California Department of Social Services (CDSS)
Confidentiality and Security Requirements for
Vendors
Contracts/Memoranda of Understanding (MOU)/Agreements

I. GENERAL REQUIREMENTS

These requirements provide a framework for maintaining the confidentiality and security of Confidential Data compiled for the CDSS. Definitions of commonly used terms relating to confidentiality and security of data are provided.

In addition to any other contract provisions, contractors shall be responsible for maintaining the confidentiality and security of CDSS confidential and sensitive data. No exceptions from these policies shall be permitted without the explicit, prior, written approval of CDSS. All information security requirements, as stated in this attachment, shall be enforced and implemented immediately upon effective date of this Agreement, and continue throughout the term of the Agreement.

II. DEFINITIONS

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

Audit Trail: Systems information identifying source/location of access, date and time, user-identification, targeted service and activity performed. The audit trail shall identify all accesses to the source file, success or failure of the access, the completion status of the access (e.g., failed or successful authentication, or user terminated) and the record and field modified.

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 include personal identifiers.

De-Identification: Removal of personal identifiers**.** Personal information does not include publicly available information that is lawfully made available to the general public.

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.

Personal Identifiers: Are specific personal identifiers such as name, social security number, address, date of birth, driver's license numbers, and account numbers with access codes.

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

III. DATA SECURITY

A. Access to CDSS Data

1. Request and Re-disclosure: All contractors seeking access to confidential CDSS data files shall request access from CDSS. The contractor shall not re-disclose or re-release CDSS confidential data.

2. Referral for Request: The contractor shall refer any persons not affiliated with the contractor, nor included under this contract with CDSS, to CDSS to request access to the confidential data.

B. Data Security Requirements

1. Contractor Responsibility: The contractor and its subcontractors, if any, are responsible for security of the CDSS confidential data.

2. Protection of Data: The contractors and its subcontractor, if any, shall ensure that electronic media that contains confidential or sensitive data is protected.

3. General Requirements: The contractor and its subcontractors, if any, shall:

   a. Confirm the identity of any individual who has requested confidential or sensitive data.

   b. When there is a business need to discuss confidential CDSS information within the office, discuss the information in an enclosed room, if possible.

   c. Not allow dial-up communication or Internet access to confidential data prior to de-identification of the data. Any use of dial-up or Internet access after de-identification of the data shall include, but not be limited to the following protections; (1) auditing usage of dial-up communications and Internet access for security violations, (2) periodically changing dial-up access telephone numbers, and (3) responding to losses, misuse or improper dissemination of information. Refer to Information Security Incidents for notification required in response.

   d. Not use or store CDSS confidential data on portable or wireless devices. For purposes of this requirement, portable devices include, without limitation, notebook computers, personal digital assistants, and wireless devices including cellular phones with data storage capability.

4. Data Transmission

   a. General Requirement: The contractor shall ensure the confidentiality of CDSS data transmission.

   b. Data transferred via tape, optical media, or cartridge: Confidential data that is transferred on tapes, optical media, or cartridges shall be encrypted. The contractor shall place the transferred data in separate files with identifiers and an index on one file. On another file place the index and remaining data. These files shall be transported separately. Additionally, the tapes, optical media and cartridges shall be transferred by bonded mail service (i.e., accountable mail using restricted delivery). All packages must be double packed with a sealed envelope and a sealed outer envelope or locked box.

c. Data transferred electronically: All File Transport Protocol (FTP) accounts that transfer confidential data with personal identifiers shall be highly restricted in access by the contractor. These accounts shall maintain an audit trail. Their accounts are to be accessible to a limited number of contractor and/or subcontractor staff. No other accounts on contractor's computers may have access to this account. The contractor's and/or subcontractor are to maintain a current listing of the personnel who have access to the FTP account. All CDSS confidential data transferred from contractor machines shall be encrypted. The contractor may not transfer CDSS confidential data via FTP without the approval of CDSS.

d. Data transferred via paper copy: Paper copies of confidential data shall be mailed using a secure, bonded mail service, such as Federal Express or by registered U.S. Mail (i.e., accountable mail using restricted delivery). All packages must be double packed with a sealed envelope and a sealed outer envelope or locked box.

e. Data transferred via fax: CDSS confidential data may not be transmitted by fax. CDSS non-confidential information may be transmitted by fax, provided that the contractor confirms the recipient fax number before sending, takes precautions to ensure that the fax was appropriately received, maintains procedures to notify recipients if the contractor's fax number changes, and maintains fax machines in a secure area.

5. Physical Security

The contractor shall provide for the management and control of physical access to information assets (including personal computer systems and computer terminals) used in performance of this contract, the prevention, detection, and suppression of fires, and the prevention, detection, and minimization of water damage. The physical security measures taken shall include, but not be limited to:

a. Implementing security measures to physically protect data, systems and workstations from unauthorized access and malicious activity.

b. Logging the identity of persons having access to restricted facilities and the date and time of access.

c. Restricting the removal of CDSS confidential data from the work location.

d. Placement of devices used to access CDSS confidential data in areas not open to the public. For purposes of this requirement, "devices" shall include, but not be limited to, dumb terminals, personal computers and printers.

