ATTORNEY GENERAL OF TEXAS
GREG ABBOTT
CHILD SUPPORT DIVISION

June 28, 2010

The Honorable Laura Hinojosa
Hidalgo County District Clerk
P.O. Box 87
Edinburg, TX 78540-

RE: Two Originals of FY11/12 State Case Registry and Local Customer Service Contract

Dear Ms. Hinojosa:

Attached are two originals of the renewal for the FY11/12 State Case Registry/Local Customer Service (SCR/LCS) Contract. Please have both originals signed where indicated.

Also attached is the Incident Response Plan, Attachment G, which is designed to provide a general reference to both OAG and county staff when a security incident may threaten the confidentiality of OAG data. We included the Incident Response Plan (printed on green paper) from your current SCR/LCS Contract for your convenience. You will need to submit a new Incident Response Plan even if no changes occurred since the previous contract. Pursuant to contract requirement 6.4.1.1, please complete the Incident Response Plan and return it along with both signed originals to the following:

Office of the Attorney General
Child Support Division
P. O. Box 12017
Mail Code 062, Attn: Kristi Morgan
Austin, Texas 78711-2017

Upon receipt of the two signed originals and the completed Incident Response Plan, the documents will be routed to Alicia G. Key, Deputy Attorney General for Child Support, for signature. After the documents have been signed by all parties, one original will be returned to you for your records. Please be advised, the contract cannot be executed before both signed originals and a current Incident Response Plan have been returned.

If you have questions regarding the execution of this contract, please contact Robert Canales at (512) 460-6283.

Sincerely,

Allen Broussard
Manager, Government Contracts

Cooperative Agreement
between
The Office of the Attorney General
of the State of Texas
and
Hidalgo County, Texas

CONTRACT NO. 11-C0036

1. INTRODUCTION & PURPOSE

1.1. This document encompasses furnishing Registry Only court order information relating to Child Support, Protective Orders and Family Violence under the Texas Family Code, Title 4, Subtitle B and Suits Affecting the Parent-Child Relationship under the Texas Family Code, Title 5, Subtitle B for use in the State and Federal Case Registries ("State Case Registry") and local handling of inquiries on (including any necessary research) and receiving information about Child Support Cases where child support payments are remitted to the Texas State Disbursement Unit (TXSDU) ("Local Customer Service"). A County may contract to provide State Case Registry services only. However a county contracting to provide Local Customer Service must also contract to provide State Case Registry.

1.2. Hidalgo ("County") is contracting with the Office of the Attorney General ("OAG") to furnish Registry Only court order information relating to Child Support, Protective Orders and Family Violence under the Texas Family Code, Title 4, Subtitle B and Suits Affecting the Parent-Child Relationship under the Texas Family Code, Title 5, Subtitle B for use in the State and Federal Case Registries and handle inquiries on (including any necessary research) and receive information about Child Support Cases where child support payments are remitted to the TXSDU.

1.3. This Contract and its attachments (all of which are made a part hereof and expressly included herein) is entered into under the authority of Texas Family Code Section 231.002.

1.4. The term "OAG Systems" when used in this Contract encompasses the OAG Child Support Case Management System (commonly referred to as TXCSES and TXCSES Web) and any applicable automated systems used by the OAG's Vendor for the TXSDU including all of their subsystems, functions, processes, and security requirements.

1.5. Unless specified otherwise in this Contract, all procedures required to be followed by the County will be made available to the County on the OAG child support portal at http://portal.cs.oag.state.tx.us.

2. CONTRACT PERIOD

2.1. This Contract shall commence on September 1, 2010 and shall terminate on August 31, 2012, unless terminated earlier by provisions of this Contract.

3. REQUIREMENTS OF THE OAG AND THE COUNTY

3.1. State Case Registry Activities

3.1.1. County shall provide to OAG new and modified child support court orders entered after the effective date of the Contract for Registry Only child support court order information relating to Suits Affecting the Parent-Child Relationship.

3.1.1.1. County shall use the original court ordered documents to obtain the relevant information for entry to the OAG Systems or may use the "Record of Support" published in the Texas Family Law Manual, or a similar form completed by the District Clerk or Local Registry's office that summarizes the relevant court ordered child support information.

3.1.1.2. County must provide, if available, the following data elements:

3.1.1.2.1. participant type (dependent, custodial parent, non-custodial parent)

3.1.1.2.2. family violence indicator, if applicable

3.1.1.2.3. name of each participant (last and first)

3.1.1.2.4. sex code for each participant

3.1.1.2.5. social security number for each custodial parent and non-custodial parent and/or date of birth for each participant

3.1.1.2.6. cause number

3.1.1.2.7. cause county code

3.1.1.2.8. start date of cause

3.1.1.2.9. order modification date

3.1.1.2.10. address lines 1, 2, and 3, City, State, Zip (custodial parent only).

