarter, the response file is populated with wage data for that year and then the Benefits copy of the Tax file is searched to retrieve employer information [Name, Address, Federal Employer Identification Number
(FEIN) and North American Industry Classification System (NAICS) code]. If there is a tax record, the response file is populated with that employer information if the employer is not on the Tax file, the response file will not contain employer data.

Job _____ deletes the triggering dataset created in job _____ and then formats the response file (program _____) into a header and detail record that can be transmitted to Conduent, the SWIS Clearinghouse. The job then bundles/blocks the response record (program _____) into 80 byte records for transmission to Conduent and generates a file to trigger job _____.

Job _____ deletes the triggering dataset created in job _____ and transmits the response file (program _____) via a dedicated line to Conduent; the SWIS Clearinghouse contractor.

Table 2 – SWIS Daily Wage Request Process


SWIS Daily Wage Request Process
SWIS Clearinghouse (Conduent)
UI – Benefits ()
Start
Conduent sends SWIS Daily Request file
SWIS Daily Request File Populated?
No
End
Yes
SWIS Daily Request File
For requested SSNs, executes the daily automated batch jobs bundling SSN, wage and tax data
Batch jobs successful
Yes
No
transmits Response file to SWIS Clearinghouse (Conduent) via automated batch job
Yes
SWIS Daily Response File
and Conduent take necessary steps to resolve data transmission issues
and take necessary steps to resolve data issues
Data issues Resolved?
Yes
No
verifies SWIS Response File job ran
SWIS Daily Response File successfully transmitted?
No
Yes
End

4.2 Quarterly Process (Note: for the Quarterly Process the Job/Program names are still reflecting WRIS, for processing until Conduent changes their naming convention)

The Quarterly schedule is distributed in advance by Conduent, the SWIS Clearinghouse. Prior to the due date, parameters are modified to reflect the quarter being reported and to generate a file that includes the last eight (8) quarters of wages for all records on the Benefits Wage file.

____ Production Control, is sent an email requesting the run of "As Requested" job _____. Job _____ (program _____) reads the wage file and populates an output file with a header, detail records [SSN and an indicator to reflect whether __ has wages in the last eight (8) quarters, one (1) equals wages, and zero (0) equals no wages] and a trailer record of control totals. ____ utilizes its ___ scheduling software to submit the job and notifies the requestor that the job is running. When _____ completes, the requestors reviews the output file for accuracy and obtains control totals from the trailer record.

Once the output from _____ is validated, ____ Production Control, _____ ,is sent an email requesting the run of "As Requested" job _____ (program _____) to transmit the Distributed Data Base Index (DDBI) file via a dedicated line to Conduent, the SWIS Clearinghouse. ____ utilizes its ___ scheduling software to submit the job and notifies the requestor that the job is running. The requestor monitors the transmission of the job and then emails Martha Stevens (Conduent) Martha.Stephens@conduent.com with the create date, number of records transmitted, and transmission time.

