

California Department of Social Services (CDSS)
Confidentiality and Security Requirements for
CALIFORNIA STATE AGENCIES
Interagency Agreements/Memoranda of Understanding

I. GENERAL REQUIREMENTS

- 1.1 These requirements provide a framework for maintaining the confidentiality and security of confidential data the State agency gathers or processes in the course of carrying out the terms of this agreement with CDSS. Definitions of commonly used terms are provided. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data*.
- 2.1 No exceptions from these policies shall be permitted without the explicit, prior, written approval of authorized CDSS staff. All confidentiality and security requirements, as stated in this agreement, shall be enforced and continue throughout the term of the agreement. Data protection and security plans may be required prior to receipt of confidential data.
- 3.1 In addition, the State agency will be expected to demonstrate that it has taken specific steps to ensure the data is kept secure and confidential as evidenced by, at minimum, the following:

II. PRIVACY, SECURITY, AND CONFIDENTIALITY

- 1.1 All confidential data made available in order to carry out this Agreement, will be protected from unauthorized use and disclosure through the observance of the same or more effective means as that required by the State Administrative Manual, sections 4840 et. seq., Civil Code 1798 et. seq., Welfare and Institutions Code 10850, and other applicable federal and/or State laws governing individual privacy rights and data security. Upon request, CDSS reserves the right to review, and then accept security and privacy procedures that are relevant to its data.

The State agency is responsible for the security of the confidential data and compliance with the terms of this agreement by its employees, contractors, or sub-contractors.

III. ACCEPTABLE USE AND DISCLOSURE

- 1.1 The State agency shall not use or further disclose confidential data other than as permitted or required by this agreement.

- 2.1 The State agency shall refer any persons not included under this agreement with CDSS, to CDSS to request access to the confidential data.
- 3.1 The State agency agrees that the information obtained will be kept in the strictest confidence and shall make information available to its own employees only on a "need to know" basis. Need to know is based on those authorized employees who need information to perform their official duties in connection with the uses of the information authorized by this agreement.
- 4.1 The State Agency and CDSS agree that CDSS will instruct its licensing offices and its county delegees that all appropriate licensing applicants at the orientation will be informed that their name, address and other identifying information are confidential data and will be forwarded to the State Agency solely for the purpose of training and education. It is also agreed that CDSS will inform these applicants that the State Agency is required to protect the confidential data from unauthorized use and disclosure.
- 5.1 The State Agency and CDSS agree that applicants and existing licensees may request that their confidential data not be provided to the State Agency.
- 6.1 The State Agency and CDSS agree that the confidentiality of the applicants and licensees shall be protected at all times, and that the State Agency shall respect that right and not attempt to further persuade applicants or licensees who have declined to attend training or opted out.

IV. INFORMATION SECURITY INCIDENTS

- 1.1 Notification: The State agency shall notify the CDSS or its designated agent of any actual or attempted information security incidents, as defined below, within 24 hours of initial detection. Information security incidents shall be reported by telephone to:

Cynthia Fair
Information Security Officer
Information Systems Division
California Department of Social Services
744 P Street, M.S. 8-17-33
Sacramento, CA 95814
(916) 651-9923

- 2.1 Cooperation: The State agency shall cooperate in any investigations of information security incidents.
- 3.1 Isolation of system or device: The system or device affected by an information security incident, and containing CDSS confidential data, shall be removed from operation upon CDSS confidential data immediately. It shall remain removed from operation until correction and mitigation measures have been applied. CDSS must be contacted prior to placing the system or device, containing CDSS confidential data, back in operation. The affected system or device, containing CDSS confidential data, shall not be returned to operation until CDSS gives its approval.