3.1.1.3. County shall provide data elements and/or information updates to the OAG Systems for Registry Only child support court orders signed on or after October 1, 1998.

3.1.1.4. County shall enter updates on OAG Systems for new case and /or member information provided by the custodial parent, non-custodial parent, employer, court or attorney of record to the County. This includes but is not limited to address information, changes in custody, court order terminations of all types, child emancipation, multiple payees or payors, case closure and order transfers.

3.1.1.5. County shall endeavor to provide all available new case information necessary to process child support payments received by the State Disbursement Unit within five (5) business days of the "date received time stamp" indicating that the order was received by the District Clerk or Local Registry's office. While this Timeliness Performance Standard is established as a goal for counties rather than a requirement, the OAG intends to monitor and report County performance toward meeting the Standard.

3.1.1.6. The provisions of 3.1.1.5 notwithstanding, County shall provide essential new case information necessary to process child support payments received by the State Disbursement Unit within five (5) business days of notification by the Texas TXSDU that a payment was received.

3.1.1.7. County shall provide updated information on existing orders within three (3) working days of receipt.

3.1.1.8. County shall provide new and updated case information by data entry directly onto OAG Systems, unless agreed to otherwise in writing by the OAG Contract Manager.

3.1.1.9. County shall ensure that payments on cases that have been redirected from the County registry to the TXSDU are paid to the TXSDU and that disbursements on such cases are no longer made by the County. The District Clerk or the Domestic Relations Office (as applicable) shall send all erroneously received child support payments to the TXSDU within one day of receipt.

3.1.1.10. County agrees that all court orders must direct child support payments to the (TXSDU) in accordance with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations. Where the County identifies a pattern of court orders from a

particular court or attorney that fail to comply with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations, the County will notify the OAG of same.

3.1.1.11. County shall work with the TXSDU to perform the required due diligence to place child support payments into the hands of custodial parents.

3.2. LOCAL CUSTOMER SERVICE

3.2.1. County Customer Service Unit Resources and Services

3.2.1.1. The term "Child Support Cases" when used in this Section and its Subsections means: Registry Only cases (a Registry Only case is a case where the payment is remitted to the State Disbursement Unit by an employer pursuant to an original order signed on or after January 1, 1994) and all IV-D cases (also known as "Full Service Cases").

3.2.1.2. County shall provide the resources necessary to accomplish the following allowable categories of customer service activity on Child Support Cases in accordance with the requirements of the Confidentiality and Security Section below: Payment Inquiry, Payment Research, Employer Payment Related Calls, OAG Payment Related Calls, Withholding Inquiry (Employer, Custodial Parent, Non-Custodial Parent).

3.2.1.2.1. These activities include but are not limited to:

3.2.1.2.1.1. Researching payments on Child Support Cases that should have been but were not received by the OAG.

3.2.1.2.1.2. Researching disbursements on Child Support Cases that should have been but were not received by the custodial parent.

3.2.1.2.1.3. Providing payment records on Child Support Cases to the court, the guardian ad litem for the child, the custodial and non-custodial parent and their attorneys, a person authorized by the custodial or non-custodial parent to have the payment history information, and a District or County attorney for purposes of pursuing prosecution for criminal non-support of a child.

3.2.1.2.1.4. Providing a certified copy of the court order timely to the OAG upon request.

3.2.1.2.2. The County Customer Service unit shall take inquiries and receive information by, but not limited to, e-mail, letters, phone calls, facsimiles and walk-ins.

3.2.2. Resources as used in this Customer Service Unit Resources and Services section include, but are not limited to, personnel, office space, equipment, phones and phone lines.

3.2.3. Customer Service Unit Documentation

3.2.3.1. County shall follow OAG procedures relating to data integrity, set forth in Attachment D, when accepting changes to case information *i.e.*, procedures to properly identify the caller.

3.2.3.2. County shall perform the Customer Service Unit services using the following guidelines:

3.2.3.2.1. Respond to written inquiries within five (5) County work days,

3.2.3.2.2. take action on information received within three (3) County work days,

3.2.3.2.3. document case record of action or information received at time of receipt,

3.2.3.2.4. follow up to a telephone inquiry within three (3) County work days,

3.2.3.2.5. return phone calls within three (3) County work days,

3.2.3.2.6. see a customer the same day or schedule appointment within three (3) County work days of request.

3.2.3.3. County shall use OAG processes and procedures for forwarding misdirected inquiries between the County, and the OAG and the OAG's designated agent where necessary by providing the toll free number to the OAG's Call Center (800-252-8014).

