Policy

SECTION: HUMAN RESOURCES	POLICY #	PAGE 1 OF 4
TITLE: System Access Policy	EFFECTIVE DATE: 11/20/2019	
APPROVED BY: LWDB #14	REPLACES: N/A	

PURPOSE: The purpose of this policy is to communicate Worknet Pinellas, Inc dba CareerSource Pinellas and to formalize the standard operating procedure for maintaining and protecting access to the internal and state systems used by CareerSource employees, DEO staff located in CareerSource offices, volunteers, interns, other authorized users, contractors and partners and to describe all associated requirements that are necessary to ensure compliance on this subject.

BACKGROUND: As part of its workforce development and TANF responsibilities, CareerSource collects and retains in its Electronic Data Management System, accounting software, and workflow module system large quantities of personal identifiable information and sensitive information relating to its customers, both job seekers and employers, and staff. CareerSource also enters and reports data (programmatic and fiscal), tracks participation, monitors performance and receipt of services in various workforce systems, such as the One-Stop Service Tracking (OSST) system, Employ Florida (EF), etc. As a part of the Workforce system of Florida, in most circumstances CareerSource has "read only" access to the Florida MIS system (DCF mainframe), The RACF, Connect and Suntax MIS systems obtained through a DCF, DEO or regional security officer. With this access to customers' personally identifiable information, as well as sensitive financial data, it is incumbent upon CareerSource to develop policies and procedures to properly handle and protect access to this information.

POLICY: This policy is to provide appropriate role-based system access, to maintain and control such access, and, as necessary, to revoke such access to all state and local data (programmatic and financial) systems to protect the security of each system and the privacy of all personally identifiable information and sensitive information obtained from customers and/or other individuals.

APPLICABILITY: Failure of any of the individuals listed above under "Applicability" to comply with this policy shall result in disciplinary action in accordance with the applicable Employee Handbook. Failure by a partner agency that is located in a CareerSource Pinellas facility or a program contractor to comply with this policy may result in termination of any MOU, agreement or contract.

RESULTS OF FAILURE TO COMPLY WITH POLICY: Failure of any individual listed under "Applicability" above, other than customers, to follow this policy may result in disciplinary action in accordance with CareerSource Pinellas' Personnel Handbook. Failure of a program contractor or training vendor to follow this policy may result in contract or agreement termination.

DETAILS: Following are definitions and details that pertain to this policy. See accompanying policy on handling Personally Identifiable Information for associated detail. Note, use of the term "employee" or "staff" shall man any of the individuals listed under "Applicability."

A. Initial Access or a Change in Access- When a staff is hired the following steps shall be followed.

1. The staff's Director or supervisor will require the staff to complete and sign the security access form(s) to any and all data systems to which the individual's job responsibilities require access. Staff do not all require the same access or level of privilege; both should be determined by the individual's job responsibilities. Each request shall include specifics such as any OSST units, WP CareerSource centers, EFM groups or identification of veteran staff (LVER or DVOP) to properly set-up staff privileges. If a higher level of privilege or a different type of access than is the norm for the job title is requested, the Director or supervisor must justify that higher level of privilege in writing and attach to the security access form.
2. Staff's access to Microix will be set-up by the primary RSO (Regional Security Officer). Access will be limited to the individual's job responsibilities as well as their applicable workflow (i.e., WTP, Adult/Dislocated Worker, TAA, Youth, etc.) The staff's Director or supervisor will email the staff's (a) first and last name (b) email address (c) phone number (d) name of a staff set-up in Microix with the security profile needed for the newly hired staff and (e) applicable workflow(s) to the primary RSO. Set-up will be processed within 2 business days of receipt of information. A follow-up email will be sent to the newly hired staff and Director or supervisor once access has been set-up.
3. The newly hired staff will be required to complete a statement of non-disclosure and confidentiality as part of the HR on-boarding process.
4. All newly hired staff will be required to complete the online security training as well as annual refresher with completion documented by completion of a security awareness training form. New hire access will not be granted until said training is completed and documented. Failure to complete annual refresher may result in removal of security privileges.
5. The security access form(s) should be signed by the staff, the staff's supervisor or Director and then immediately scanned to the Atlas queue, MIS Security Forms. Once the security forms are scanned, then the supervisor shall destroy the original paperwork by placing it in the CareerSource supplied shred bins.
6. The RSO will process the paperwork within 2 business days and forward to the state as necessary for state system access. The RSO will also provide local system access as requested and appropriate for job position. As a backup, the RSO will forward the new hire notice to the IT Department for access to our server if notice has not already been provided to the IT Department.
7. An email alert is forwarded to the RSO team and to IT who manage creation or update of staff access or privileges as forms are added to the EDMS designated queue. Upon completion, the RSO will advise the Director or supervisor by email that the paperwork has been processed and provide any additional pertinent information. The Director or supervisor will instruct the staff in their initial login to various MIS systems or server.
8. The RSO will create and maintain a secured, limited access, on-line file of the security access forms; one for active users and one for users whose access has been revoked. This should be maintained in a manner to allow easy and immediate access of an individual's paperwork to the RSO.
9. Ad hoc reporting will be used to maintain a current listing of user access and level of privilege in the various MIS systems or server.
10. If a need for amended security access or privileges arises, the staff's Director or supervisor will complete a "change" security form requesting the change. The RSO will make approved changes and communicate back to Director or supervisor of its completion. The change request form will be retained in the appropriate file. The RSO may develop further specific instructions in the form of desk guides for any system access.

