Texas Penal Code, Title 7,33.02 Breach of Computer Security, states:
(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.
(c) An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:
   (1) a state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or
   (2) a felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.
(d) A person who is subject to prosecution under this section and any other section of the code may be prosecuted under either or both sections.

Security Policies and Procedures

Providers accessing DFPS systems and information are restricted to that which is necessary to perform assigned duties and is for approved official agency business purposes only.

The operator must sign off the application each time he/she leaves or whenever the terminal is unattended.

Provider supervisors must notify the DFPS Program Specialist of staff terminations, prior to the staff person's last day of employment in the current position, to coordinate removal of access to the web page.

Any issued ID and/or password is for official state-approved business only. IDs and/or passwords must be kept confidential and cannot be shared with anyone. Do not use initials, names, or something easily guessed for a password. Passwords should be a minimum of eight (8) characters and or numbers. If a password is forgotten or becomes unusable the personal identification code word will be needed to verify the user's identity before assistance is provided to access the system. The code word should be easily remembered and not shared with any other person.

Providers are prohibited from changing any computer software ("Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network) that reside on any DFPS computer system ("Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network) or automated storage medium unless this change is approved by authorized DFPS Information Technology staff.

Providers are prohibited from accessing any automated system, subsystem, or automated storage medium for which they have not previously received proper authorization. Providers are prohibited from altering any data or database other than that which is specifically authorized as required in the performance of assigned work.

Information which may come to the Provider's knowledge while using the DFPS computer system is confidential and may not be disclosed except as expressly authorized by DFPS management and may only be discussed with authorized persons. Providers may not access or read anything in the computer files or systems except as authorized by DFPS management. By law, information in DFPS files is confidential. It is unlawful to change, alter, or damage files. Only authorized staff may change confidential information. (TX Criminal Law, PC 33.03)

Copyrighted material, including but not limited to commercial computer software, which may be made available to Providers by DFPS, is protected by copyright laws and is not to be copied for any reason without permission from the copyright owner and DFPS. Violation of copyright laws, including those applicable to computer software, may result in fines and/or other legal action. This includes both copying and altering licensed software and applying to systems software, application packages, documentation, or other material provided by vendors.

If Providers have any questions or problems, they are to immediately report the situation to their CYD ☑ PEI ☐ STAR ☐ YFH ☐ Contact.

In addition to restrictions on unauthorized access to information on computer files, the operator must be aware of the limitations on releasing information in computer files. Questions concerning release of information, should be directed to the DFPS Supervising Attorney.

Providers agree, by signing this agreement, that they understand the stated policies and procedures and that these apply to all security codes the Provider receives to conduct state-related business. Providers further understand that failure to follow the policies and procedures, and laws of the State of Texas may result in loss of access to DFPS computer system(s) and their ability to perform any duties on DFPS systems. Failure to follow these policies and procedures may result in disciplinary action under any contract which the Provider may have with DFPS, which may include termination of the contract. Under certain circumstances, the violation of the policies against the use of the equipment and the confidentiality of information may result in criminal prosecution.
Texas Department of Family and Protective Services

DPEI (DIVISION OF PREVENTION AND EARLY INTERVENTION) ❑
DFPS (DEPARTMENT OF FAMILY AND PROTECTIVE SERVICES)
CYD ❑ PEI ❑ STAR ❑ YFH ❑

SECURITY AGREEMENT

The following policy is necessary to ensure the security and integrity of confidential DPEI ❑ ECI ❑ DFPS ❑ client and administrative data which will be accessed via the DPEI ❑ ECI ❑ DFPS ❑ Web Page. The DPEI ❑ ECI ❑ DFPS ❑ Web Page is an automated system maintained by the Department of Family and Protective Services (DFPS). For purposes of this agreement, Provider shall mean each employee or staff person working for the Contract Provider. Please read the following agreement thoroughly before signing.

INSTRUCTIONS:
1. A separate form must be completed by each user for each program to which access is requested.
2. The form must be signed by the user, whose signature indicates agreement with the security policies and procedures detailed on this page and on Page 2.
3. Provider staff seeking access must obtain the approval and signature of their supervisor and DPEI ❑ ECI ❑ DFPS ❑ Contact.
4. Sand completed agreement to your DPEI ❑ ECI ❑ DFPS ❑ Contact.
5. DPEI ❑ ECI ❑ DFPS ❑ Providers must notify their DPEI ❑ ECI ❑ DFPS ❑ Contact immediately upon user’s termination via phone and follow-up with the written Remove User request. The DPEI ❑ ECI ❑ DFPS ❑ Provider will be held responsible for all transactions completed by their staff while accessing the DFPS Network and DPEI ❑ ECI ❑ DFPS ❑ Web Page.

[☐] Add DPEI ❑ ECI ❑ DFPS ❑ Access [☐] Edit DPEI ❑ ECI ❑ DFPS ❑ Access [☐] Inactivate DPEI ❑ ECI ❑ DFPS ❑ Access
Provider Name:
Provider # (if known):

Types of Access:
- PEI
  - Provider With Reports
  - Provider Without Reports
  - State Level
  - Administrative Maintainer (State)

- STAR / CYD
  - Provider
  - Contract Specialist
  - State Level

- YFH
  - Volunteer
  - State Staff
  - Other [specify]

USER INFORMATION (Please type or print clearly)

<table>
<thead>
<tr>
<th>First Name</th>
<th>Middle Initial</th>
<th>Last Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Title: Social Security Number:

Work E-mail Address: Work Telephone:

Hint: Personal Identification Code: (For verification purposes)

Date of Birth:

APPROVAL

User’s Supervisor Name (Print or Type):

User’s Supervisor Signature:

Date:

DPEI Approver (Print or Type):

DPEI Approval Signature:

Date:

AGREEMENT

I understand I will receive a User Identification Code (User ID/Login) and a password that will allow me access to the DPEI ❑ ECI ❑ DFPS ❑ Web Page application. I understand that I am responsible for any actions performed under my User ID. I agree to change my password immediately if I know or suspect that my password has been compromised (if, for example, someone learns my password or it becomes known during problem functions).

I have read Page 2 (Appendix A, DPEI ❑ ECI ❑ DFPS ❑ Security Agreement) of this agreement related to data security and data confidentiality and agree to follow all policies and procedures as defined. I understand that the policies and procedures stated above and on Page 2 apply to all security codes I receive to conduct state-related business. I understand that failure to follow the policies, procedures, and laws of the State of Texas may result in loss of access to the web page application as well as civil and/or criminal prosecution.

USER’s Signature:

Date:

FOR DFPS USE ONLY

Temporary Network Password: Login: PEIS password:

User Login Date: Browser: NS ❑ IE ❑ Other:

IT SECURITY ADMINISTRATION

Received: Completed By:

Date Completed: