**COLORADO DEPARTMENT OF HUMAN SERVICES (CDHS)**

**Application for Access to**

**PeerPlace Aging, Food Processor and/or CBRES**

USE THE FOLLOWING INSTRUCTIONS TO COMPLETE THIS ACCESS FORM:

Form needs to be completed fully, including the contact information of the user, the name of the region and the provider, the user role, the user category, and the default program or they cannot be processed. Some of the information can be selected from the drop-down list on the form; the rest needs to be written in.

If the application is for PeerPlace access, here is what you need to select for the following categories:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of user** | **User Role** | **User Category** | **Default Program** |
| **AAA User who helps with user setup and training new users** | Program Administrator | AAA Wide / Area Agency on Aging | Internal Administration for respective AAA |
| **AAA User who only enters data into PeerPlace** | Program User | User / Staff | Historic Data for respective AAA |
| **Provider User** | Program User | User / Staff | Historic Data for respective AAA |

All access requires the AAA Director approval. Once it has been signed by the AAA Director responsible for the provider who is requesting access, the application should be submitted to the SUA (State Unit on Aging). It needs to be signed, scanned and e-mailed as an attachment to Doug Davis doug.davis@state.co.us or faxed to (303) 866-2977, ATTN: Doug Davis.

**Applicant Information:**

This section needs to be completed for all requests. Please fill out this information and have the AAA director sign on the page with the requested application(s).

If requesting a revoke or change in access for an existing user, enter the proper *User ID / Login ID*. If the application is creating a new user, CDHS will complete the *User ID/Login ID* section. The applicant and his/her supervisor must sign the application request on the last page.

Check “*ADD NEW USER*” if applicant has no existing access. Note if the user is replacing an existing user and include the existing user’s *User ID/Login ID* and attach a separate completed form requesting revocation of the existing user.

The new applicant and his/her supervisor both sign the System Application Statement of Compliance on the last page.

**WHAT HAPPENS NEXT?**

Users with access to Food Processor, CBRES, or the PeerPlace Aging System are required by CDHS policy to take a mandatory on-line security training.

The user and the AAA Director or his/her representative will be notified via e-mail where to log on to take the training, once a valid application has been received by SUA. After completion of the security training, the user will be set up on the requested application and the *User ID/Login ID* and password will be sent via secure e-mail to the user and the appointing AAA Director or his/her representative.

If the application is for the PeerPlace Aging system, SUA will set up any user with the Program Administrator role with access to all regional programs. Users with the role of Program User, will be set up with the default program only and it is up to the respective AAA’s Program Administrator to add all the programs they want the user to access.

**State Unit on Aging**

**Colorado Department of Human Services**

**Application Access**

[ ]  Add New User **EFFECTIVE DATE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

[ ]  Change User’s Access

**Applicant Information:**

Last Name: First Name: M.I.

Work Phone: Area code Phone # Extension:

Alternative Phone - daytime contact (8 – 5pm)

Email

PeerPlace Application Access:

Responsible AAA (Region): Choose an item.

Agency Name (Provider):

*Please check the appropriate box to Add or Remove access to the desired functions.*

 **ADD**

 [ ]  PeerPlace Aging System (Make sure to select the defaults on the three drop downs below)

 User Role: Choose an item.

 User Category: Choose an item.

 Default Program: Choose an item.

 [ ]  Food Processor (used by RDs and Nutrition Programs to complete nutrient analysis on menus and recipes only)

 [ ]  CBRES - Colorado Budget and Reimbursement Expenditure System (used by regions to bill SUA for service units provided)

Authorization: Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State Unit on Aging**

**Colorado Department of Human Service**

**System Applications Statement of Compliance**

(To be read and signed by new or change request for users of PeerPlace Aging, FoodProcessor , or CBRES)

It is the policy of this agency that the Executive Order dated July 1, 1978 & the Division of ADP Policy Statement regarding access of public records be strictly adhered to.

It is the public policy of this State that all public records shall be open for inspection by any person at reasonable times, except as provided in Part 2 of Article 72 of Title 24, C.R.S. 1973 as amended, or as otherwise specifically provided by law. The release of any information to the public, supplied through automated processes, shall not take place unless the following events have transpired:

* Written requisition delineating the desired information, records, or data must be received by the official custodian.
* The official custodian must determine if the requested information, record, or data constitutes public record and its disclosure is within the law.

All data resulting from the activities of an agency considered the private data of that agency. Use and dissemination of this data by any Government, or Corporate personnel is prohibited without the proper authority being given. The department’s Executive Director, the official custodian, must receive a written request for access to the department’s data prior to that data being released in any manner to any individual, government agency, or private concern. It is the requester’s responsibility to adopt adequate safeguards to protect data stored in their facility. Protection is to be in accordance with the FIBS Pus 41 May 30, 1975.

Any person who violates ARTICLE I (GENERAL-PROVISIONS) TITLE 26-1-114 subsection (1) or (3) is guilty of a misdemeanor and may be punished by a fine of not more than $500, or imprisoned in the county jail for not more than three months, or by both fine and imprisonment. The data supplied by the Colorado Department of Human Services shall be used only for official State business. Confidentiality of CDHS data from accidental, unauthorized, intentional, malicious modification, destruction, or disclosure must be maintained.