6. Storage

CDSS confidential data shall be stored in a place physically secure from access, use, modification, disclosure, or destruction by an unauthorized person. All media containing confidential information shall be stored in a secured area (a locked room or locked file cabinet). Keys to these locks shall be held by a limited number of contractor organization personnel. Confidential information in electronic format, such as magnetic tapes or discs, shall be stored and processed in such a way that an unauthorized person cannot retrieve the information by computer, remote terminal or other means.

7. Encryption

   The contractor shall encrypt CDSS confidential data, whether for transmission or in storage, using non-proprietary, secure generally-available encryption software. Proprietary encryption algorithms shall not be acceptable. Passwords or biometrics templates used for user authentication shall be encrypted using data encryption standard, or better, one-way only encryption. Data encryption shall meet the National Institute of Standards and Technology Advanced Encryption Standard. Data encryption shall equal or exceed 128-bit key encryption. A documented security plan is required for encryption key management.

8. De-Identification of Data

   a. Assignment of Unique Identifier*:* The contractor shall remove personal identifiers from CDSS confidential data and substitute unique identifiers, within 30 days of receipt of the CDSS confidential data.

   b. No connection before de-identification: CDSS confidential data that includes personal 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 personal identifiers have been removed from the data.

   c. Return or destruction of confidential data upon de-identification: CDSS confidential data shall be returned to CDSS upon completion of de-identification or destroyed in accordance with this Agreement, no more than 30 days after completion of de-identification.

C. Network Security Requirements

The contractor shall provide the following electronic access measures at a minimum:

1. A notification at initial logon that unauthorized access is prohibited by law.

2. An audit trail.

3. A method for verification of the identity of an individual accessing the system, such as user identification, PIN, fingerprint, voiceprint, retinal print, or other appropriate verification method.

4. A limited access to data to those authorized employees of the contractor who have a functional requirement to use the data.

5. The revoking of access from a user after three unsuccessful access attempts.

6. A security manual or package, which shall adequately protect against loss or unauthorized (accidental or intentional) access, use, disclosure, modification, or destruction of data. All proposed changes to programs, network systems, connectivity and storage of CDSS data shall be provided to CDSS for review prior to implementation.

7. User access authentication shall be disabled (revoked) immediately upon termination of employment or after no more than 60 days of non-use.

8. User verification which is unique to each individual and not assigned to groups or job location. These measures shall include, but not necessarily be limited to, the development of passwords and access controls to protect the security of data from any individual who is not authorized to access the data.

9. An automated log-off or time-out from all networked systems that contain confidential CDSS information when the user leaves the work area for a ten-minute period of time.

D. Ownership and Destruction of Confidential Data

1. Ownership and Return or Destruction: All data used, compiled, developed, processed, stored, or created under this contract is the property of CDSS. All such data shall either be returned to CDSS in an agreed upon format within 30 days of termination of the contract or destroyed. If the data is returned, the contractor shall provide CDSS with the media and an inventory of the data and files returned.

2. Methods of Destruction: The contractor 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 personal identifiers shall be destroyed. The contractor 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. 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.

E. Contractor Staff

1. Former Employees: The contractor shall ensure that confidential data are not accessible to former employees of the contractor.

2. Employee Authorization: The contractor shall maintain a record of the access authorization for each individual employee that has access to the confidential data. The contractor's security systems administrator designated pursuant to this Agreement shall maintain an appointment/separation checklist for each employee which documents how access authorization was modified when any employee terminates employment or changes duties.

F. Information Security Incidents

1. Notification: The contractor shall notify the CDSS or its designated agent of any actual or attempted information security incidents, as defined above, immediately upon detection. Information security incidents shall be reported by telephone or email to:

Lloyd Indig
Information Security & Privacy Officer
California Department of Social Services
744 P Street, M.S. 9-9-70
Sacramento, CA 95814

916-651-5558
iso@dss.ca.gov

2. Cooperation: The contractor shall cooperate in any investigations of information security incidents.

3. 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 immediately. It shall remain removed from operation until correction and mitigation measures have been applied. The affected system or device, containing CDSS confidential data, shall not be returned to operation until CDSS gives its approval.

G. Confidentiality Statements

1. Requirement: All staff of the contractor with actual or potential access to CDSS confidential data shall read and sign a Confidentiality Agreement. (See section IV.)

2. Supervisory Review: The supervisor of the employee shall review the signed Confidentiality Agreement with the employee and document this review.

3. Submission: The signed original Confidentiality Agreements shall be submitted to the CDSS Project representative. The contractor shall notify CDSS immediately of the appointment or separation of an employee who has been authorized access to CDSS confidential data.

