Missouri Department of
SOCIAL SERVICES

DSS CONFIDENTIALITY & INFORMATION SECURITY AGREEMENT

This agreement applies to all Department of Social Services (DSS) workforce members including DSS employees, volunteers, contract workers, trainees, interns and other persons who are in a DSS facility or access/use DSS information systems in a regular course of business. Examples of information systems include DSS local and statewide communication networks, computers connected to these networks, laptops, Personal Digital Assistants (PDA's), database storage, electronic record systems, internet and e-mail, facsimiles, stand-alone personal computers, mainframe systems, on-line services, computer files, and production systems.

As a DSS workforce member, you may have access to confidential information and records, including information created and/or stored in any information system. You are required to keep confidential all information made available to you in the performance of your duties. You are responsible for assuring confidentiality of such information and releasing information only to authorized agencies or individuals as provided for by law and/or policy. It is your responsibility to check with supervisors/managers if unsure whether particular information is considered confidential.

You are prohibited from accessing or making inquiries or updates to information systems and/or records that are not required in the performance of your duties. For mainframe programs (e.g., child abuse records, client case records), only individuals specifically authorized by DSS may access these systems and use must be limited to work-related activities and inquiries (e.g., it is prohibited for workforce members to access information regarding themselves, friends, relatives or a case that is not in their caseload).

You are responsible for all use associated with your assigned unique User ID and password and care should be taken to protect the confidentiality of such. User IDs and passwords should not be shared with anyone under any circumstances. Use of unauthorized User IDs or passwords to gain access to information systems is prohibited.

Any written, recorded or electronically retrieved or transmitted communications that are harassing, discriminatory, defamatory, offensive, demeaning, insulting, threatening, intimidating, sexual, pornographic, inappropriate, breaching confidentiality, or in violation of copyrights is prohibited. You should immediately report to your supervisor/manager the receipt of any inappropriate, threatening and unsolicited communications, any accidental access to Internet sites, and any unauthorized use of DSS information systems by others.

You **DO NOT** have any personal privacy rights regarding your use of DSS information systems. Your **USE** of DSS information systems indicates that you understand and **CONSENT** to DSS' right to inspect and audit all such use. All DSS information systems and any matter created, received, accessed, stored or transmitted via DSS information systems are the property of DSS. DSS may override any individual password and access, inspect, copy and monitor your use of information systems and technology including all information transmitted by, received from, or stored on such systems any time deemed appropriate, with or without notice to you.

Electronic communications are subject to provisions of the Open Meetings and Records Law. For confidentiality purposes, caution should be used when sending work-related information of a sensitive nature (e.g., personnel matters, performance issues, and discipline issues). Any protected health information that is disclosed should be done so in accordance with the Health Insurance Portability and Accountability Act (HIPAA) provisions and DSS policy.

State and federal statutes and DSS policy require confidentiality of information and records and provide penalties for the unauthorized access, use, release and/or commission of a fraudulent act with regard to such information (refer to page 2). Violations of statutes and DSS policies may result in disciplinary action, up to and including suspension, dismissal and civil or criminal court action.

If the vendor provides any "personal information" as defined in §105.1500, RSMo concerning an entity exempt from federal income tax under Section 501(c) of the Internal Revenue Code of 1986, as amended, the vendor understands and agrees that it is voluntarily choosing to seek a state contract and providing such information for that purpose. The state will treat such personal information in accord with §105.1500, RSMo.

By signing this Agreement I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it. If I am a DSS employee or trainee, this form will be placed in my official DSS personnel file. If I am a non-DSS employee, this form will be maintained by the DSS divisional information security officer.

Workforce Member's Name (Please Print)	Social Security Number
Workforce Member's Signature	**Date**

Distribution Section

Completed forms by DSS employees should be sent to divisional human resource managers or designees. The divisional human resource manager or designee will forward to the Human Resource Center for inclusion in the employee's official personnel file.

Completed forms for non-DSS employees should be sent to the individual or address listed as follows:

Name

DSS Office of Workforce & Community Initiatives

Address (Street, City, State, Zip Code)

P.O. Box 2320, Jefferson City, MO 65102-2320

Important Notice

There are many state and federal laws and regulations that safeguard client information. These laws mandate the use and protection of all facts and circumstances of the client when determining his/her eligibility. Regardless of how the information is obtained, whether by collateral, document, computer match, etc. It is to be treated confidentially. Some of the laws and regulations concerning confidentiality and your liability are listed below. This is not an all-inclusive list but just a sample of the laws and their consequences for unauthorized disclosure of confidential information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) - Protects the privacy of client health information and establishes civil and criminal penalties for violations of this regulation. There is a $100 civil penalty up to a maximum of $25,000 per year for each standard violated and a graduated criminal penalty that may escalate to a maximum of $250,000 for particularly flagrant offenses.

