

Attachment 2



## Employee and Non-Employee Acknowledgment of Confidentiality

### Confidential case records.

OKDHS case records are confidential. Employees and non-employees are prohibited from accessing or viewing these records for any reason other than performance of assigned duties. Employees are prohibited from removing case files from any office outside of routine, official business processes without expressed consent from a supervisor.

Unauthorized disclosure of case records is prohibited by State and Federal law. Disclosure of certain records, such as records relating to child abuse and neglect, is also punishable as a crime under Oklahoma law. [10 O.S. §7107 and 56 O.S. §240.22C] Access to confidential databases, such as tax and earnings history, may not be used for any purpose other than performance of assigned duties. Unauthorized access or improper disclosure of case records or database information may result in disciplinary action, up to and including discharge from employment.

### Computer and Internet usage.

OKDHS provides personal computers for staff use in the performance of their assigned job duties. In this regard, every employee must be aware of, and adhere to, the following restrictions and guidelines.

1. There is no expectation of privacy for use of an OKDHS computer for any purpose, whether business or personal. This may include, but is not limited to, the use of OKDHS network services local area network (LAN), Internet, including e-mail, and Web site browsing.
2. OKDHS may audit the use of any computer provided to any of its agents and employees to identify unauthorized activity. Audits review stored data, read and monitor electronic mail, record Web sites visited, and delete unauthorized files.
3. Uses of OKDHS computers for non-job-related activities must be minimal and must not diminish the number of actual hours worked or impede the employee's ability to complete tasks for which the employee is responsible.
4. Any action that threatens security or integrity of programs or data on any OKDHS computer must be avoided. Any action that might be in violation of any software license must be avoided.
5. Unacceptable use of OKDHS computers includes, but is not limited to:
  - displaying, viewing, storing, printing, or sending vulgar, offensive, or harassing material to anyone;
  - accessing sexually oriented Web sites, or storing, or viewing sexually oriented graphic images;
  - accessing sites for gambling, such as on-line casinos;
  - accessing sites to sell personal property, such as on-line auction services;
  - using OKDHS computers or equipment for outside business interests;
  - initiating or forwarding chain letters, or any non-job-related messages urging recipients to forward them to others;

- Intentionally or recklessly Introducing a virus or virus-like program onto an OKDHS computer;
- encrypting or password protecting data stored on OKDHS computers without prior written approval of the Data Services Division (DSD) and adherence to any conditions imposed upon such approval. Use of password protected data available in a read only status is permissible. See <http://infonet/office/dsd/ets/sec/docs/internetusagepolicy.htm> for a list of other approved uses of encryption and password protection;
- accessing confidential client records for purposes unrelated to performance of job duties;
- transferring confidential client records to persons unauthorized by law to receive such information;
- using software in such a manner as to violate copyright laws;
- loading personal copies of software not licensed to OKDHS or approved for use in OKDHS computers. A list of approved software is located at <http://infonet/office/dsd/ets/sec/docs/internetusagepolicy.htm>.
- loading, downloading, or using any software harmful to the operation of OKDHS computers; or
- using any screen saver not supplied with an OKDHS workstation.

**Failure to abide by these restrictions and guidelines may result in disciplinary action, up to and including, termination from employment, based on the severity of the violation. Access to computers or certain computer functions, such as e-mail, LAN, or the Internet, may be suspended or denied at the sole discretion of OKDHS. OKDHS reports any facts reasonably believed to be a violation of State or Federal criminal law to appropriate law enforcement authorities for prosecution.**

6. Access to the Internet from the OKDHS network is through a single access point.
7. An approved level of encryption must be used when transmitting confidential OKDHS data over the Internet, by use of Internet e-mail or file transfer, using DSD procedures. Transmission of confidential data over the Internet requires prior approval by the DSD Data Security Unit.

I acknowledge that I will comply with the restrictions and guidelines set forth above. I further acknowledge that I will abide by State and Federal laws regarding confidentiality of client records.

I understand that failure to comply with and sign acknowledgment of these terms may result in disciplinary action, up to and including, termination from employment, and prosecution of criminal violations.