V. RETURN OR DESTRUCTION OF DATA

- 1.1 Return or Destruction: Confidential data used, compiled, processed, stored or derived by the State agency in the performance of this agreement shall be destroyed or returned by the agency. All such data shall either be returned to CDSS in an agreed-upon format within 30 days of termination of this contract or be destroyed, unless this agreement expressly authorizes the State agency to retain specified confidential data after the termination of this agreement. If the data is returned to CDSS, the State agency shall provide CDSS with the media and an inventory of the data and files returned.
- 1.2 For purposes of this subsection, "derived" confidential data shall refer to a data set, containing confidential data, that is derived from another data set by (a) elimination of fields from the original data set, (b) addition of fields to the original data set, (c) manipulation of the structure of the original data set or a derivative data set, or (d) renaming an original data set.
- 2.1 Methods of Destruction: The State agency shall destroy all confidential data not returned when the use authorized ends in accordance with approved methods of confidential destruction (via shredding, burning, certified or witnessed destruction, or degaussing of magnetic media). All computer sets containing individual identifiers shall be destroyed. The agency shall use wipe software on all the hard drive surfaces of computers used to process or store CDSS confidential data when the computer is withdrawn from use in processing or storing such data. This includes back-up media. Destruction shall occur before the effective date of termination of this contract and a letter of confirmation shall be provided to CDSS detailing when, how, and what CDSS data was destroyed. This certification letter is required whether destruction services are contracted or the agency performs the destruction.

VI. ENCRYPTION AND TRANSMISSION

- 1.1. The State agency shall ensure the confidentiality of CDSS data transmission. CDSS confidential data may not be transmitted by fax.
- 1.2. The State agency shall ensure that all electronic file media used in data exchanges are either:
 - 1.2.1.1. Transferred by secure file transfer protocol; or
 - 1.2.1.2. Encrypted or protected with equally strong measures if placed on any personal computer (either desktop or laptop), or on any removable storage media of any kind, pursuant to Budget Letter 05-32.

VII. INTERNET CONNECTIVITY

- 1.1 CDSS confidential data that includes confidential identifiers shall not be used or stored in a device connected to the Internet or to a local area network, or dial-up communication, until the confidential identifiers have been removed from the data. Exceptions to this provision require the prior approval by the CDSS ISO.

VIII. CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT

Based on the requirements of the Welfare and Institutions Code 10850, Civil Code 1798 et.seq., State Administrative Manual 4840 et.seq., the California Community Colleges Chancellor's Office shall provide security sufficient to ensure protection of confidential information from improper use and disclosures, including sufficient administrative, physical, and technical safeguards to protect personal information from reasonable anticipated threats to the security or confidentiality of the information.

AGREEMENT NUMBER: _____

NAME OF STATE _____

AGENCY _____

<i>*Signature of Authorized State Official</i>	
<i>Title:</i>	<i>Date:</i>
<i>Phone:</i> <i>Fax:</i>	<i>E-Mail Address:</i>
<i>*Title: Information Security Officer Signature</i>	<i>Date:</i>
<i>Phone:</i> <i>Fax:</i>	<i>E-Mail Address:</i>

** Signatures are required by the Information Security Officer and Authorized State Official. This may include the Agency Chief Information Officer, System Administrator, or other individual responsible for ensuring compliance with the confidentiality and security requirements.*

IX. DEFINITIONS

For the purposes of these requirements, the stated terms are defined as noted:

State Agency: For purposes of this agreement, the terms State agency, agency, or contractor, refers to the California State agency with which CDSS enters into this agreement.

Confidential Data: Information, the disclosure of which is restricted or prohibited by any provision of law. Some examples of "confidential information" include, but are not limited to, public social services client information described in California Welfare and Institutions Code section 10850, and "personal information" about individuals as defined in California Civil Code section 1798.3 of the Information Practices Act (IPA) if the disclosure of the "personal information" is not otherwise allowed by the IPA. Confidential data includes personal identifiers. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data*

Confidential Identifiers: Are specific personal identifiers such as name, social security number, address and date of birth.

De-Identification: Removal of personal identifiers. Examples of personal identifiers include name, social security numbers, driver's license numbers, and account numbers with access codes. Personal information does not include publicly available information that is lawfully made available to the general public. (See definitions for confidential data and confidential/ personal identifiers.)

Information Assets: Information assets include anything used to process or store information, including (but not limited to) records, files, networks, and databases; information technology facilities, equipment (including personal computer systems), and software (owned or leased).

Information Security Incidents: Information Security incidents include, but are not limited to, the following; any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of CDSS information assets.

Risk: The likelihood or probability that a loss of information assets or breach of security will occur.

Signature of Authorized State Official: Authorized signature shall be determined by the state agency. It is recommended that the agency ISO or individual responsible for oversight of the security requirements in the agreement, review and sign the compliance statement.