**The California Department of Social Services**

**Confidentiality and Information Security Requirements – Contractor/Entity**

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as “this Exhibit”) sets forth the information security and privacy requirements Contractor/Entity (hereinafter referred to as “Contractor”) is obligated to follow with respect to all confidential and sensitive information (as defined herein) disclosed to or collected by Contractor, pursuant to Contractor’s Agreement (the “Agreement”) with the California Department of Social Services (hereinafter “CDSS”) in which this Exhibit is incorporated. The CDSS and Contractor desire to protect the privacy and provide for the security of CDSS Confidential, Sensitive, and/or Personal (CSP) Information in (hereinafter referred to as “CDSS CSP”) compliance with state and federal statutes, rules and regulations.

1. **Order of Precedence.** With respect to information security and privacy requirements for all CDSS CSP, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between Contractor and CDSS and shall prevail over any such conflicting terms or conditions.
2. **Effect on lower tier transactions.** The terms of this Exhibit shall apply to all lower tier transactions (e.g. agreements, sub-agreements, contracts, subcontracts, and sub-awards, etc.) regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each lower tier transaction to its agents, contractors, subcontractors, or independent consultants, etc.
3. **Confidentiality of Information.**
	1. **DEFINITIONS**. The following definitions relate to CDSS Confidential, Sensitive, and/or Personal Information.
		1. “Confidential Information” is information maintained by the CDSS that is exempt from disclosure under the provisions of the California Public Records Act (Government Codes Sections 6250-6265) or has restrictions on disclosure in accordance with other applicable state or federal laws.
		2. “Sensitive Information” is information maintained by the CDSS, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information is information in which the disclosure would jeopardize the integrity of the CDSS (i.e., CDSS' fiscal resources and operations).
		3. “Personal Information” is information, in any medium (paper, electronic, or oral) that identifies or describes an individual (i.e., name, social security number, driver’s license, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information (PHI), etc.) and must be protected from inappropriate access, use or disclosure and must be made accessible to information subjects upon request. It can also be information in the possession of the Department in which the disclosure is limited by law or contractual Agreement (i.e., proprietary information, etc.).
		4. “Breach” is
			1. the unauthorized acquisition, access, use, or disclosure of CDSS CSP in a manner which compromises the security, confidentiality or integrity of the information; or
			2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).
		5. “Security Incident” is
			1. an attempted breach;
			2. the attempted or successful unauthorized access or disclosure, modification or destruction of CDSS CSP, in violation of any state or federal law or in a manner not permitted under the Agreement between Contractor and CDSS, including this Exhibit; or
			3. the attempted or successful modification or destruction of, or interference with, Contractor’s system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDSS CSP.
	2. CDSS CSP by the CDSS which may become available to the Contractor as a result of the implementation of the Agreement shall be protected by the Contractor from unauthorized access, use, and disclosure as described in this Exhibit.
	3. Contractor is notified that unauthorized disclosure of CDSS CSP may be subject to civil and/or criminal penalties under state and federal law, including but not limited to:
* California Welfare and Institutions Code section 10850
* Information Practices Act – California Civil Code section 1798 et seq.
* Public Records Act – California Government Code section 6250 et seq.
* California Penal Code Section 502, 11140-11144, 13301-13303
* Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) – 45 CFR Parts 160 and 164
* Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50
	1. **EXCLUSIONS.** “Confidential Information”, “Sensitive Information”, and “Personal Information” (CDSS CSP) does not include information that
		1. is or becomes generally known or available to the public other than because of a breach by Contractor of these confidentiality provisions;
		2. already known to Contractor before receipt from CDSS without an obligation of confidentiality owed to CDSS;
		3. provided to Contractor from a third party except where Contractor knows, or reasonably should know, that the disclosure constitutes a breach of confidentiality or a wrongful or tortious act; or
		4. independently developed by Contractor without reference to the CDSS CSP.
1. **Contractor Responsibilities**.
	1. **Training.** The Contractor shall instruct all employees, agents, and subcontractors with access to the CDSS CSP regarding:
		1. The confidential nature of the information;
		2. The civil and criminal sanctions against unauthorized access, use, or disclosure found in the California Civil Code Section 1798.55, Penal Code Section 502 and other state and federal laws;
		3. CDSS procedures for reporting actual or suspected information security incidents in Paragraph V – Information Security Incidents and/or Breaches; and
		4. That unauthorized access, use, or disclosure of CDSS CSP is grounds for immediate termination of this Agreement with CDSS and the Contractor and may be subject to penalties, both civil and criminal.
	2. **Use Restrictions.** The Contractor shall ensure that their employees, agents, contractors, subcontractors, and independent consultants will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement.
	3. **Disclosure.** The Contractor shall not disclose any individually identifiable CDSS CSP to any person other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement. Contractor is permitted to disclose individually identifiable CDSS CSP with the consent of the individual to its service providers, its vendors, and its partners for the purposes of Contractor providing services to CDSS or otherwise to meet Contractor’s obligations under the Agreement. For CDSS CSP, Contractor must provide CDSS Program Manager and CDSS Information Security Office with a list of Contractor authorized service providers and ensure they are bound by obligations sufficient to protect CDSS CSP in accordance with this Agreement.