_____ Employee signature	_____ Title	_____ Job code
_____ Employee printed name	_____ User ID number	_____ Date
_____ Non-employee signature	_____ Title	_____ Job code
_____ Non-employee printed name	_____ User ID number	_____ Date



OKLAHOMA DEPARTMENT OF HUMAN SERVICES



**Logon Authorization Request  
for Non-OKDHS Employees**

**Section A. Action requested**

- Assign User Identification
- Re-activate User Identification
- Cancel User Identification
- Change User Information

User ID:	_____
Effective date:	_____
Expiration date:	_____
<b>Required</b>	

**Section B. Requestor information**

Last name	M.I.	First	Social Security number	
Job title	Phone	Organization name		
Office street address	City	State	Zip	

**Section C. Privileges requested**

OKDHS network	Local area network (LAN)		
IMS <input type="checkbox"/> IMSTEST <input type="checkbox"/> E-MAIL <input type="checkbox"/> TSP system <input type="checkbox"/> List specifics.	System name	Server name	CO #

**Section D. Requestor acknowledgment**

I, the undersigned, understand that the information which this user identification enables me to access, is to be utilized only in the performance of my assigned duties as an employee of the above-named organization. I therefore agree to make no inquiry or updates which are not required for the performance of these duties. I am aware that there are numerous federal statutes and numerous statutes of the State of Oklahoma making information confidential and that these statutes carry penalty provisions. Therefore, I will keep confidential any information made available to me. In addition, I agree not to divulge or share any terminal access information with anyone. I understand that my failure to comply with security procedures may result in termination of my access to information.

\_\_\_\_\_

Requestor signature Date

Last name	M.I.	First	Social Security number
-----------	------	-------	------------------------

**Section E. Approval signatures.**

USER supervisor	Phone	Date
Decentralized security representative signature		Date
Data security administrator signature		Date

Attachment 4



OKLAHOMA DEPARTMENT OF HUMAN SERVICES



## Agreement to Safeguard Federal Tax Information

Federal tax returns and federal tax information are confidential (26 U.S.C. § 6103). Child Support agencies may only use federal tax information for establishing and collecting child support obligations.

Unauthorized inspection of federal tax information can result in both a:

- a) Misdemeanor punishable by a fine up to \$1000, Imprisonment up to 1 year, and the cost of prosecution (26 U.S.C. § 7213A); and
- b) Civil judgment to the taxpayer of \$1000 or actual damages, whichever is greater, attorney fees, and the cost of action (26 U.S.C. § 7431).

Unauthorized disclosure of federal tax information can result in both a:

- a) Felony punishable by a fine up to \$5000, Imprisonment up to 5 years, and the cost of prosecution (26 U.S.C. § 7213); and
- b) Civil judgment to the taxpayer of \$1000 or actual damages, whichever is greater, attorney fees, and the cost of action (26 U.S.C. § 7431).

All persons with access to Oklahoma Child Support Services (OCSS) reports, files, and records have access to federal tax returns or federal tax information. This information must never be printed. Printing for any reason, or viewing or disclosing such information for any reason other than establishing or collecting child support obligations will result in:

- a) Referral to appropriate state or federal law enforcement or prosecution authorities;
- b) Referral to the Office of the Inspector General (OIG) for investigation of potential or alleged misuse;
- c) Disciplinary action, including termination of employment, termination of any contract that authorizes offending users continued access to the OCSS computers, files, or records; or offset of amounts due to employees or contractors to reimburse OKDHS for any civil or criminal penalties imposed for unauthorized use.

I acknowledge that I have access to federal tax returns and federal tax information. I certify that I have read and understand the above statements regarding the inspection or disclosure of federal tax information.

I agree to maintain the confidentiality of federal tax returns and return information in accordance with the provisions of the Internal Revenue Code (26 U.S.C. § 6103).

I understand that failure to safeguard confidential data may result in the imposition of penalties, including fines, costs of prosecution, dismissal from office, discharge from employment, and imprisonment (42 U.S.C. § 653(1); 26 U.S.C. §§ 7213, 7213A, 7431; 5 U.S.C. § 552a(l)).

If I observe any conditions, which could cause federal tax returns and return information to be compromised in any way, I understand that it is my responsibility to take action to safeguard OCSS data and report the incident to my manager.