3.2.3.4. The electronic files associated with customer service activity that the County may receive and process are:

3.2.3.4.1. Full Service and Registry Only Collections, technical document name: Interface Control Document 012 (ICD012).

3.2.3.4.2. Registry Only Disbursement Data, technical document name: Interface Control Document 013 (ICD013).

3.2.3.4.3. Full Service and Registry Only Collection Adjustments, technical document name Interface Control Document 015 (ICD015).

3.2.3.4.4. Registry Only Case Data from Local Registries, technical document name: Interface Control document 050 (ICD050).

3.2.4. The electronic file associated with customer service activity that the County may transmit is:

3.2.4.1. OAG Systems and Local Registries Customer Service Activities, technical document name: Interface Control Document 035 (ICD035).

3.2.5. In the event of a failed transmission, or if an unprocessable electronic file is produced, County shall correct the problem and retransmit within one (1) working day of notification by the OAG.

3.2.6. County shall record on its automated system all financial data available from the OAG required to support the accurate dissemination of payment record information contemplated by this Contract or the County shall access, as needed, an OAG/TXCSES payment history record, as available, from the OAG TXCSES Web application.

3.3. ACCESSING OAG SYSTEMS

3.3.1. County Responsibilities

3.3.1.1. Work with the OAG or its designated agent to acquire, when needed, (at no cost to the County) from the OAG or its designated agent one personal computer, including the necessary software, to access the OAG Systems. County will work with the OAG or its designated agent to obtain the database access required. County is responsible for connecting the hardware to its own County network and for the cost associated therewith.

3.3.1.2. County must make necessary programming changes to its own automated child support system to accomplish the local customer service activities in this Contract. If the County employs a Vendor for maintenance and changes to its automated child support system, County must coordinate efforts between the County Vendor and the OAG or its designated agent.

3.3.1.3. Should the County desire to retain their legacy case management system, whether in-house or vendor based, the County is required to maintain strict data synchronization with the OAG Systems. To accomplish this, the County must demonstrate sufficient resources and

ability to receive and process into the County legacy system daily data updates from the OAG in ICD050 format.

3.3.1.4. County will be authorized to implement the data synchronization process upon completion of demonstrated ability and a documented system test.

3.3.1.5. Whether the County retains their legacy case management system or if data synchronization with the OAG Systems is not feasible the County shall enter all case/member information directly onto the designated OAG System unless agreed to otherwise in writing by the OAG Contract Manager.

3.3.1.6. The ICD050 computer file specifications and format will be made available to the County on the OAG child support portal. If these specifications change during the term of the Contract, the changes will be made available on the OAG child support portal and an e-mail notice of such availability will be sent to the County liaison. The County shall be responsible for implementing the changes to the electronic file specifications when and as required for OAG Systems processing, within a reasonable time frame.

3.3.1.7. To the extent necessary to fulfill its obligations under this Contract, County shall maintain, at no cost to the OAG, County hardware and software compatibility with the OAG Computer Systems and OAG file format needs, to include OAG software and OAG computer hardware and related equipment upgrades. OAG will provide County with as much notice as possible of intended OAG Computer Systems upgrades.

3.3.1.8. County is responsible for all the necessary phone lines. For those counties that do not have internet access the OAG will ensure that internet service is established for at least one personal computer. However, if the County is not covered by a local Internet Service Provider local telephone coverage area, then the County is responsible for any unavoidable long distance telephone charges that occur.

3.4. OAG Responsibilities

3.4.1. OAG will work with the County to make sure the County has one personal computer, including the necessary software, to access the OAG Systems. For those counties that do not have internet access, the OAG will ensure that internet service is established for at least one personal computer. However, if the County is not covered by a local Internet Service Provider local telephone coverage area, then the County is responsible for any unavoidable long distance telephone charges that occur.

4. REIMBURSEMENT

4.1. OAG shall monitor County OAG Systems State Case Registry and, if applicable, Local Customer Service activities (direct data entry or electronic file) and summarize for monthly reimbursement amounts.

4.2. OAG shall forward a Summary and Reimbursement Voucher for any particular month's activities to the County for review and approval by the 25th day of the following month.

4.3. If the County approves the Summary and Reimbursement Voucher, the County signs the voucher and returns it to OAG for payment within ten (10) County work days. County's signature constitutes approval of the voucher and certification that all services provided during the period covered by the voucher are included on the voucher. The OAG shall process the invoice for payment in accordance with the state procedures for issuing state payments and the Texas Prompt Payment Act.