Table 3 – SWIS Quarterly DDBI Update Process – Page 1

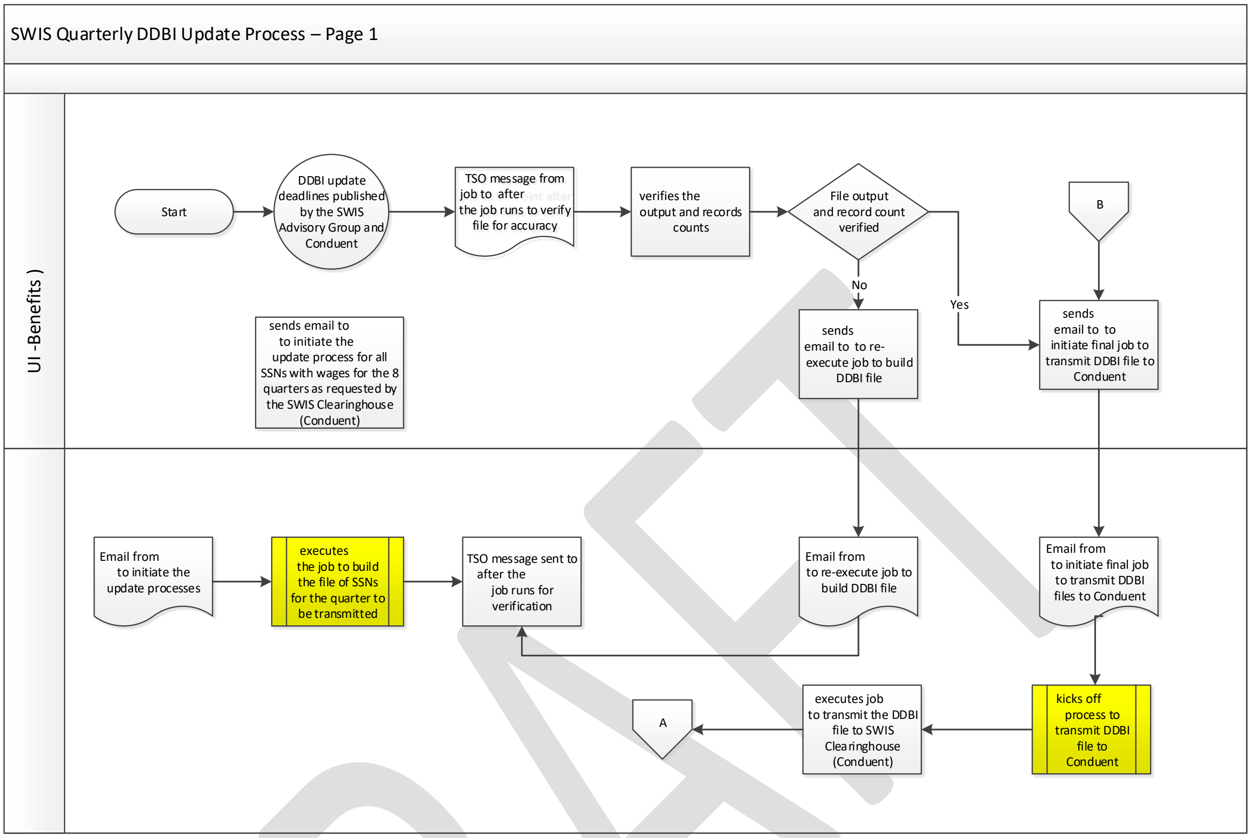
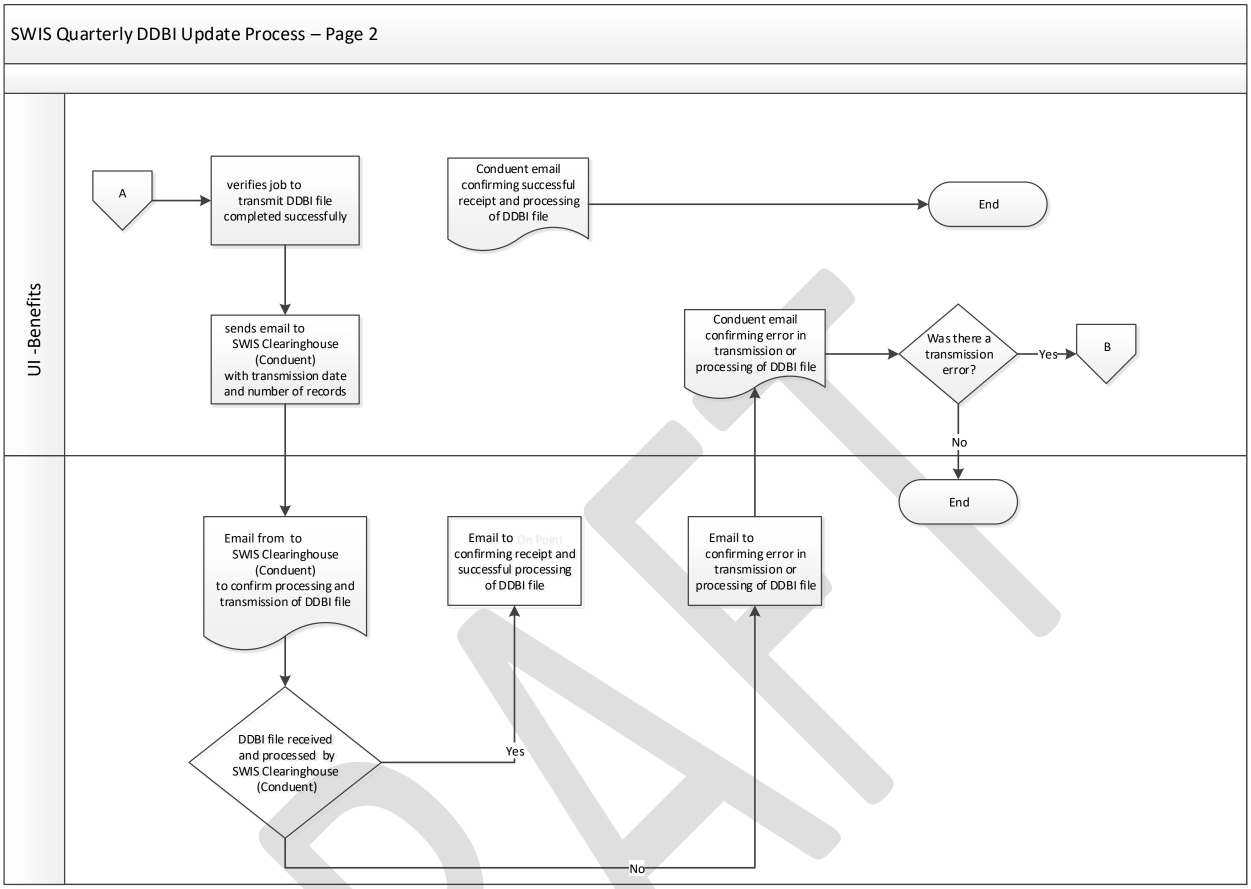