From **The Code of Colorado Regulations:**

* Users understand that the State of Colorado owns, through the Dept. of Human Services (State Departments), the various system applications and all information that can be accessed through the systems. Access to these systems is restricted to those who have been authorized by the State Departments and their organization’s Security Administrator to enter.
* Users are responsible for reading and complying with any/all applicable Privacy/Security Policies and Procedures as provided by the State Security Administrator.
* Users shall only use/disclose records and/or information that is created, received, maintained, or transmitted within these applications as authorized by the State Departments, and as required to perform authorized obligations and responsibilities.
* Users shall limit use/disclosure of records and/or information concerning State Program clients or applicants to the purposes directly connected with the administration, operation, or oversight of the applicable State Program.
* Users shall not knowingly cause or allow the addition, modification, destruction or deletion of any records and/or information accessible through state applications, except solely in the course of performing their authorized work.
* Users shall not make unauthorized use/disclosure of, or knowingly permit unauthorized access by others to, records and/or information contained within the applications used.
* Users shall maintain an assigned, unique User ID for each system application.
* **Users understand that they are responsible for any activity that occurs under their individual User ID.** In the event that a User suspects that another person knows and/or has used his/her User ID and Password, the User must notify his/her Security Administrator immediately. Additionally, it is a security violation for a User to mask his/her identity or assume the identity of another User.
* **Users shall practice adequate Password management by keeping Passwords confidential.**
* **Users shall not share their Passwords with anyone else for any reason, and are discouraged from writing down their Passwords and posting in view of others.**
* Users understand that the State Departments may monitor, track, and record all Users and uses of all system applications at any time.
* Users shall not attempt to alter, exploit, or otherwise interfere with any system application used. The State Departments have the right to update the system at any time.
* Users shall report any violations, or suspected violations of this Agreement immediately to their Supervisor and/or State Security Administrator and/or the State / County Security Administrator or Liaison.
* Users understand that any violation of this Agreement may be cause for sanction including account termination.
* System users who are designated as a State / AAA Administrator or Liaisons or a Backup State / AAA Administrator or Liaison also have the following responsibilities: Authorized State / AAA Administrators and Liaisons shall ensure system application Users are aware of any/all applicable Privacy/Security Policies and Procedures and any updates/clarifications provided by the Application Program Area and/or the State Security Administrator.
* Authorized State / AAA Administrators and Liaisons shall establish additional appropriate administrative, technical, procedural, and physical safeguards to ensure the confidentiality, integrity, and availability of client/applicant records and/or information created, received, maintained, or transmitted within CDHS system applications.
* Authorized State / AAA Administrators and Liaisons or designated State or AAA Information Technology personnel shall ensure all computers used to access any and all system applications are updated with current anti-virus software.
* Authorized State / AAA Administrators and Liaisons shall immediately notify the State Security Administrator to terminate account access for any user no longer authorized to perform required obligations and responsibilities within the designated counties.
* Authorized State / AAA Security Administrators and Liaisons shall serve as the initial contact for any privacy/security issue that requires escalation or investigation.
* Authorized State / AAA Security Administrators and Liaisons shall immediately report alleged or actual privacy/security incidents to the State Security Administrator. These would include any/all incidents that could affect the system such as virus incidents, unauthorized access, improper use/disclosure of client records and/or information, and any other activity that may be considered a violation, or suspected violation, of this Agreement.

**Additionally:**

* Food Processor users agree to use the Food Processor program solely for menu development, recipe development, and nutrient analysis of menus and recipes for the Older Americans Act Nutrition programs only.
* Food Processor users agree to not enter any client or individual(s) information into Food Processor, including de-identified information for any reason.
* Users agree to attend occasional training sessions, as required by the SUA or AAA, to maintain a sufficient level of knowledge about providing valid data and keep up with changes to the systems as those affect their use of such systems
* Users who do not log on to any of the systems for a period of six months will get their access to that system revoked, without prior notification of such access loss.
* AAA Security Administrators/AAA Directors will notify the SUA immediately to revoke user access for any user who resigns or no longer needs access to SUA systems for any other reason.
* AAA Security Administrators/AAA Directors will make sure the user receives adequate training in the SUA systems. If such training cannot be accomplished locally, the AAA Security Administrators/AAA Director will make arrangements for training with the SUA.
* All internet traffic used while connected to the Food Processor Program will be monitored and any miss use of this connection can result in a revocation of access to the system.

**SUA User Agreement**

By signing this agreement, the User agrees: 1) to safeguard any information accessed on any SUA system according to the rules of confidentiality and release of information as specified in the Colorado State Department of Human Services, Volume 6; and 2) to utilize the information solely for business purposes, and inquiry into any case that the user has a personal interest in, whether a party to the case or an acquaintance of a party to the case, is strictly prohibited. The SUA reserves the right to edit/update this Agreement at any time.

**FOR SECURITY PURPOSES: Only To Be Completed by User**:

**By signing this Agreement, I consent and agree to be bound by all of the terms and conditions listed above, and I understand that any failure to comply with these terms and conditions may result in sanction, which can include termination of my user account. This Agreement applies to my granted access to any and all system applications provided by the Colorado Department of Human Services. Execution of this Agreement is required before access will be granted. I understand the account(s) assigned to me by the State Unit on Aging - Colorado Department of Human Services grants me access to information, which may be confidential.**

I understand that my daily job responsibilities and activities in regards to this account may involve viewing sensitive and/or confidential data. I accept the responsibility for protecting this account from unauthorized access and agree to ensure that the access to this account is not disclosed to any other individual.

**FOR SECURITY PURPOSES ONLY** (To Be Completed by User and Supervisor):

Employee’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor’s Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_