4.3.1. County shall submit the invoice to:

Contract Manager, State Case Registry and Local Customer Service
Mail Code: 062
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

4.4. If County does not approve the Summary and Reimbursement Voucher, it shall return the voucher to the OAG within ten (10) County work days of receipt, detailing the basis of any disputed item, and include supporting documentation. The OAG shall review the returned voucher. If the dispute is resolved in the County's favor the OAG shall make payment as set forth in the preceding subsection. If the dispute is not resolved in the County's favor, the OAG shall make payment in accordance with the voucher originally sent to the County and forward a letter of explanation to the County.

4.4.1. OAG Rights Upon Loss of Funding

4.4.1.1. Legislative Appropriations

4.4.1.1.1. All obligations of the OAG are subject to the availability of legislative appropriations and, for federally funded procurements, to the availability of federal funds applicable to this procurement (see Provision of Funding by the United States, subsection below). The parties acknowledge that the ability of the OAG to make payments under this Contract is contingent upon the continued availability of funds for the Child Support Enforcement Strategy and the State Disbursement Unit Strategy (collectively "Strategies"). The parties acknowledge that funds are not specifically appropriated for this Contract and the OAG's continual ability to make payments under this Contract is contingent upon the funding levels appropriated to the OAG for the Strategies for each particular appropriation period. The OAG will use all reasonable efforts to ensure that such funds are available. The parties agree that if future levels of funding for the OAG Child Support Enforcement Strategy and/or the State Disbursement Unit Strategy are not sufficient to continue operations without any operational reductions, the OAG, in its discretion, may terminate this Contract, either in whole or in part. In the event of such termination, the OAG will not be considered to be in default or breach under this Contract, nor shall it be liable for any further payments ordinarily due under this Contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. The OAG shall make best efforts to provide reasonable written advance notice to County of any such termination. In the event of such a termination, County shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. OAG shall be liable for payments limited only to the portion of work the OAG authorized in writing and which the County has completed, delivered to the OAG, and which has been accepted by the OAG. All such work shall have been completed, per the Contract requirements, prior to the effective date of termination.

4.4.2. Provision of Funding by the United States

4.4.2.1. It is expressly understood that any and all of the OAG's obligations and liabilities hereunder are contingent upon the existence of a state plan for child support enforcement approved by the United States Department of Health and Human Services providing for the statewide program of child support enforcement, pursuant to the Social Security Act, and on the availability of Federal Financial Participation for the activities described herein. In the event that such approval of the state plan or the availability of Federal Financial Participation should lapse or otherwise terminate, the OAG, in its discretion, may terminate

this contract, either in whole or in part. In the event of such termination, the OAG will not be considered to be in default or breach under this contract, nor shall it be liable for any further payments ordinarily due under this contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. The OAG shall make best efforts to provide reasonable written advance notice to Contractor of any such termination. In the event of such a termination, County shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. OAG shall be liable for payments limited only to the portion of work the OAG authorized in writing and which the County has completed, delivered to the OAG, and which has been accepted by the OAG. All such work shall have been completed, per the Contract requirements, prior to the effective date of termination.

4.5. Reimbursement Rates

4.5.1. State Case Registry

4.5.1.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated cost that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purpose of reference only the federal share on the effective date of this Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of new and modified Registry Only Court Orders (together with all required data elements) provided to the OAG during the calendar month multiplied by a per new and modified Registry Only Court Order fee of $12.61 plus the number of Registry Only Court Orders updated during the calendar month multiplied by a per Registry Only Court Order updated fee of $4.01 per Registry Only Court Order updated. Thus: [(Calendar Month new and modified Registry Only Court Orders provided x $12.61) + (Calendar Month Registry Only Court Orders updated x $4.01)] x Federal Share = OAG Liability.

4.5.2. Local Customer Service

4.5.2.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated cost that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purpose of reference only the federal share on the effective date of this Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of inquiries on IV-D cases handled by County personnel during the calendar month, plus the number of inquiries on Registry Only cases (See Section 3.2.1 for the meaning of Registry Only cases) minus the Federal Disallowance Percentage, multiplied by a per inquiry fee of $4.13 per inquiry. For purpose of reference only the Federal Disallowance Percentage for SFY 2009 annualized is 19%. Thus: (Calendar Month IV-D Inquiries Handled by County Personnel) + (Calendar Month Registry Only Inquiries Handled by County Personnel - Federal Disallowance Percentage) x ($4.13) x (Federal Share) = OAG Liability.

4.6. Limitation of OAG Liability

4.6.1. The OAG shall be liable only for Contract associated costs incurred after commencement of this Contract and before termination of this Contract.

4.6.2. The OAG may decline to reimburse Allowable Costs which are submitted for reimbursement more than sixty (60) calendar days after the State Fiscal Year calendar quarter in which such costs are incurred.

