



CAREER CONNECT STAFF USER DATA CONFIDENTIALITY AND SECURITY AGREEMENT

PURPOSE

The Chicago Cook Workforce Partnership (“The Partnership”) administers Career Connect, an integrated workforce data system designed to improve economic outcomes for job seekers and employers. As a technology tool, Career Connect:

1. helps staff at all levels track and manage their work more efficiently and effectively;
2. enhances coordination and collaboration across The Partnership’s network and across the county-wide workforce system; and
3. allows workforce service providers to extract real-time program data in order to track outcomes and make data-informed decisions about programs and services.

It is The Partnership’s policy that Career Connect:

- is used in accordance with The Partnership’s written policies and procedures;
- is secure from unauthorized use; and
- that information contained therein is secure from unauthorized or accidental disclosure, alteration, or destruction.

Receipt of a Career Connect username for the purposes of accessing Career Connect constitutes agreement with this Data Confidentiality and Security Agreement (“Agreement”).

In addition to this Agreement, The Partnership will provide users with written policies and procedures governing how data is to be entered and managed in Career Connect. These policies and procedures may be updated from time to time.

SCOPE

This Agreement governs the security and authorized use of Career Connect, including all information stored, processed, and/or transmitted from, to, and through Career Connect. Authorized users of Career Connect are:

- Chicago Cook Workforce Partnership staff;
- workforce service providers and their staff authorized by The Partnership to use Career Connect to manage workforce programs for employers and job seekers;
- independent contractors of The Partnership who need access to Career Connect to perform their contractual work;
- consultants or other individuals granted specific rights in connection with the performance of specific Partnership business;
- authorized auditors and grant compliance officers;
- authorized staff from agencies whose data systems interface and share data with Career Connect; and
- authorized staff from Geographic Solutions, Inc. for the purposes of hosting and maintaining Career Connect.

ENFORCEMENT

Violations of this Agreement will be considered on a case-by-case basis and could result in revocation of access and/or disciplinary action up to and including termination of employment/contract and prosecution. Violators may be subject to civil and/or criminal penalties under the applicable laws.

EXCEPTIONS TO THE POLICY

There shall be no departure from this policy unless the Chief Executive Officer of The Partnership grants an exception in writing. Additionally, The Partnership will perform periodic review of exceptions, as appropriate.

AUTHORIZED USE OF RESOURCES

Career Connect includes data on employers, job seekers, and workforce programs. Much of this information is confidential, proprietary, or privileged from disclosure. Each Career Connect user has authorized access only to that information which is necessary to perform the user's assigned responsibilities. Unauthorized access to information other than that stated above is strictly prohibited. All users must safeguard all Career Connect information and consider it proprietary and confidential unless otherwise designated. Users must ensure that information is not disseminated to unauthorized persons, or otherwise improperly disclosed, even inadvertently.

IDENTIFICATION AND AUTHENTICATION

All users will be assigned a unique username. Each username must have a password associated with it for authentication. The user must log on to Career Connect with the assigned username and enter an associated password for authentication.

PASSWORD REQUIREMENTS

Unique usernames with passwords control access to Career Connect and shall be confidential and protected by assigned users to prevent unauthorized use and release of information. The following requirements apply to passwords:

- Minimum of eight (8) and maximum of twenty (20) characters
- Must contain at least one (1) upper case and at least one (1) lower case letter
- Must contain at least one (1) number
- Must contain at least one special character. Allowable special characters are: !, @, #, \$, %, ^, *, ., _
- Password cannot be the same as the user ID
- Password cannot be reused within a twelve (12) consecutive month period
- Password must be changed every thirty (30) days
- User accounts will be locked after multiple failed password attempts
- Passwords shall be confidential and protected by assigned users to prevent unauthorized use and release of information
- Passwords may not be written or stored where they may be readily viewed (e.g. sticky notes on or next to the computer or monitor)
- **Usernames and passwords are assigned to specific users and must not be shared with others**
- Users are responsible for the results of any use of their assigned accounts

In the event that you forget your password, you should first contact the designated Career Connect support person at your office. If your support person is unavailable or cannot reset your password, you should contact The Partnership at helpdesk@chicookworks.org.

JOB SEEKER AND EMPLOYER IDENTITY

In order to maintain compliance with federal and local program reporting requirements, Career Connect contains sensitive information concerning the identities of job seeker and employer customers ("Personally Identifying Information" or "PII") including, but not limited to, name, address phone number, social security number, date of birth, driver's license number, and federal employer identification number (FEIN). **Under no circumstances shall Personally Identifying Information be utilized for personal profit or entertainment.**

ACKNOWLEDGEMENT

Read and initial each step below to indicate that you understand what is required and then sign and date below.

_____ I agree to abide by all terms and conditions contained in this Data Confidentiality and Security Agreement.

_____ I agree to use Career Connect in accordance with The Partnership's written policies and procedures.

_____ I agree to enter factual and accurate data into Career Connect to the best of my knowledge.

_____ I will use Career Connect and the data contained within solely for authorized purposes as described above and as required by my position.

_____ **I will not disclose any Personally Identifying Information** to anyone inside or outside of my organization that does not have access to that information in Career Connect unless:

- I am sharing job seeker contact, education, and work history information with an employer for the purposes of helping a job seeker obtain employment;
- I have written consent from a job seeker or employer client to share such information for the purpose of referring that job seeker or employer client to additional training or services;
- I have written consent from The Partnership; or
- I am required to do so by law, regulation, or subpoena (and will notify The Partnership of such).

_____ I will:

- maintain my username and password in the strictest of confidence and not share it with anyone inside or outside of my organization;
- immediately change them if I suspect their secrecy has been compromised; and
- immediately report activity that is contrary to the provisions of this agreement to my supervisor or The Partnership.

_____ I will be accountable and accept all responsibility for all transactions performed using my Career Connect username and access privileges.

_____ I will store any Personally Identifying Information extracted from Career Connect so that only authorized personnel can access it. Any physical data files will be stored in an area that is physically secure from access by unauthorized persons during both duty and non-duty hours. Any computer containing data files will be password protected. Passwords will be given only to personnel who require them for the performance of their job duties. Electronic files with Personally Identifying Information stored on external devices such as, but not limited to, thumb drives, flash drives, external hard drives and CDs, must be password encrypted. I will take all reasonable steps to maintain these data storage conditions and will not share keys, passwords, or other means to access the data with unauthorized users.

_____ I agree to immediately report to The Partnership any suspicious activity or security breach.

_____ I understand that my responsibility to ensure the confidentiality, security, and appropriate use of the Career Connect data continues after my termination of employment from my current organization.

I acknowledge that I have read and understand the information above and that my signature below signifies my agreement with the Career Connect Data Confidentiality and Security Agreement. I further acknowledge that the willful 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 The Partnership, and any other appropriate legal action.

Signature: _____

Date:

Print name:

Agency:

Street Address:

Suite #

City:

State:

Zip:

Job Title:

Office(s) – List Office(s) that you need access to. Please use the Career Connect Office Name(s).

1)

2)

3)

4)

Phone #:

Email Address: