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, trainees, volunteers, contractors, interns and other persons who have access to or use DSS information systems and records in the course of business, on-site and from alternate work sites. Examples of information systems include DSS local and statewide communication networks, computers connected to these networks, stand-alone PC's, laptops, mobile electronic devices, database storage, electronic record systems, paper records generated from information systems, internet and email.

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 or through your association with DSS. 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 or your divisional privacy officer if unsure whether particular information is considered confidential.

You are prohibited from accessing or viewing information regarding yourself, friends, relatives, a case that is not in your assigned work load or making any other inquiries or updates that are not required in the performance of your official 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.

You are responsible for all use associated with your assigned 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. Passwords are only to be used to gain access for the execution of official state business.

Any written, recorded or electronically retrieved or transmitted communications that are harassing, discriminatory, defamatory, offensive, romantic, sexual, pornographic, inappropriate, breaching confidentiality, or in violation of copyrights is prohibited. You should immediately report to your Security Information Officer/Privacy Officer(s) and appropriate management staff the receipt of any inappropriate, and unsolicited electronic communications, any accidental access to inappropriate internet sites and other security incidents as outlined in DSS Policy 6-100.

You are expected to use DSS property only as intended and authorized for the performance of your job duties. You are prohibited from using DSS information systems and equipment for personal reasons. E-mail and Internet are to be used for work-related reasons only.

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 including all information transmitted by, received from, or stored on such systems any time it is deemed appropriate, with or without notice to you.

Employees should be aware that DSS may observe content and information made available by employees through personal social media use and accounts. Examples of social media include, but are not limited to: Facebook, Twitter, Instagram, Snapchat, and/or blogs. The same standards of conduct found in DSS Policy 2-101 (Sexual Harassment/Inappropriate Conduct), DSS Policy 2-115 (Work Rules), DSS Policy 2-119 (Confidentiality), DSS Policy 2-120 (Code of Conduct) and DSS Policy 2-500 (Conflict of Interest) apply to social media. Do not use social media while on work time or on work equipment, unless it is work-related and authorized by your supervisor. Do not use your DSS email address to register on social networks, blogs, or other online tools utilized for personal use. For more information, refer to DSS Policy 6-100 (Information Security Management). Employees are not to publish, post, or release any work-related information or pictures that are considered confidential or not public. Employees must refrain from off duty conduct that tends to bring state service into public disrepute or negatively affects the employee's job performance.

Electronic communications are subject to provisions of the Open Meetings and Records Law. Transmitting information of a confidential or sensitive nature (e.g., personal matters, performance issues, and discipline issues) via e-mail to entities that do not have a mo.gov e-mail address is only permitted if the e-mail is encrypted. 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 dismissal, as well as prosecution in a court of law.

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

Address (Street, City, State, Zip Code)

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. **In any instance of unauthorized disclosure of confidential information, employees may be subject to fines, criminal prosecution and disciplinary action, up to and including dismissal from employment.**

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 - 26 U.S.C. 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.

Internal Revenue Code - 26 U.S.C. 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.

Internal Revenue Code - 26 U.S.C. section 6103 - Prohibits a person from willfully disclosing any return or return information, except as authorized by **Title 26 of the United States Code**.

Section 208.120 RSMo - Prohibits the sharing or releasing of Income Maintenance information from the case record, microfiche, terminals or computerized printouts to **anyone but the client** except as needed for purposes directly connected with the administration of public assistance.

Section 208.155 RSMo - Prohibits the disclosure of any information concerning applicants and recipients of medical assistance (MO HealthNet or Medicaid benefits) except for purposes directly connected with the administration of the medical assistance program.

Wage Data Utilization - 45 CFR 205.50.7 CFR 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. This data is protected from disclosure by the laws governing the programs IEVS draws data from, as well as **section 208.120 RSMo.**

Unemployment Insurance - 20 CFR Part 603 - Information may be used only to administer specific programs and may not be shared with unauthorized persons.

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.

Department of Health and Senior Services Vital Statistics records - 193.245 RSMo - The unauthorized disclosure of information from the DHSS vital statistics files is a violation of state and federal law. Violation is a Class A misdemeanor.

Missouri State Children's Services Law - sections 210.110-210.165 RSMo - State law provides that all reports made by CD local offices and the central registry shall be confidential. Violation is a Class A misdemeanor, punishable by a fine of up to $1,000 and/or a jail sentence of up to one year.

Adoption information – sections 453.120 and 453.121 RSMo - Prohibits the disclosure of <u>any</u> information pertaining to an adoption to anyone, to include the adopted children or the adoptive parents. Violation is a class C misdemeanor.