4.6.3. County shall refund to the OAG within thirty (30) calendar days any sum of money which has been paid to the County which the OAG and County agree has resulted in an overpayment to County, provided that such sums may be offset and deducted from any amount owing but unpaid to County.

4.6.4. The OAG shall not be liable for reimbursing the County if the County fails to comply with the State Case Registry Activities, the County Customer Service Unit Resources and Services, and/ or the Customer Service Unit Documentation Sections above in accordance with the requirements of those sections.

4.6.5. The OAG shall not be liable for reimbursing the County for any activity currently eligible for reimbursement as of right without the necessity for a prior existing contract e.g. sheriff/processor fees. Nor shall the OAG be liable for reimbursing the County for any activities eligible for reimbursement under another contract or Cooperative Agreement with the OAG e.g. customer service related to cases in the same County's Integrated Child Support System ("ICSS") caseload, when the County has an ICSS contract with the OAG. Nor shall the OAG be liable for reimbursing the County for information correcting erroneous information previously provided by the County.

4.6.6. Notwithstanding any other provision of this Contract, the maximum liability of the OAG under this Contract is **Forty Eight Thousand Seven Hundred Dollars and No Cents ($48,700.00)**.

4.7. Assignment of Claims

4.7.1. County hereby assigns to the OAG any claims for overcharges associated with this Contract under 15 U.S.C. §1, et seq., and Tex. Bus. & Comm. Code §15.01, et seq.

5. CONTRACT MANAGEMENT

5.1. Written Notice Delivery

5.1.1. Any notice required or permitted to be given under this Contract by one party to the other party shall be in writing and shall be addressed to the receiving party at the address hereinafter specified. The notice shall be deemed to have been given immediately if delivered in person to the recipient's address hereinafter specified. It shall be deemed to have been given on the date of certified receipt if placed in the United States mail, postage prepaid, by registered or certified mail with return receipt requested, addressed to the receiving party at the address hereinafter specified.

5.1.1.1. County

The address of the County for all purposes under this Contract and for all notices hereunder shall be:

The Honorable Laura Hinojosa (or his/her successor in office)
Hidalgo County District Clerk
P.O. Box 87
Edinburg, TX 78540-

5.1.1.2. OAG

The address of the OAG for all purposes under this Contract and for all notices hereunder shall be:

Alicia G. Key (or her successor in office)
Deputy Attorney General for Child Support
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

With copies to:

Joseph Fiore (or his successor in office)
Managing Attorney, Contracts Attorneys, Child Support Division
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

and

Allen Broussard (or his successor in office)
Manager, Government Contracts
Office of the Attorney General
PO Box 12017
Austin, TX 78711-2017

5.2. Controlled Correspondence

5.2.1. After execution of this Contract, for a communication between the County and the OAG to be considered authoritative and binding it must be in writing and generated in accordance with procedures mutually agreed to by the County and the OAG. The OAG has procedures in place to number and track such communications as Controlled Correspondence. Any communication not generated in accordance with such procedures and not signed out by a designated position shall not be binding upon the parties and shall be of no effect. The OAG IV-D Director and the Contract Manager are designated as authorized signatories for all Controlled Correspondence with the County on behalf of the OAG. Unless otherwise notified by the County, the OAG shall consider the District Clerk or Local Registry's office, as the County signatory to this Contract, as authorized signatories for all Controlled Correspondence on behalf of the County. In the case of any inconsistency or conflict between such procedures and a Contract provision, the Contract provision shall control. Controlled Correspondence shall not be used to change pricing or alter the provisions of this Contract. Any such change requires a Contract amendment. Controlled Correspondence may be used to document interpretations of the provisions of this Contract.

5.3. Inspections, Monitoring and Audits

5.3.1. The OAG may monitor and/or conduct fiscal and/or program audits and/or investigations of the County's program performance at reasonable times. The OAG may at its option or at the request of County provide technical assistance to assist County in the operation of this program. County shall provide physical access without prior notice to all sites used for performance of service under this Contract to the OAG, United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas. County shall grant to the OAG, the United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas access, without prior notice, to all books, documents, and records of the County pertinent to this Contract. The County books, documents, and records may be inspected, monitored, evaluated, audited and copied. County shall cooperate fully with

the OAG, United States Department of Health and Human Services, Comptroller General of the United States, and State Auditor of Texas in the conduct of any audit and/or investigation including the providing of any requested books, documents, and records. County shall retain all financial records, supporting documents, statistical records, and any other records, documents, papers, logs, audit trails or books (collectively referred to as records) relating to the performances called for in this Contract. County shall retain all such records for a period of three (3) years after the expiration of the term of this Contract, or until the OAG or the United States are satisfied that all audit claim, negotiation, and litigation matters are resolved, whichever period is longer. Reports or other information relating to this program prepared by the County or at the request of the County shall be furnished to the OAG within ninety (90) days of availability. The requirements of this Subsection shall be included in all subcontracts.