SWIS Quarterly DDBI Update Process – Page 1
UI -Benefits)
Start
DDBI update deadlines published by the SWIS Advisory Group and Conduent
TSO message from job to after the job runs to verify file for accuracy
verifies the output and records counts
File output and record count verified
No
Yes
B
sends email to to initiate the update process for all SSNs with wages for the 8 quarters as requested by the SWIS Clearinghouse (Conduent)
sends email to to re-execute job to build DDBI file
sends email to to initiate final job to transmit DDBI file to Conduent
Email from to initiate the update processes
executes the job to build the file of SSNs for the quarter to be transmitted
TSO message sent to after the job runs for verification
Email from to re-execute job to build DDBI file
Email from to initiate final job to transmit DDBI files to Conduent
A
executes job to transmit the DDBI file to SWIS Clearinghouse (Conduent)
kicks off process to transmit DDBI file to Conduent

Table 4 – SWIS Quarterly DDBI Update Process – Page 2


SWIS Quarterly DDBI Update Process – Page 2
UI -Benefits
A
verifies job to transmit DDBI file completed successfully
sends email to SWIS Clearinghouse (Conduent) with transmission date and number of records
Conduent email confirming successful receipt and processing of DDBI file
End
Conduent email confirming error in transmission or processing of DDBI file
Was there a transmission error?
Yes
B
No
End
Email from to SWIS Clearinghouse (Conduent) to confirm processing and transmission of DDBI file
Email to On Point confirming receipt and successful processing of DDBI file
Email to confirming error in transmission or processing of DDBI file
DDBI file received and processed by SWIS Clearinghouse (Conduent)
Yes
No

5. PACIA WAGE MATCH PROCESS

PIRL and Quarter/Annual Federal Reports:

- Participant Individual Record Layout (PIRL)
- ETA-9172 PIRL DOL-only Participant Individual Record Layout File
- Quarterly ETA-9173 Workforce Innovation and Opportunity Act (WIOA) (Adult/Dislocated Worker/Youth), Wagner-Peyser, Jobs for Veterans' State Grant and Trade Adjustment Assistance (TAA).
- Annual Reports: ETA-9169 WIOA (Adult/Dislocated Worker/Youth) and Wagner-Peyser.