I agree that my obligation to safeguard the confidentiality of federal tax returns or federal tax information shall survive the termination of my employment.

---

Signature

Date

## ATTACHMENT 5

### **Authority Matrix**

Person	Migration approval responsibilities
<p><b>Migration authority</b></p> <p>(minimum of one person from each entity within CBPE attends)</p> <ul style="list-style-type: none"> <li>• CBPE Security Representative is the final authority</li> </ul>	<ol style="list-style-type: none"> <li>1. Each member attends weekly migration meeting</li> <li>2. Ensure all migration approval steps are complete, as appropriate.</li> <li>3. Technical PIT lead makes sure the end user business community is aware of any changes made.</li> <li>4. The CBPE Security Representative authorizes migration if procedures are followed and authorizations have occurred.</li> </ol>
<p><b>Analysts</b></p> <ul style="list-style-type: none"> <li>• Contractor</li> <li>• ISD Development Staff</li> </ul>	<ol style="list-style-type: none"> <li>1. Updates the migration sheet prior to the Migration meeting when a change or Project is to move to IMSTRAIN.</li> <li>2. Attends weekly migration meeting.</li> <li>3. Ensures proper security has been requested for new transactions.</li> <li>5. Notify CSED IT Security Representative when there are new transactions or Reports.</li> <li>6. Requests the ISD CM# providing description of changes three working days prior to the anticipated IMSPROD Migration.</li> <li>7. Provide QCT testing status</li> <li>8. Remove information from migration sheet one week after the item has been moved to IMSPROD.</li> <li>9. Ensure migration occurred on scheduled date and inform migration meeting attendees that it did.</li> </ol>

Person	Migration approval responsibilities
<b>DSD Change management coordinator</b> <ul style="list-style-type: none"> <li>• ISD staff</li> </ul>	<ol style="list-style-type: none"> <li>1. Attends weekly migration meeting</li> <li>2. Provides CM# for each change or project.</li> </ol>
<b>Migration Facilitator</b> <ul style="list-style-type: none"> <li>• Contractor</li> </ul>	<ol style="list-style-type: none"> <li>1. Attends and facilitates migration meeting</li> <li>2. Creates weekly migration sheets to distribute in the meeting.</li> <li>3. Updates and Distributes the final sheet after the migration meeting.</li> <li>4. Ensures required individuals are present for the meeting.</li> </ol>
<b>CBPE Security Representative</b> <ul style="list-style-type: none"> <li>• CBPE Security Representative</li> </ul>	<ol style="list-style-type: none"> <li>1. Requests security for new transactions.</li> <li>2. Updates the Report matrix &amp; OIL documentation</li> </ol>

## ATTACHMENT 6

### Oklahoma Department of Human Services Child Support Enforcement

#### Experience and Skill Matrix for Proposed Staff

Name	Title	Position
	Skill Set	Years of Experience      Last Year Tool or Skill used
1	High Level Technical Management	
2	Lan/PC Mainframe Communication	
3	Client/Server Architecture Development Experience	
4	System Life Cycle	
5	Diagnose/Debug Code	
6	PC Databases	
7	PC Operating Systems – Windows XP, Win7, Linux, Unix	
8	PC Databases (Access)	
9	Efficient Modular Code	
10	Microsoft NT/LAN Operating systems Experience and Problem Resolution	
11	Business Requirement Analysis/Functional Design	
12	Child Support experience	
13	Cobol (Microfocus), Cobol II, MVS Cobol	
14	OSIS (Oklahoma automated child support system)	
15	Java	
16	Data Analysis	
17	Visual Basic	
18	.Net	
19	Microsoft Office (Word, Excel, Powerpoint, Outlook, Visio)	
20	Microsoft Project	
21	Powerbuilder	
22	Batch Message Processing (BMP) checkpoint/restart	
23	On-Line Large Scale IMS Applications	
24	Proficiency in TSO	
25	IMS database design	
26	SQL Database Design and Optimization	
27	IBM JCL	
28	Project Management (PMI principles)	
29	Written Communication (developing clear, concise, and detailed requirements and design documents)	
30	SQL	
31	DB2	
32	Oracle	
33	Application Servers (jboss, tomcat, websphere, etc...)	