5.4. Reimbursement of Audit Penalty

5.4.1. If funds are disallowed as a result of an audit finding contained in an audit (by County or County's independent auditor, the OAG, the State Auditor, the U.S. Department of Health and Human Services, the Comptroller General of the United States, or any of their duly authorized representatives) that County has failed to follow federal requirements for the IV-D program, then County agrees that the County shall refund to OAG the amount disallowed within thirty (30) calendar days of the date of the written OAG request for refund; provided further that such amounts may be offset and deducted from any funds payable under this Agreement.

5.5. Remedies for Non-Performance

5.5.1. Failure of the County to perform the contracted for services as required by this Contract shall be considered unsatisfactory performance. Any finding of unsatisfactory performance shall be communicated to the County in writing by the OAG Contract Manager. If the County wants to dispute the finding, a written dispute must be received by the OAG Contract Manager no later than fifteen (15) calendar days from the date the County received the written finding of unsatisfactory performance. The written dispute must detail why the County believes the finding is erroneous and must contain all supporting documentation. The OAG Contract Manager will review the dispute submission to determine the validity of the original finding of unsatisfactory performance. The determination of the OAG Contract Manager shall be final and shall conclude the review process. The OAG Contract Manager's determination shall be communicated to the County in writing. If a written dispute of the original finding of unsatisfactory performance is not received by the OAG Contract Manager by the time set forth above, the finding of unsatisfactory performance shall be deemed validated and the County shall have waived its right to dispute the finding.

5.5.2. If the finding of unsatisfactory performance is validated, the County shall be requested to provide the OAG Contract Manager with a corrective action plan. A corrective action plan, acceptable to the OAG Contract Manager, must be provided within a reasonable time period as specified by the OAG Contract Manager. Failure to provide an acceptable corrective action plan within the specified time period shall result in a withholding of payments due to County under this Contract until such time that an acceptable corrective action plan is provided.

5.5.3. If the County does not return to satisfactory status within four months of receiving notice that an unsatisfactory performance finding has been validated, OAG may withhold payments due to County under this Contract until the County is once again performing satisfactorily. If the unsatisfactory status persists for a total of six months after receiving notice of the validated unsatisfactory performance finding, OAG may terminate this Contract (in accordance with the Termination Section below) without payment to County for any costs incurred by County from the time that OAG commenced withholding payments due to County being in an unsatisfactory status. Where payments are to resume due to County having provided an acceptable corrective

action plan or having attained satisfactory performance status the first payment after resumption shall include all costs accrued during the period when payments to the County were withheld.

5.6. Training on OAG Systems

5.6.1. Any County staff performing functions under this Contract must be trained on OAG Systems. Classroom Training on OAG Systems will be scheduled upon request from the County, by the end of the quarter following such request. Classroom Training will be provided by OAG Regional Trainers at each of the OAG Regional Training Centers. County shall be responsible for any and all costs associated with this training, including, but not limited to, costs for travel, lodging, meals and per diem; provided, however that the OAG shall be responsible for the cost of training materials and equipment required to complete the training class. County is responsible for scheduling the training with the OAG and shall direct training requests to:

Larry Acevedo
Office of the Attorney General
Mail Code 053
PO Box 12017
Austin, TX 78711-2017
email address: CSD-TRN@cs.oag.state.tx.us

5.7. Assignment

5.7.1. County will not assign its rights under this Contract or delegate the performance of its duties under this Contract without prior written approval from the OAG.

5.8. Liaison

5.8.1. County and OAG each agree to maintain specifically identified liaison personnel for their mutual benefit during the term of the Contract. The liaison(s) named by County shall serve as the initial point(s) of contact for any inquiries made pursuant to this Contract by OAG and respond to any such inquiries by OAG. The liaison(s) named by OAG shall serve as the initial point(s) of contact for any inquiries made pursuant to this Contract by County and respond to any such inquiries by County. The liaison(s) shall be named in writing at the time of the execution of this Contract. Subsequent changes in liaison personnel shall be communicated by the respective parties in writing.

5.9. Subcontracting

5.9.1. It is contemplated by the parties hereto that County shall conduct the performances provided by this Contract substantially with its own resources and through the services of its own staff. In the event that County should determine that it is necessary or expedient to subcontract for any of the performances specified herein, County shall subcontract for such performances only after County has transmitted to the OAG a true copy of the subcontract County proposes to execute with a subcontractor and has obtained the OAG's written approval for subcontracting the subject performances in advance of executing a subcontract. County, in subcontracting for any performances specified herein, expressly understands and acknowledges that in entering into such subcontract(s), the OAG is in no manner liable to any subcontractor(s) of County. In no event shall this provision relieve County of the responsibility for ensuring that the performances rendered under all subcontracts comply with all terms of this Contract.