Other Wage Request via SWIS Request Form (SRF):

- ETP-9171 Eligible Training Provider (Annual)
- Third Party Entity (TPE)

USDOL (US Department of Labor) has separate software, Workforce Integrated Performance System (WIPS), to check the validity of the PIRL file that is generated by the contractor for Federal reports. The PIRL file contains SWIS wage data. The PIRL file is run through WIPS to have the Federal reports in the format that is acceptable by USDOL in order to produce the Quarterly and Annual Reports.

A wage request file is generated and sent to the SWIS for matches and once the SWIS Wages are returned, they are populated into an Internal Wage Database that resides on the ____ server. Since SWIS doesn't allow states to pull their own state wages (Intrastate), __ runs a separate process, requesting _____ to pull __ UI Intrastate wages, which are then returned and placed into the Internal Wage Database that resides on the ____ server.

Quarterly maintenance is performed on the database to generate a file to the contractor to be loaded into the case management database so that the contractor can create the Participant Individual Record Layout (PIRL) file daily, which is used to produce the federal reports. The performance of the agency is dependent on the information that we get on the wage match files. Utmost care must be taken to load the wage match files into the internal wage database.

5.1 Steps for the PACIA SWIS wage match process (PIRL and Quarterly/Annual Reports):

5.1.1 Creation of wage request file for PIRL and Quarterly/Annual Reports

- Make changes to the SWIS Wage Request File Query. The number of quarters we request wages for is eight (8). One oldest quarter is deleted and the recent quarter is added. For example, in the wage request file for 2020 2nd quarter, the quarters we request wages for is 20183, 20184, 20191, 20192, 20193, 20194, 20201, and 20202. The recent quarter is 20202 and the oldest quarter is 20183.
- The request file includes all Wagner Peyser, WIOA and TAA participants for the last eight (8) quarters (distinct).
- Run the query and save the results in a pipe delimited text file in ANSI format. There should be NO duplicates SSNs in the request file. The text file should only contain nine digit numeric data on each line without "dashes" as separators.
- The query should ensure that SSNs submitted are valid according to the Social Security Administration website. This process will decrease the transmission and processing time associated with invalid SSNs.

    - SSNs may not have zeros in positions four (4) through nine (9).
    - The first three positions may not be all zeros or greater than 772.
    - SSNs of all 1’s, 2’s, 3’s, 4’s, 5’s, 6’s, 7’s, 8’s, or 9’s are invalid.
- Load the wage request file into a table in tempVOS database on DOESSV25 server
- Logon to SWIS Clearinghouse and upload the file to SWIS.
- Request eight (8) quarter matches.
- The request file is sent to SWIS at the very end of the Quarter.

5.1.2 Processing wage return file for PIRL and Quarterly/Annual Reports

- SWIS notifies us of the fact that the files are available for download. (It usually takes about two weeks unless a shorter time is requested. We usually request a two-week time frame so the results are as complete as possible.)
- Logon to SWIS Clearinghouse and download the file from SWIS.
- Open the file and delete the header records from the file.
- Upload the file into table in InternalWages database on ________ server.
- The file is a ~ delimited file.
- Make changes to the SWIS query and execute it.
- Validate the results and uncomment the section of creating SWIS table and run the query again. This should create the SWIS table. For validation, check the number of records before and after. The number of records will increase.

