Attachment A

Confidentiality and Security Requirements for Research Organizations

March 2005

CONTENTS

I. GENERAL PROVISIONS

In addition to any other contract provisions, researchers and research organizations shall be responsible for maintaining the confidentiality and security of California Department of Social Services (CDSS) confidential data. No exceptions from these policies shall be permitted without the explicit, prior, written approval of CDSS.

II. DEFINITIONS

For the purposes of these requirements, the stated terms have the following meaning:

Applicant or Recipient - An individual applying for or receiving public social services under Division 9, commencing with section 10000, of the Welfare and Institutions Code.

Audit Trail - Systems information identifying all accesses to the source file, including source/location of access, date and time, user-id, targeted service and activity performed, success or failure of the access, the completion status of the access (e.g. “failed authentication,” or “successful,” or “user terminated”) and any 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 includes confidential identifiers.

Confidential Identifiers - Specific personal identifiers such as name, social security number, address and date of birth**.**

De-identification – Assignment of unique identifiers to confidential identifiers such that the individual cannot be identified through the unique identifier.

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

Information Security Incidents - Any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized exposure or disclosure of CDSS information assets or confidential data.

Researcher or **Research Organization** (hereafter, **Research Organization**) - An individual or organization conducting research of potential benefit to CDSS and the State of California which requires access to CDSS confidential data.

III. CONFIDENTIAL DATA SECURITY

A. Access to CDSS Confidential Data

1. *Request and Redisclosure:* All research organizations seeking access to CDSS confidential data shall submit a written request to CDSS. The research organization shall not redisclose or re-release CDSS confidential data.

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

3. *Local Institutional Review Board Approval:* The research organization shall submit a copy of its project approval from the organization's Institutional Review Board (IRB) as a condition of receiving CDSS confidential data. If the research organization does not have a local IRB, it may submit documentation of reliance on another IRB for review of its projects.

4. *Committee for the Protection of Human Subjects Approval:* The research organization shall submit a copy of its project approval letter from the Committee for The Protection of Human Subjects (CPHS) for the California Health and Human Services Agency (CHHSA) as a condition of receiving CDSS confidential data. The research organization shall also submit an annual update to the CPHS approval, as well as any approval letters for any revisions to the project as a condition of continued access to CDSS confidential data.

B. Confidential Data Security Requirements

1. *Research Organization Responsibility:* The research organization is responsible for security of the CDSS confidential data.

2. *Level of Protection:* The research organization shall ensure that electronic media containing confidential data is protected at the level of the confidential data.

3. *General Requirements:* The research organization shall have adequate security measures. These measures shall include, but are not limited to, the development of passwords and access controls to protect the security of the data from any individual who is not authorized to access the data. All research organizations, and their staff, shall:

a. Designate, in advance, the individuals who will have access to CDSS confidential data.

b. At the point an authorized individual requests access to confidential data, confirm his or her identity.

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

d. Neither use nor store CDSS confidential data on wireless devices. For purposes of this requirement, “wireless devices” include, without limitation, notebook computers or Personal Digital Assistants (PDAs) equipped for 802.11x wireless networking. This restriction shall apply whether or not the data are encrypted.

4. *Data Transmission:*

a. *General Requirement:* The research organization shall ensure the confidentiality of confidential data transmission.

b. *Data transferred via tape, cartridge or CD:* All confidential data that is transferred on tapes, cartridges or CDs shall be encrypted and placed in separate files with identifiers and a crosswalk on one file, the crosswalk and remaining data on another file, with the files transported separately. Additionally, the tapes, cartridges and CDs shall be delivered using a bonded accountable mail service.

c. *Data transferred electronically:* The research organization may not transfer CDSS confidential data via File Transfer Protocol (FTP) without prior written approval of CDSS. All CDSS confidential data must be encrypted before it can be transfer via FTP. All FTP accounts that transfer confidential data shall be highly restricted in access by the research organization and shall be accessible to only those research organization staff that needs access for performance of the research. These accounts shall maintain an audit trail. No other accounts on the research organization’s computers may have access to these FTP accounts. The research organization shall maintain a current listing of the personnel who have access to the FTP account.

d. *Data transferred via paper copy:* Paper copies of confidential data shall be mailed using double envelopes and shall be delivered using a bonded accountable mail service. Paper copies of confidential data shall be stored in a locked file cabinet. Access to the key shall be highly restricted.

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 research organization confirms the recipient fax number before sending, takes precautions to ensure that the fax was appropriately received, maintains procedures to notify recipients if the research organization's fax number changes, and maintains fax machines in a secure area.

5. *Physical Security:* The research organization 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. In addition, the organization shall provide for 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 authorized work location.

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

   e. Preventing printed records, microfilmed records, and records stored on any electronic media (including, without limitation, diskette, hard drive, or optical media) from unauthorized access or viewing by unauthorized persons, whether in work areas, in transit, or in storage.