5.10. Dispute Resolution Process for County Breach of Contract Claim

5.10.1. The dispute resolution process provided for in Chapter 2260 of the Government Code shall be used, as further described herein, by the OAG and County to attempt to resolve any claim for breach of contract made by County.

5.10.2. County's claim for breach of this Contract that the parties cannot resolve in the ordinary course of business shall be submitted to the negotiation process provided in Chapter 2260, subchapter B, of the Government Code. To initiate the process, the County shall submit written notice, as required by subchapter B, to the Director, Child Support Division, Office of the Attorney General, P.O. Box 12017 (Mail Code 033), Austin, Texas 78711-2017. Said notice shall specifically state that the provisions of Chapter 2260, subchapter B, are being invoked. A copy of the notice shall also be given to all other representatives of the OAG and the County otherwise entitled to notice under this Contract. Compliance by the County with subchapter B is a condition precedent to the filing of a contested case proceeding under Chapter 2260, subchapter C, of the Government Code.

5.10.3. The contested case process provided in Chapter 2260, subchapter C, of the Government Code is the County's sole and exclusive process for seeking a remedy for any and all alleged breaches of contract by the OAG if the parties are unable to resolve their disputes under the immediate preceding subsection.

5.10.4. Compliance with the contested case process provided in subchapter C is a condition precedent to seeking consent to sue from the Legislature under Chapter 107 of the Civil Practices and Remedies Code. Neither the execution of this Contract by the OAG nor any other conduct of any representative of the OAG relating to the Contract shall be considered a waiver of sovereign immunity to suit.

5.10.5. The submission, processing and resolution of the County's claim is governed by the published rules adopted by the OAG pursuant to Chapter 2260, as currently effective, hereafter enacted or subsequently amended.

5.10.6. Neither the occurrence of an event nor the pendency of a claim constitutes grounds for the suspension of performance by the County, in whole or in part.

5.11. Reporting Fraud, Waste or Abuse

5.11.1. County must report any suspected incident of fraud, waste or abuse associated with the performance of this Contract to any one of the following listed entities:

5.11.1.1. the Contract Manager

5.11.1.2. the Deputy Director for Contract Operations, Child Support Division

5.11.1.3. the Director, Child Support Division the Deputy Director, Child Support Division

5.11.1.4. the OAG Ethics Advisor

5.11.1.5. the OAG's Fraud, Waste and Abuse Prevention Program ("FWAPP") Hotline (866-552-7937) or the FWAPP E-mailbox (FWAPP@oag.state.tx.us)

5.11.1.6. the State Auditor's Office hotline for fraud (1-800-892-8348).

5.11.2. The report of suspected misconduct shall include (if known):

5.11.2.1. the specific suspected misconduct

5.11.2.2. the names of the individual(s)/entity(ies) involved

5.11.2.3. the date(s)/location(s) of the alleged activity(ies)

5.11.2.4. the names and all available contact information (phone numbers, addresses) of possible witnesses or other individuals who may have relevant information; and

5.11.2.5. any documents which tend to support the allegations.

5.11.3. The words fraud, waste or abuse as used in this Section have the following meanings:

5.11.3.1. Fraud is the use of one's occupation for obtaining personal benefit (including benefit for family/friends) through the deliberate misuse or misapplication of resources or assets.

5.11.3.2. Waste is the extravagant careless or needless expenditure of funds or consumption of property that results from deficient practices, system controls, or decisions.

5.11.3.3. Abuse is the misuse of one's position, title or authority to obtain a personal benefit (including benefit for family/friends) or to attempt to damage someone else.

6. CONFIDENTIALITY AND SECURITY

6.1. Confidentiality and Security Provisions

6.1.1. General

6.1.1.1. Both OAG and County recognize and assume the duty to protect and safeguard confidential information. Confidential information specifically includes personally identifiable information such as Social Security Number, full name, date of birth, home address, account number, and case status. Each entity acknowledges that the loss of confidentiality, integrity and availability of information assets is a risk which can be minimized by effective security safeguards and enforced compliance with information security policies, standards and procedures.

6.1.1.2. OAG recognizes that County has existing statutory responsibilities to maintain confidentiality of records related to state district courts (juvenile, family, probate, civil and criminal), county courts and national and state criminal records (FBI, NCIC, TCIC). OAG also recognizes that County has existing processes and procedures that ensure the security and confidentiality of this information and data and is subject to security audits or assessments by these authorities.