5.1.3 Process internal wage database for PIRL and Quarterly/Annual Reports

- Since SWIS doesn’t allow states to pull their own Intrastate wages, __ runs a separate process with _____ pulling __ UI Intrastate wages which are then included in the internal wage process (See Intrastate Wage Request Process)
- Once all the tables are created for the wage match files, execute query for internalwagedatabase.
- Validate the results and uncomment the section of creating internalwagedatabase table and run the query again. This should create the internalwagedatabase table with a column identifying the returning entity. For validation check the number of records before and after. The number of records will increase.

5.1.4 Creating wage file – contractor assists - for PIRL and Quarterly/Annual Reports

- After the internalwagedatabase table is created, run wages for the contractor after making necessary changes to the query.
- Save the results in a pipe delimited text file in ANSI format.
- Zip the file and make it password protected.
- Place the above zip file () to ___ folder Data Files From the contractor case management system to __/Wages on the contractor SFTP site.
- Create a change order in the contractor system.
- Make a note of the number of records in the contractor database.
- Once the wages are imported into the case management system, the number of records in the database will increase.
- **The timeliness of this is very important as the wages files drive the performance measures on the reports. Early access to the final results allow staff to take corrective actions, if needed.**

- Send notice to ____ Performance Team when contractor confirms wages have been loaded.

5.2 Steps for the PACIA SWIS wage match process for Other Wage Request (ETP or TPE):

5.2.1 Receive ETP or TPE Wage Request File and Corresponding Documents

- Review the SWIS Request Form for ETP/TPE, the data being provided, and corresponding documents to ensure they meet the requirements of the standard operating procedure and DSA.
- Run the query and save the results in a pipe delimited text file in ANSI format. There should be no duplicate SSNs in the request file. The text file should only contain nine-digit numeric data on each line without dashes as separators.
- The query should ensure that SSNs submitted are valid according to the Social Security Administration website.
- Load the wage request file into a table on a secure server.
- Logon to SWIS Clearinghouse and upload the file to SWIS.
- Request quarter matches based on the SWIS Request Form [up to eight (8) quarters allowed].
- The request file is sent to SWIS.

5.2.2 Processing wage return file for ETP or TPE

- SWIS provides an alert that the files are available for download. (It usually takes about two weeks unless a shorter time is requested. A two-week processing time frame is usually requested to provide time to sufficiently compile the results.)
- Logon to SWIS Clearinghouse and download the file from SWIS.
- Open the file and delete the header records from the file.
- Upload the file into a table in InternalWagesDatabase on the ___ server and name the table based on the SWIS Request Form (SRF).
- Since SWIS doesn't allow states to pull their own intrastate wages, ____ must pull __ UI intrastate wages that are placed in the InternalWagesDatabase on the _____ server. The name is based on the SWIS Request Form (SRF). (See Intrastate Wage Request Process)
- Once all the tables are created for the wage match files, execute a query to combine __ and SWIS and create a usable table for processing of (ETP or TPE) requirements.
- If ETP, notify the requestor to verify the data from the secured server.
- If TPE, design/run a query to aggregate the data based on the SRF.
- If TPE, validate the results and return aggregated results.

Appendix A – Global SWIS Management and Procedure MATRIX

Process	PACIA Procedure/Plan	SUIA Procedure/Plan
Standard Operating Process	• Individual(s) identified as SWIS contact. • Confidentiality agreement is completed. • Confidentiality agreement is verified and authorized by PACIA agency. • PACIA Process: A request is initiated by PACIA employee based on Quarterly schedule and Annual need. Other request is sent on the official SWIS Request Form (SRF). Example: ETP or **TPE Request. • Request is verified as valid. • Request data is reviewed for accuracy. • Request data is submitted to SWIS web based system. Request is accepted by SWIS and all documentation is stored. • SWIS data is downloaded to secure location and is done from a secure physical location. • SWIS data is loaded into appropriate system(s). • If the request was done based on the SWIS Request Form and for ETP; the data will be placed on a secured server and the requester will be informed to verify the data. • If the request was done based on the SWIS Request Form and for a TEP; the data will be aggregated and only aggregated data will be returned to the original requestor to ensure completion of the original request. *** TPE is defined at Section V.CC. of the SWIS Agreement, is any public body, public agency, or private provider of training services required by law to meet State and/or Federal performance measures for such programs as identified in Section IX.B.4. of the Agreement.*	• Individual(s) identified as SWIS contact. • Confidentiality agreement is completed. • _____ Mainframe or Network infrastructure is configured for secured communication with the SWIS Clearinghouse (Conduent). • Request data is received from the Clearinghouse (Conduent). • Request is processed on the mainframe or network and response file is generated and sent back to the clearinghouse.

