Worker Connect

WORKER CONNECT USER RESPONSIBILITY POLICY

This Policy sets forth your responsibilities, as a user of the Worker Connect system, for safeguarding the privacy and security of all data to which you have been granted access in Worker Connect ("Worker Connect Information").

Permitted Use of Worker Connect

Your access to Worker Connect and Worker Connect Information has been approved by one or more agencies in New York City so that you may perform a specific job function, and you understand and agree that you will obtain, use, and disclose Worker Connect Information only to carry out tasks and responsibilities in connection with such job function ("Permitted Use"). Worker Connect provides legally authorized access to specific client demographic and program data owned by participating agencies. In some instances, access to such information is conditioned upon the prior written consent from the client whose data will be disclosed for the Permitted Use; in such cases, you must verify that written consent has been received from the client before accessing that individual's data.

Worker Connect management reserves the right to suspend your Worker Connect account if it determines that you are using the account in violation of the Permitted Use or any other terms of this Policy.

Confidential Information

You must treat all Worker Connect Information as confidential. This designation is consistent with the highest level of sensitivity under the DoITT's Citywide IT security data classification standards. Worker Connect Information includes, but is not limited to Personally Identifiable Information ("PII"), which is information that can be used alone or in combination with other information to identify or locate a person, and Protected Health Information ("PHI"), which can also include information about an individual's health status and heath care.

Consequences of Unauthorized Use or Disclosure of Confidential Information

Unauthorized use or disclosure or use of confidential information may cause substantial and irreparable harm to individuals whose personal information is misused or improperly disclosed. It may also damage an agency's reputation and ability to perform its business function. Improper use or disclosure of confidential information or failure to safeguard the privacy and security of such information may result in, among other consequences, the imposition of fines and other civil liability, dismissal from employment, criminal prosecution, and imprisonment.

User Monitoring

As a User of Worker Connect, you have no right to privacy when using the Worker Connect system. All content and use of Worker Connect is subject to monitoring and review by Worker Connect management. Any unauthorized use or disclosure of Worker Connect information, or suspicion of such actions, will be reported to the appropriate authorities.

Worker Connect

WORKER CONNECT USER RESPONSIBILITY POLICY

Safeguarding Worker Connect Information

Your responsibilities to protect Worker Connect Information include compliance with the following requirements:

1. Disclosure to Third Parties: You may not disclose Worker Connect Information to any third parties, or publish, sell, license, distribute or otherwise reveal this information.
2. Copying, Printing, Emailing and Faxing: You may not copy, print, email or fax Worker Connect Information except when absolutely necessary in connection with the Permitted Use for which you have been granted access to Worker Connect. When copying, printing, or faxing is complete, all documents must be removed from common areas and discarded or stored in a confidential and secure manner,

   Fax cover sheets and emails containing Worker Connect information must include the following language, and fax recipients should be called in advance to ensure proper receipt and management:

   "Confidentiality Notice: This communication, and any attachments, may contain confidential and privileged information for the exclusive use of the recipient(s) named above. If you are not an intended recipient, or the employee or agent responsible to deliver it to an intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please notify me immediately and delete or destroy this communication. Thank you."
3. Work Stations: You must lock your active workstation screen when it is left unattended.
4. Electronic Storage: You may not store Worker Connect Information on mobile devices (e.g., smartphones, tablets, laptops, etc.) or on removable data devices (e.g., USB drives, CDs, and external drives, desktops, etc.).
5. Social Security Numbers: You may not email, mail, fax, print or otherwise disseminate any Social Security Numbers obtained through Worker Connect unless expressly authorized by law, as determined, in advance and in writing, by counsel for both Worker Connect and the relevant agency data source(s).
6. Additional Responsibilities: If you observe any conditions that could cause Worker Connect Information to be compromised in any way, it is your responsibility to take action to safeguard this Information and immediately report the incident to your manager or to your unit director.
7. Passwords and Account Security: You may not share your Worker Connect account or password. You must adhere to the Citywide Information Security Password Policy which includes a requirement that passwords be a minimum length of eight (8) characters and be constructed using at least one alphabetic and one numeric or special character. The full Citywide Information Security Password Policy can be found here: http://cityshare.nycnet/html/cityshare/downloads/it_wireless/info_security_policies/Password.pdf

WORKER CONNECT USER RESPONSIBILITY POLICY

Post-Employment Obligations
Your obligation to safeguard the confidentiality of Worker Connect information shall survive the termination of your employment with New York City.

Miscellaneous
Worker Connect Management reserves the right to revise and otherwise change the terms of this Policy at any time and without notice. Any modification is effective immediately upon posting, unless otherwise stated. Your continued use of Worker Connect following the posting of any modification signifies your acceptance thereof. You should periodically visit this page to review it for any Policy updates or modifications.

Questions

Any questions about this Policy should be addressed to the Worker Connect team at: liaisons@hhsconnect.nyc.gov.