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 research 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 research organization shall encrypt CDSS confidential data, whether for transmission or in storage, using non-proprietary, secure generally-available encryption software. The CDSS confidential data shall be encrypted upon receipt from CDSS and shall remain encrypted other than when in active use by the research organization. Proprietary encryption algorithms shall not be acceptable. Passwords or biometrics templates used for user authentication shall be encrypted using Double Encryption Standards (DES), or better, one-way only encryption. Data encryption shall meet the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES).

8. *De-identification:*

    a. *Assignment of Unique Identifier:* The research organization shall remove confidential identifiers from CDSS confidential data, and substitute unique identifiers, as soon as possible but no later then 60 days after receipt of the CDSS confidential data.

    b. *No connection before de-identification:* 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 (LAN) until the confidential identifiers have been removed from the data.

    c. *Data Outputs*: Full-time security personnel shall review all data outputs prior to removal from secured work areas to ensure that they are in an aggregated and non-confidential form. Personal identifiers must be removed, geographic identities must be specified only in large areas, and as needed, variables must be recoded in order to protect confidentiality.

C. Security Manual or Package

The research organization shall maintain a security manual or package which describes safeguards against loss or unauthorized (accidental or intentional) access, use, disclosure, modification, or destruction of confidential data.

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 are 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 are returned, the research organization shall provide the CDSS with the media and an inventory of the data and files returned.

2. *Methods of Destruction:* The research organization shall destroy all confidential data not returned when the authorized use ends in accordance with approved methods of confidential destruction (via shredding, burning or certified or witnessed destruction). Destruction standards shall be in accordance with the National Security Center Standards ("*A Guide to Understanding Data Reminisce in Automated Information Systems*").

E. Research Organization Staff

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

2. *Employee Authorization:* The research organization shall maintain a record of the access authorization for each individual employee that has access to the confidential data. The research organization's security systems administrator designated pursuant to Section III. H. 1. 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 research organization shall within 24 hours notify the CDSS or its designated agent, the institution's IRB, and the CHHSA CPHS of any actual or attempted information security incidents, as defined above. Information security incidents shall be reported by telephone to:

   Sherland Jordan
   Information Security Officer (ISO)
   California Department of Social Services
   744 P Street, M.S. 17-33
   Sacramento, CA 95814
   (916) 654-1767 or (916) 296-5608

2. *Cooperation:* The research organization shall cooperate with CDSS, its own IRB and the CHHSA in any investigations of information security incidents.

3. *Isolation of system or device:* The system or device using CDSS confidential data and affected by an information security incident shall be immediately removed from operation until correction and mitigation measures have been applied. CDSS must be contacted prior to placing the system or device, containing CDSS data, back in operation. The affected system or device shall not be returned to operation without approval by CDSS.

G. Confidentiality Statements

1. *Requirement:* All staff of the research organization with actual or potential access to CDSS confidential data shall read and sign a Confidentiality Agreement (see page 12).

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 Agreement shall be submitted to the CDSS Project Representative.

4. *Annual Notification:* The research organization shall provide to CDSS in January of each calendar year a current list of authorized users and a newly signed Confidentiality Agreement for all authorized users.

H. Security Systems Administrator Duties

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

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

3. *Employee Verification:* The research organization 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, the research organization's security clearance procedures shall ascertain if the employee who performs the duties of security systems administrator has any past 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 to process or store CDSS confidential data.

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 administrator has reviewed the integrity of the patch or upgrade.

I. Risk Analysis

The research organization 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 research organization that are used to process or store CDSS confidential information, 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 research organization 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 taken for protecting the CDSS confidential data. The research organization shall take the necessary steps to protect the CDSS confidential data.

J. Contingency Plans:

Contingency plans shall be established and implemented for the research organization's information assets containing CDSS confidential information 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 not be limited to the regular backup of automated files and databases, secure storage, recovery, and restarting planning procedures.

K. 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 research organization shall contain CDSS data only in aggregated form. No disaggregate data identifying individuals shall be released to unauthorized staff, outside parties, or to the public.

2. *Prerelease Edits:* The data system of the research organization 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 shall be five participants for any data table released to outside parties or to the public.

IV. Requirements Document Update and Revision

A. *Update*: These policies will be reviewed by DSS semi-annually for conformance to current law and changes in technologies.

B. *Revision*: The CDSS Information Security Officer, with input and concurrence from The Research and Evaluation Bureau, will be responsible for updating and distributing revisions to these policies.

CONFIDENTIALITY AGREEMENT

I (please print), _____an employee of (please print)

_____ hereby acknowledge that records, documents and data provided by the California Department of Social Services (CDSS), under agreement number

_____,are subject to strict confidentiality requirements imposed by state and federal law including California Welfare and Institutions Code Sections 10850 & 827, California Penal Code Section 11167.5, and 45 Code of Federal Regulations (CFR) 205.50.

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

I (initial) _____ acknowledge that my supervisor or appropriate data security staff 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 agreement with the CDSS and may subject me to penalties both civil and criminal.

_____ _____
Signed (Employee) Date

_____ _____
Signed (Supervisor/Data Security Staff) Date