4. Annual Notification: The contractor shall provide to CDSS, in January of each calendar year, a current list of authorized users and newly signed Confidentiality Agreements for all authorized users.

H. Security Systems Administrator Duties

1. Designation: The contractor shall designate a single person as the security systems administrator. The name of the individual so designated shall be supplied to CDSS.

2. Access Control: The security systems administrator shall have the ability to change or remove any computer access authorization of an individual having access to the system at any time.

3. Employee Verification: The contractor shall verify that the employee who performs the duties of the security systems administrator is a trusted person who has demonstrated in past jobs a capability to perform in this role. Additionally, these security clearance procedures shall ascertain if the employee who performs the duties of security systems administrator has any past criminal or employment background which would call into question their ability to perform this role successfully.

4. Vulnerability Assessments and Mitigation Validation: The security systems administrator shall assess system security vulnerabilities and validate mitigation actions performed and shall disable all applications, components, and services that are not required for performance of the contract with CDSS. This assessment shall be provided in writing to the contract administrator along with a description of corrective actions.

5. Security Patches and Upgrades: The security systems administrator shall ensure that security patches and upgrades released by the respective manufacturers of the components of the information assets used to process CDSS confidential data are promptly applied to the components. Patches and upgrades downloaded from public networks shall be applied only if digitally signed by the source and only after the security systems analyst has reviewed the integrity of the patch or upgrade.

I. Risk Analysis/Contingency Plans

1. The contractor shall carry out a risk analysis with sufficient regularity to identify and assess vulnerabilities associated with all information assets owned, maintained, or used by the contractor that are used to process or store CDSS confidential data, and shall define a cost-effective approach to manage such risks. Specific risks that shall be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of employees and outsiders; fire, flooding, and electrical disturbances and loss of data communications capabilities. The contractor shall advise the CDSS or its designated agent of any vulnerability that may present a threat to CDSS confidential data and of the specific safeguards used for protecting CDSS confidential data. The contractor shall take the necessary steps to protect CDSS confidential data.

2. Contingency plans shall be established and implemented in order to assure that operations can be back to normal in minimum time after natural or man-made disasters, unintentional accidents, or intentional acts such as sabotage. These plans shall include, but are not limited to, the regular backup of automated files and databases, secure storage, recovery, and restarting planning procedures.

J. Rules of Aggregation

1. Requirement: "Aggregated," as used in this subsection, refers to a data output report that does not allow identification of an individual. All reports developed by the contractor shall contain CDSS confidential data only in aggregated form. Personal identifiers should be removed, geographic identifiers should be specified only in large areas, and as needed, variables should be recorded in order to protect confidentiality. No disaggregate data identifying individuals shall be released to outside parties or to the public.

2. Pre-Release Edits: The data system of the contractor shall have prerelease edits, which shall not allow the production of data cells that do not comply with the requirements of this section.

3. Minimum Data Cell Size: The minimum data cell size or derivation thereof shall be five participants for any data table released to outside parties or to the public.

K. Security Plans

1. Submission: When required**,** the contractor shall submit a written security plan to CDSS prior to receipt of CDSS confidential data. The security plan shall address the methods and processes the contractor will use to meet the security and confidentially requirements of this Agreement. CDSS will not release CDSS confidential data to the contractor before CDSS approval of the contractor's security plan.

2. Maintenance/Signature: The contractor shall maintain continuous compliance with its approved security plan. The contractor shall secure prior CDSS approval for any changes to its approved security plan. CDSS may require the contractor to amend its security plan as a condition of continued receipt or use of CDSS confidential data. The security plans shall be signed by the contractor and person(s) responsible for the contractor's system administration.

IV. CONFIDENTIALITY AGREEMENT

I (please print), _____an employee of

(please print) _____ hereby acknowledge that the California Department of Social Services (CDSS) public assistance records and documents are subject to strict confidentiality requirements imposed by State and federal law including California Welfare and Institutions Code sections 10850 California Penal Code section 11167.5, 45 Code of Federal Regulations 205.50, and 1798.24 of the Civil Code relating to research.

I (initial) _____ acknowledge that my supervisor, or the data librarian, has reviewed with me the appropriate provisions of both State and federal laws including the penalties for breaches of confidentiality.

I (initial) _____ acknowledge that my supervisor or the data librarian has reviewed with me the confidentiality and security policies of the CDSS.

I (initial) _____ acknowledge that my supervisor or the data librarian has reviewed with me the policies of confidentiality and security of our organization.

I (initial) _____ acknowledge that unauthorized use, dissemination or distribution of CDSS confidential information is a crime.

I (initial) _____ hereby agree that I will not use, disseminate or otherwise distribute confidential records or said documents or information either on paper or by electronic means other than in the performance of the specific research I am conducting.

I (initial) _____ also agree that unauthorized use, dissemination or distribution is grounds for immediate termination of my organization's Contract/Memorandum of Understanding/Agreements with the CDSS and may subject me to penalties both civil and criminal.

_____ _____
Signed Date