	4. **Subpoena.** If Contractor receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CDSS CSP, Contractor will immediately notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer. In no event should notification to CDSS occur more than twenty-four (24) hours after knowingly receiving such request.
	5. **Information Security Officer.** The Contractor shall designate an Information Security Officer to oversee its compliance with this Exhibit and to communicate with CDSS on matters concerning this Exhibit.
	6. **Requests for CDSS CSP by Third Parties**. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer all requests for disclosure of any CDSS CSP requested by third parties to the Agreement between Contractor and CDSS (except from an Individual for an accounting of disclosures of the individual’s personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.
	7. **Documentation of Disclosures for Requests for Accounting**. Contractor shall maintain an accurate accounting of all requests for disclosure of CDSS CSP Information and the information necessary to respond to a request for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.
	8. **Return or Destruction of CDSS CSP on Expiration or Termination**. Upon expiration or termination of the Agreement between Contractor and CDSS for any reason, Contractor shall return or destroy the CDSS CSP. If return or destruction is not feasible, Contractor shall provide a written explanation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information in this Agreement. CDSS, in its sole discretion, will make a determination of the acceptability of the explanation and, if retention is permitted, shall inform Contractor in writing of any additional terms and conditions applicable to the retention of the CDSS CSP.
	9. **Retention Required by Law.** If required by state or federal law, Contractor may retain, after expiration or termination, CDSS CSP for the time specified as necessary to comply with the law.
	10. **Obligations Continue Until Return or Destruction**. Contractor’s obligations regarding the confidentiality of CDSS CSP set forth in this Agreement, including but not limited to obligations related to responding to Public Records Act requests and subpoenas shall continue until Contractor returns or destroys the CDSS CSP or returns the CDSS CSP to CDSS; provided however, that on expiration or termination of the Agreement between Contractor and CDSS, Contractor shall not further use or disclose the CDSS CSP except as required by state or federal law.
	11. **Notification of Election to Destroy CDSS CSP**. If Contractor elects to destroy the CDSS CSP, Contractor shall certify in writing, to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer, using the contact information, that the CDSS CSP has been destroyed.
	12. **Background Check.** Before a member of the Contractor’s workforce may access CDSS CSP, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to the State’s information technology systems and the data contained therein. The Contractor shall retain each workforce member’s background check documentation for a period of three (3) years following Agreement termination.
	13. **Confidentiality Safeguards.** The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the CDSS CSP that it creates, receives, maintains, uses, or transmits pursuant to the Agreement. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor’s operations and the nature and scope of its activities, including at a minimum the following safeguards:
		1. **General Security Controls**
			1. ***User Confidentiality Statement.*** All persons with access to CDSS CSP must sign the Paragraph XI – CDSS User Confidentiality Agreement below. The statement must be signed prior to access to CDSS CSP. The statement must be renewed annually. The Contractor shall retain each person’s written confidentiality statement for CDSS inspection for a period of three (3) years following contract termination.
			2. **Workstation/Laptop Encryption.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDSS Information Security Office.
			3. **Data Encryption.** Any CDSS CSP shall be encrypted at rest when stored on network file shares or document repositories.
			4. **Server Security.** Servers containing unencrypted CDSS CSP must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
			5. **Minimum Necessary.** Only the minimum necessary amount of the CDSS CSP required to perform necessary business functions may be copied, downloaded, or exported.
			6. **Removable Media Devices.** All electronic files that contain the CDSS CSP must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart phone, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.
			7. **Antivirus Software.** All Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
			8. **Patch Management.** Contractor must submit a documented patch management system, to be approved by the CDSS Information Security Office, in place to install security patches in a timely manner on all Contractor-owned or managed workstations, laptops, tablets, smart phones, and similar devices that process and/or store CDSS CSP as appropriate based on Contractor’s risk assessment of such patches, the technical requirements of Contractor’s systems, and vendor’s written recommendations. In lieu of an approved patch management system, all applicable patches must be installed within thirty (30) days of vendor release or patch installation occurs within the CDSS approved timeframes by the next scheduled change release, or accept risk with an approved risk analysis by the Contractor.
			9. **User IDs and Password Controls.** All users must be issued a unique user name for accessing CDSS CSP which meets or exceeds CDSS current Password policy. (Contact CDSS Information Security and Privacy Officer for current policy.)
			10. **Data Destruction.** Upon termination of the Agreement, all CDSS CSP must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDSS Information Security Office.
		2. **System Security Controls**
			1. **System Timeout.** The system providing access to the CDSS CSP must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
			2. **Warning Banners.** All systems containing CDSS CSP must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
			3. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDSS CSP, or which alters CDSS CSP. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If CDSS CSP is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence.
			4. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.