Internal Revenue Code - Section 7213 (A) - Makes the unauthorized disclosure of Federal Tax Returns or return information a felony punishable by a $5,000 fine, up to five years imprisonment or both, together with the costs of prosecution. Unauthorized disclosure may also result in disciplinary actions, including dismissal by the Department of Social Services.

IRS - Section 7431 permits a taxpayer to bring suit against individual staff for civil and punitive damage in U.S. District Court for willful disclosure or gross negligence. These penalties apply for unauthorized disclosures of returns and return information even after Department of Social Services employment terminates.

IRS - Section 6103 - Prohibits a person from willfully disclosing any return or return information, except as authorized by Title 26 of the United States Code.

IRS - Section 2651 (DEFRA) requires that Social Security information from computer matches be treated the same as IRS data (26 U.S.C. 6103). The same penalties apply for the unauthorized disclosure of the claimant's circumstances.

The 1997 Taxpayer Browsing Protection Act provides a penalty for the willful, unauthorized access or inspection of federal tax information, both electronic and paper formats. Upon conviction, the criminal misdemeanor penalty is a fine of up to $1,000 and/or imprisonment up to one year. Civil damages for finding of liability are up to $1,000 or actual damages whichever is greater. If gross negligence or willful unauthorized inspection of disclosure, punitive damages may be assessed. **For further information, please refer to Internal Revenue Code - Section 7213 (A).**

Income Maintenance - #42 - Section 431.300-431.307 and 208.120; #45 - Section 205.50 - Makes the sharing or releasing of Income Maintenance information from the case record, microfiche, terminals or computerized printouts to anyone but the client a violation of the law. Workers violating this section may be sued in court, disciplined or fired.

Wage Data Utilization by the States - #45 - Section 403, PL 95-216. Wage data utilization is protected by Chapter II, Title 45, Code of Federal Regulations, parts 205 and 206. Section 272.8 Income and Eligibility Verification system - (IEVS) - requires state agencies to use IEVS. IEVS also requires states to use SAS, IRS, UIB, SEU and SSI income to determine eligibility. These regulations specify the requirements for state agencies to request wage data from the state unemployment compensation agencies.

Unemployment Insurance - 20 CFR 603.6-7 - Information may be used only to administer specific programs and may not be shared with unauthorized persons. Violations of this section may result in suspension, fines or dismissal.

Food Stamps - 7 CFR 272.1(c) restricts the use of Food Stamp information obtained on applicants or recipients of Food Stamps to persons directly connected to the administration of the Food Stamp Act or regulations, other Federal assistance programs, or people who are directly connected to programs required by the Income and Eligibility Verification System (IEVS) legislation. Workers making unauthorized disclosures are in violation of the law and may be subject to suit, discipline, or termination of employment. Information released to the State agency pursuant to section 6103(1) of the Internal Revenue Code of 1954 shall be subject to the safeguards established by the Secretary of the Treasure in Section 6103(1) of the Internal Revenue Code and implemented by the Internal Revenue Service in its publication, Tax Information and Security Guidelines.

Department of Health and Senior Services - 193.245 RSMo - The unauthorized disclosure of information from the DHSS files is a violation of state and federal law and the worker may be found guilty of a misdemeanor.

Missouri State Children's Services Law - 208.120, 210.110-210.150 and 453.120 RSMo. Children's Services Procedure Handbook (A8-A9, B-7, C13-C14, D26-D27, and E17-E18). Missouri State law requires Family Support Division to determine the eligibility from all facts and circumstances surrounding the claimant, including his living conditions, earning capacity, income and resources, from whatever resource received. All reports made by the local offices and central registry shall be confidential. Any violations of Sections 210.110- 201.165 shall be guilty of a Class "A" Misdemeanor (punishable by a fine of up to $1,000 and/or a jail sentence of up to one year.) Violation of 453.120 RSMo is a Class "C" Misdemeanor. Children's Services case files contain Child Abuse, Protective Services and Alternative Care information which is restricted by these laws. Access, with the Family Support Division, is only to specific workers on a need to know basis.