Process	PACIA Procedure/Plan	SUIA Procedure/Plan
Data Storage	• Case Management Solution is provided by the contractor. • Any downloaded data is stored on a secure server. • Access to data on the secure server is limited through Active Directory accounts specific to each individual folder. • The PACIA shall retain the Wage Data received from the SUIA only for the period required to utilize it for assessment and reporting purposes, or to satisfy applicable Federal or state records retention requirements. Thereafter, the Wage Data shall be destroyed, including the degaussing of magnetic tape files and permanent deletion of electronic data. The PACIA shall not retain the records for more than five (5) years from the date the Result is received.	• Mainframe or network batch requests, responses and Quarterly SWIS DDBI files are stored in secure data files at the data center. • Mainframe or network batch requests, responses and Quarterly SWIS DDBI files are not stored on other media (i.e. CD, DVD, etc). • Mainframe or network batch requests, responses and Quarterly SWIS DDBI files are destroyed when the next request is received. • Access to Mainframe or network batch requests, responses, and Quarterly SWIS DDBI files are controlled through the batch requests. • Responses and Quarterly SWIS DDBI files are stored on the mainframe or network only, not in offices or filing cabinets.
Data Flagging	• Data is flagged in all appropriate systems as SWIS data. • Data flag will allow ability to verify all SWIS data within each system for security purposes. • Data flagged in systems can be deleted via normal data removal process.	• Mainframe or network batch requests, responses (SWIS) and Quarterly SWIS DDBI files are flagged as SWIS data respectively. • Batch requests, responses (SWIS) and Quarterly DDBI files names will allow ability to verify all SWIS data within each system for security purposes. • Batch requests, responses (SWIS) and Quarterly DDBI files can be deleted via normal data removal process.
Security Protocol and Measures	• ____ SWIS Data Processing and Storage Policy • Applicable Section of the SWIS Agreement	• ____ SWIS Data Processing and Storage Policy • Applicable Sections of the SWIS agreement
Risk Management	• ____ RISK Management Plan Policy	• ____ RISK Management Plan Policy

Process	PACIA Procedure/Plan	SUIA Procedure/Plan
Plan		
Incident response plan	- ____ SWIS Data Processing and Storage Policy	- AUDIT Policy - ____ SWIS Data Processing and Storage Policy
How is the Request Process tracked?	- SWIS request form is submitted via email to appropriate PACIA employee for verification. (Form currently in Digital Library) - Request to SWIS for data is tracked via email. - All emails from SWIS because of PACIA request are stored for documentation purposes.	- N/A to batch process
How is the Response Process tracked?	- All SWIS response emails to PACIA about requested match are stored for documentation purposes. - SWIS completion form is completed and returned to original PACIA employee requesting the SWIS match via email.	- N/A to batch process –

Appendix B – PACIA Wage Match Process 5.1 PIRL and Quarterly/Annual

After the end of each quarter (approximately after one to two weeks), the Wage Match request file is created and the SWIS request is initiated. Pending on the 4th Quarter Results, an additional request may be requested to complete the Annual Report. __ Wages are pulled based on DDBI Schedule.