B. Audits of System Access - To ensure that CareerSource maintains proper security as it pertains to access to our internal EDMS and access to the various state systems, periodic "audits" of the list of approved users and their level of privilege for each system will be conducted at least semi-annually by the RSO. This will be accomplished by the RSO sending out a spreadsheet listing each staff's name, hire date or date access was granted, their job title, their current access and level of privilege and requiring each Director to review the list and provide the following feedback within 15 business days:

1. Look for any names on this list that should no longer have ATLAS, local server, or state system privileges because they are no longer an employee of CareerSource, a DEO employee located in a CareerSource office, contracted provider staff or eligible partner staff
2. Of the individuals who remain an employee of CareerSource, a DEO employee located in a CareerSource office, contracted provider staff or eligible partner staff
    a) Should each retain access to ATLAS and each of the state systems at the same level of privilege shown on the spreadsheet based on their current job responsibilities;
    b) Has the individual moved to a different position within the organization that no longer requires the access or level of privilege shown on the spreadsheet; and/or
    c) Should the individual never have had system access or the level of privilege shown on the spreadsheet?
3. Are there current staff that are not on the spreadsheet that
    a) Currently have access. If so, the Director or supervisor shall provide a breakdown of the system(s) both local and state, to which the employee(s) have access and define the level of privilege already in use; and/or
    b) Are any individuals missing needed access and if so, the system(s) the staff needs access to and the level of privilege necessary based on their job responsibilities. In this circumstance, the Director should have the appropriate security access forms completed, signed and scanned to the RSO.

The RSO will then review the information received from each Director or supervisor, make any changes warranted to access or the level of privilege, request a new signed security form(s) as appropriate, update the spreadsheet, and distribute the updated spreadsheet to all Directors for their reference within 10 business days of the due date of all reports from the Directors.

The RSO will also monitor Microix system access at least annually or more frequently if necessary. A spreadsheet listing the workflow module and access rights, by user, will be emailed to the Director with instructions to delete or modify user name, workflow module, and access rights, as applicable. Directors will be requested to provide their response within 15 business days of receipt of the monitoring notice.

C. Revoking Access – When a staff is dismissed or resigns the following steps shall be followed.

1. The HR Manager will provide notification to the RSO, IT and other key staff who control access to the various systems via email. The RSO will place a completed termination checklist and a signed set of security forms with termination or revocation noted into the Atlas queue, MIS Security Forms. This information should be sent prior to the last date of employment whenever possible to give time for responsible parties to revoke all access to ensure timely revocation.
2. The RSO, key staff controlling access, or IT will revoke or request revocation of access to local server(s), all state systems and the local ATLAS system, as applicable, by no later than the effective date and time provided by the HR Manager.
    a) EFM – revocation of access is handled locally
    b) OSST – revocation of access is handled locally
    c) RACF – revocation of access is requested thru DEO state security officer; modification of RACF is handled locally
    d) CONNECT - revocation of access is handled locally
    e) Suntax – revocation of access is requested thru DEO state security officer, locally disable user access
    f) Florida MIS – revocation of access is requested thru DCF regional security officer
    g) Any special MIS access due to grant management - revocation of access is handled locally

h) OSMIS financial – revocation of access is requested through DEO
i) Microix – revocation of access is handled locally through primary RSO only
j) MIP Fund Accounting - revocation of access is handled locally
k) Card Reader System – revocation of access is handled locally
l) CareerSource Atlas – revocation of access is handled locally
m) CareerSource email and server access – revocation of access is handled locally by CTS

3. The HR Manager and/or the RSO will advise other staff within CareerSource, as appropriate and necessary, to ensure access to all state systems is revoked.
4. The RSO, IT and other key staff controlling access will advise the HR Manager by email when access had been revoked and provide any additional pertinent information such as the system(s) for which access was revoked.
5. All paperwork on that staff who has been dismissed or who has resigned will be moved by the RSO from active staff to a separate folder within this on-line file containing access paperwork of staff who have been dismissed or who have resigned.
6. The RSO will update the spreadsheet used for system access audits by removing the staff whose access was revoked and placing the name on another tab that includes only those staff who are no longer employees of CareerSource.

ACTION STEPS REQUIRED: Following are the action steps each CareerSource employee, DEO staff located in a CareerSource facility, volunteer, intern, authorized user and contractor must take.

1. Each individual must review this policy directive. If the individual has a question about anything contained herein, it is his/her responsibility to immediately bring the question to the attention of his/her supervisor. If not resolved, the supervisor will contact the individual named under "Inquiries" below.

2. CareerSource contract managers and appropriate Directors shall provide this policy and any subsequent revisions to all partner agencies located in a CareerSource facility and to program contractors with access and require that each submit a letter stating that this policy was provided to all appropriate staff and that the partner or contractor shall abide by this policy.

3. Each individual must replace previous policies associated with system access with this policy reissuance.

4. It is the responsibility of all individuals to immediately report any breach of this policy to the individual names under "Inquiries" below.

5. Each supervisor, manager, and director is responsible for informing employees of this policy.

6. Within two weeks of termination the appropriate CareerSource Director will be responsible for ensuring caseload maintenance/transfer is completed for any staff carrying an assigned caseload who has resigned or been dismissed. A letter of notification should be forwarded to all impacted customers within the assigned caseload.

POLICY AMENDMENTS OR REVOCATION:

Notwithstanding any of the foregoing, CareerSource reserves the right to revise or revoke this policy at any time.

This policy is written to establish local procedures and is not intended to supersede any applicable laws or regulations. Failure of CareerSource to adhere strictly to the steps outlined within this policy shall not be construed as a violation of rights or administrative procedures.

INQUIRIES: Any question about this policy should be directed to the HR Business Partner**.**