			5. **Transmission Encryption.** All data transmissions of CDSS CSP outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDSS CSP can be encrypted. This requirement pertains to any type of CDSS CSP in motion such as website access, file transfer, and E-Mail.
			6. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting CDSS CSP that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.
		3. **Audit Controls**
			1. **System Security Review.** All systems processing and/or storing CDSS CSP must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.
			2. **Log Reviews.** All systems processing and/or storing CDSS CSP must have a routine procedure in place to review system logs for unauthorized access.
			3. **Change Control.** All systems processing and/or storing CDSS CSP must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.
		4. **Business Continuity / Disaster Recovery Controls**
			1. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDSS CSP in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.
			2. **Data Backup Plan.** Contractor must have established documented procedures to backup CDSS CSP to maintain retrievable exact copies of CDSS CSP. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDSS CSP should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDSS data.
		5. **Paper Document Controls**
			1. **Supervision of Information**. CDSS CSP in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information. CDSS CSP in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
			2. **Escorting Visitors**. Visitors to areas where the CDSS CSP are contained shall be escorted and CDSS CSP shall be kept out of sight while visitors are in the area.
			3. **Confidential Destruction**. CDSS CSP must be disposed of through confidential means, such as cross cut shredding and/or pulverizing.
			4. **Removal of Information**. CDSS CSP must not be removed from the premises of the Contractor except for identified routine business purposes or with express written permission of CDSS.
			5. **Faxing**. CDSS CSP that must be transmitted by fax shall require 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**.**
			6. **Mailing**. Paper copies of CDSS CSP shall be mailed using a secure, bonded mail service, such as Federal Express, UPS, or by registered U.S. Postal 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.
2. **Information Security Incidents and/or Breaches**
	1. **Incidents and/or Breaches Response Responsibility**. The Contractor shall be responsible for facilitating the Incident and/or Breach response process as described in California Civil Code 1798.29(e), California Civil Code 1798.82(f), and SAM 5340, Incident Management.
	2. **Discovery and Notification of Incidents and/or Breaches**. The Contractor shall notify the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within one working day by telephone call and email upon the discovery of the Incident and/or Breach affecting the security of CDSS CSP if the CDSS CSP was, or is reasonably believed to have been, acquired by an unauthorized person, or there is an intrusion, potential loss, actual loss, or unauthorized use or disclosure of the CDSS CSP is in violation of this Agreement, this provision, or applicable law. The Contractor shall take:
		1. Prompt corrective action to mitigate the risks or damages involved with the Incident and/or Breach and to protect the operating environment; and
		2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
	3. **Isolation of System or Device.** A system or device, containing CDSS CSP, compromised by an Incident and/or Breach involving an exploitation of a technical vulnerability, shall be promptly disconnected from Contractor’s production environment with access to only individuals who are participating in the investigation, mitigation, and remediation of the Incident and/or Breach. Such system or device shall remain disconnected from the production environment until the risk from the exploited vulnerability has been adequately mitigated. CDSS must be contacted prior to placing the previously compromised system or device, containing CDSS CSP, back in the production environment. The affected system or device, containing CDSS CSP, shall not be returned to operation in the production environment until the CDSS Information Security and Privacy Officer gives its approval.
	4. **Investigation of Incidents and/or Breaches**. The Contractor shall promptly investigate such Incidents and/or Breaches.
	5. **Updates on Investigation**. The Contractor shall provide regular (at least once a week) email updates on the progress of the Incident and/or Breach investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer until they are no longer needed, as mutually agreed upon between the Contractor and the CDSS Information Security and Privacy Officer.
	6. **Written Report**. The Contractor shall provide a written report of the investigation to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer within ten (10) working days of the discovery of the Incident and/or Breach. To the extent Contractor has such information, the report shall include but not be limited to the following:
		1. Contractor point of contact information;
		2. Description of what happened, including the date of the Incident and/or Breach and the date of the discovery of the Incident and/or Breach, if known;
		3. Description of the types of CDSS CSP that were involved and the extent of the information involved in the Incident and/or Breach;
		4. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CDSS CSP;
		5. A description of where the CDSS CSP is believed to have been improperly transmitted, sent, or utilized;
		6. A description of the probable causes of the improper use or disclosure;
		7. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered; and
		8. Full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Incident and/or Breach.
	7. **Notification of Individuals**. The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under applicable state or federal law as reasonably determined by CDSS. Contractor shall be responsible for the notifications, as well as any costs associated with the breach. The CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer shall promptly approve the time, manner and content of any such notifications, and such approval shall not be unreasonably withheld.
3. **Contact Information**. To direct communications to the above referenced CDSS staff, the Contractor shall initiate contact as indicated herein. CDSS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