Appendix C – PACIA Wage Match Process 5.2 Other Wage Request (ETP or TPE)

Appendix D

SWIS Acknowledgement of Confidentiality Requirements and Restrictions

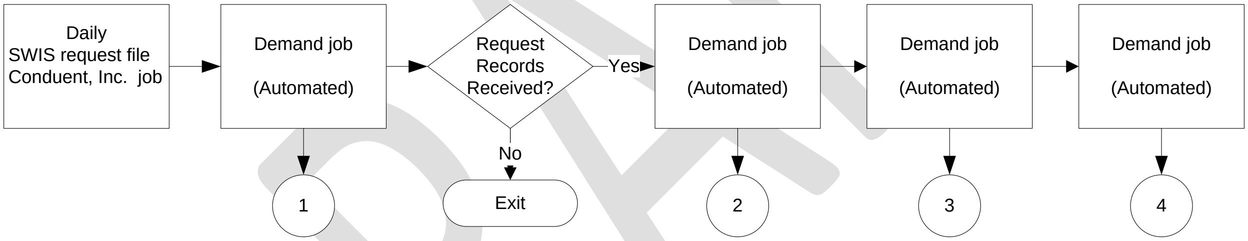
All authorized PACIA or SUIA employees, contractors, or agents requiring access to wage data and associated PII data included in the wage request process attest that they:

- have been provided a copy of the SWIS Data Sharing Agreement, the SWIS Data Sharing Agreement/FERPA Written Agreement, and any Supplemental FERPA Agreement(s) incorporated by reference into the SWIS Data Sharing Agreement;
- have reviewed the SWIS Data Sharing Agreement and the other agreements incorporated therein; and
- agree to comply with the applicable standards contained in the SWIS Data Sharing Agreement, and the other agreements incorporated therein, in carrying out their SWIS-related duties.

Appendix E - Data Management Systems Description

The contractor provides the software used to report on all workforce development services and create all Federal reports for USDOL and also hosts the _____’ system. __ sends the contractor a raw file with wage information every quarter and this file is bumped against the database for all persons enrolled in WIOA, Wagner-Peyser and TAA programs to search for those who are employed. Detailed security features prevent access to this information by anyone who is not authorized (following DSA requirement and signing of the SWIS Annex 2 form). The wage and employment information collected is used for performance calculation and reporting. Since the contractor supports other workforce systems, they are familiar with the SWIS, its policies and procedures, and the need for complete confidentiality as far as wage/SSN information is concerned.

____ utilizes ____ data centers and the corresponding systems (Mainframes) which host applications configured for automated processing of wage data request from the clearinghouse (Conduent). The Mainframe or network systems are connected to the Clearinghouse via a secured and dedicated VPN link. Summary of automated process is as follows:



____ Mainframe or Network production control maintains the specific interconnected system configurations.

Appendix F

Annex 2

State Wage Interchange System (SWIS)

Performance Accountability and Customer Information Agency (PACIA) *or* State Unemployment Insurance Agency (SUIA)

Acknowledgement of Confidentiality Requirements and Restrictions

In accordance with Section VIII of the SWIS Data Sharing Agreement, which sets out the Responsibilities of the Parties, the names and signatures of everyone who will have access to Wage Data, personally identifiable information (PII) from Education Records, or Personal Information from Vocational Rehabilitation (VR) Records, including PACIA or SUIA employees, contractors, or agents properly authorized by the PACIA or SUIA to use the SWIS Clearinghouse in accordance with the provisions of Sections VI, VIII, and XI of the SWIS Data Sharing Agreement appear below. All authorized PACIA or SUIA employees, contractors, or agents below acknowledge their understanding of:

- the confidential nature of SWIS data, including Wage Data, PII from students' Education Records, and personal information in the possession of VR agencies received through the SWIS Data Sharing Agreement;
- the standards for the handling of such data as discussed in Sections VI, VIII, and XI of the SWIS Data Sharing Agreement, the SWIS Data Sharing Agreement/FERPA Written Agreement incorporated by reference therein, and any Supplemental FERPA Agreement(s) incorporated by reference therein; and
- their obligation to comply with such standards in carrying out their responsibilities under the SWIS Data Sharing Agreement.