|  |  |
| --- | --- |
| **CDSS Program Contract Manager** | **CDSS****Information Security & Privacy Officer** |
| See the Scope of Work exhibit for Program Contract Manager information | California Department of Social ServicesInformation Security & Privacy Officer744 P Street, MS 9-9-70Sacramento, CA 95814Email: iso@dss.ca.govTelephone: (916) 651-5558 |

1. **Audits and Inspections.** From time to time, CDSS may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDSS Program Contract Manager and the CDSS Information Security and Privacy Officer in writing. The fact that CDSS inspects, or fails to inspect, or has the right to inspect, Contractor’s facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit.
2. **Amendment**. The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CDSS CSP.
3. **Interpretation**. The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.
4. **Termination.** An information Incident and/or Breach by Contractor, its employees, agents, or subcontractors, as determined by CDSS, may constitute a material breach of the Agreement between Contractor and CDSS and grounds for immediate termination of the Agreement.
5. **CDSS User Confidentiality Agreement**

**CALIFORNIA DEPARTMENT of SOCIAL SERVICES
USER CONFIDENTIALITY AGREEMENT**

Information resources maintained by the California Department of Social Services (CDSS) and provided to your entity may be confidential, sensitive, and/or personal. Confidential, Sensitive, and/or Personal (CSP) information is not open to the public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. The CDSS strictly enforces information security. If you violate these provisions, you may be subject to administrative, civil, and/or criminal penalty.

|  |  |
| --- | --- |
|  INITIAL | I hereby acknowledge that the confidential and/or sensitive records of the CDSS are subject to strict confidentiality requirements imposed by state and federal law include the California Welfare and Institutions Code §10850, Information Practices Act – California Civil Code §1798 et seq., Public Records Act – California Government Code §6250 et seq., California Penal Code §502, 11140-11144, 13301-13303, Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) – 45 CFR Parts 160 and 164, and Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50. |
|  INITIAL | I acknowledge that my supervisor reviewed with me the confidentiality and security requirements, policies, and administrative processes of my organization, the CDSS, and of the State. |
|  INITIAL | I acknowledge that I will not intentionally seek out, read, use, or disclose the CDSS CSP other than for the purposes of providing the requested services to CDSS and meeting its obligations under the Agreement. |
|  INITIAL | I acknowledge that the Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other entity workforce members under Contractor’s direct control who intentionally or negligently violate any provisions of this Exhibit. |
|  INITIAL | I acknowledge that unauthorized access, use, or disclosure of CDSS CSP is grounds for immediate termination of this Agreement with CDSS and the Contractor and may be subject to penalties, both civil and criminal. |
|  INITIAL | I hereby agree to protect the CDSS’ information on either paper or electronic form by:* Only accessing or using the CDSS supplied information as specified in the Agreement for the performance of the specific work I am assigned.
* Never accessing information for curiosity or personal reasons.
* Never showing or discussing CSP information to or with anyone who does not have the need to know.
* Never removing CSP information from the work site without authorization.
* Following encryption requirements for all CSP information in any portable device or media.
 |

**“I certify that I have read and initialed the confidentiality statements printed above and will abide by them.”**

|  |  |
| --- | --- |
| Name (Printed): |  |
|  |  |
| Signature: |  |
|  |  |
| Date Signed: |  |
|  |  |