All authorized PACIA or SUIA employees, contractors, or agents listed below attest that they:

- have been provided a copy of the SWIS Data Sharing Agreement, the SWIS Data Sharing Agreement/FERPA Written Agreement, and any Supplemental FERPA Agreement(s) incorporated by reference into the SWIS Data Sharing Agreement;
- have reviewed the SWIS Data Sharing Agreement and the other agreements incorporated therein; and
- agree to comply with the applicable standards contained in the SWIS Data Sharing Agreement, and the other agreements incorporated therein, in carrying out their SWIS-related duties.

Mailing address. Please mail the signed Acknowledgement of Confidentiality document to the current ETA SWIS support contractor, CDS2:

Command Decisions Systems & Solutions, Inc.
Attn.: SWIS
8761 Dorchester Road, Suite 200
North Charleston, SC 29420
(Fax: 843.552.8028)

In addition to the mailed original, a copy of the signed Acknowledgement document may be e-mailed to: SWIS@dol.gov and SWIS@cds2.com.

State:	
SUIA or PACIA Agency:	
SUIA or PACIA Contact Name:	
Title:	
Agency/Organization:	
Signature of SUIA or PACIA Contact:	
Date:	
Mailing Address:	
Telephone:	
Email Address:	

Please note: Signatures of Employees, contractors, or agents begin on next page.

Employee Signature:	
Date signed:	
Employee Name (*Please print*):	
Employee's Title:	
Employee's Business Unit:	
Employee's Supervisor:	
Title and Business Unit of Supervisor:	
Email of Supervisor:	
Phone Number of Supervisor:	
Is the Employee a staff member of the State SUIA?	__ Yes __ No
or a State PACIA?	__ Yes __ No
Is the individual an employee of the State, a contractor, or agent?	__ State __ Contractor __ Agent
Employee's work location including State agency, agent or contractor name, building number, street and city: ***(Agency Name)*** ***(Building or floor or suite #)*** ***(Street)*** ***(City), (State) (Zip)***	
Employee Phone Number:	
Employee Email Address:	
Does the employee require ETA-approved individual credentials to access the password-protected SWIS Clearinghouse PACIA portal?	__ Yes __ No

Appendix G: Additional Resources

Other External Roles and Responsibilities

Roles	Personnel	Responsibilities
SWIS Operations Contractor, Conduent, Inc.	**Martha Stephens** Assistant Account Manager 1-800-327-9250 Option 2 Martha.stephens@conduent.com SWIS-WIOA.Support@conduent.com	SWIS Operations Contractor is responsible for the technical operation and maintenance of the SWIS Clearinghouse hardware and software, for providing technical support to states participating in the SWIS, and for assisting ETA with its SWIS management and administrative functions.
SWIS Administration Contractor, Command Decisions Systems & Solutions (CDS2)	SWIS@cds2.com	SWIS Administration Contractor is responsible for the administration of the SWIS Clearinghouse Administration and SWIS Compliance.
Federal Oversite, Department of Labor Education & Training Administration (DOLETA)	**Karen Staha**, Chief Division of Strategic Planning and Performance Staha.Karen@dol.gov **Toquir Ahmed** SWIS Administration Ahmed.Toquir@dol.gov SWIS@dol.gov http://www.doleta.gov/performance/SWIS.cfm	ETA is responsible for the overall management and administration of the SWIS on behalf of all participating states, including providing grants to support the operational infrastructure of SWIS to allow the exchange of wage data.

SWIS Data Sharing Agreement (DSA) - References

- The roles and responsibilities of a SUIA are outlined in Section VIII.A. of the SWIS DSA.
- The roles and responsibilities of a PACIA are outlined in Section VIII.B. of the SWIS DSA.
- The roles and responsibilities of ETA are outlined in Section VIII.C. of the SWIS DSA.