6.1.1.3. This agreement requires County to retrieve data from the courts and other sources and create data within TXCSES or TXCSES Web.

6.1.1.4. County acknowledges and agrees to protect OAG Data as confidential. All references to "OAG Data" shall mean all data and information (i) originated by OAG and/or submitted to County by or on behalf of OAG, or (ii) which County accesses from OAG systems in connection with provision of the Agreement Services. OAG Data does not include data and information originated by County in the performance of its duties. Upon request by OAG, County shall execute and deliver any documents that may be necessary or desirable under any law to preserve or enable OAG to enforce its rights with respect to OAG Data. OAG rights and privileges applicable to OAG Data shall survive expiration or any termination of this Agreement, and shall be perpetual. Tex. Gov't Code Chapter 552 defines the exclusive mechanism for determining whether OAG Data are subject to public disclosure. However, data that is publicly known and generally available to the public is not subject to these Confidentiality and Security Provisions.

6.1.1.5. If any term or provision of this Confidentiality and Security Provision, shall be found to be illegal or unenforceable, it shall be deemed independent and divisible, and notwithstanding such illegality or unenforceability, all other terms or provisions in this Confidentiality and Security Provision, shall remain in full force and effect and such illegal or unenforceable term or provision shall be deemed to be deleted.

6.1.1.6. County shall develop and implement access protection lists. The access protection lists shall document the name and other identifying data for any individual, authorized pursuant to County's request, to access, use or disclose OAG Data, as well as any special conditions and limitations applicable to each authorization. County shall remove individuals from or change the access rights of individuals on the access protection list immediately upon such individual no longer requiring access. At least quarterly, OAG shall send County a list of TXCSES Web users and County shall review and update its access protection lists and ensure that the access protection lists accurately reflect the individuals and their access level currently authorized. County shall notify OAG of the authorized personnel that should have access rights to OAG Data and information in the method prescribed by OAG. County will immediately notify OAG when an individual's access to OAG systems is no longer relevant. OAG, in its sole discretion, may deny or revoke an individual's access to OAG Data and information and any of its systems.

6.1.1.7. County shall perform background reviews, to include a criminal history record review, on all County employees who will have access to OAG Data and information, and any OAG system. County shall certify to OAG that such reviews have been conducted and that in County's opinion the aforesaid employees are deemed trustworthy. County may request OAG to perform such reviews. In such an instance, County shall provide OAG with any required information, consent and authorization to perform the reviews and OAG shall perform the reviews at its own expense.

6.1.1.8. All references to "Agreement Services" shall include activities within the scope of this Agreement.

6.1.1.9. County shall comply with all applicable statutory and regulatory provisions requiring that information be safeguarded and kept confidential. These statutes and regulatory provisions include but are not limited to 42 U.S.C. §§ 653 and 654; 45 CFR §§ 307.10, 307.11 and 307.13; 26 U.S.C. 6103 (IRC 6103); IRS Publication 1075 (Rev. 10-2007) and § 231.108 of the Texas Family Code, each as currently written or as may be amended, revised or enacted. County shall also comply with OAG policy, processes and procedures concerning the safeguarding and confidentiality of information, and computer security (including any requirements set forth in Attachment F, entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information"). The requirements of these Confidentiality and Security Provisions shall be included in, and apply to, subcontracts and agreements the County has with anyone performing Agreement Services on County's behalf.

6.1.1.10. This Agreement is between County and OAG, and is not intended to create any independent cause of action by any third party, individual, or entity against OAG or County.

6.2. OAG Data Usage and Storage

6.2.1. County agrees to maintain physical security for OAG data by maintaining an environment designed to prevent loss or unauthorized removal of data. County shall ensure that all persons having access to data obtained from OAG Systems are thoroughly briefed on related security procedures, use restrictions, and instructions requiring their awareness and compliance. County shall ensure that all County personnel having access to OAG Data receive annual reorientation

sessions when offered by the OAG and all County personnel that perform or are assigned to perform Agreement Services shall annually re-execute, and/or renew their acceptance of, all applicable security documents and to ensure that they remain alert to all security requirements. County personnel shall only be granted access to OAG Systems after they have received all required security training, read the OAG Data Security Policy Manual (Attachment A), signed the acknowledgment (and County has given the signed acknowledgment to the OAG Contract Manager) and read and accepted the OAG Automated Computer System Access Statement of Responsibility (Attachment B) and the Child Support online Login Policy (Attachment C).

6.2.2. OAG Data are not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by County. Any exception to this prohibition must have OAG prior approval. Such approval may only be granted by Controlled Correspondence or Contract amendment. This prohibition does not apply to County Information Systems backup procedure. County Information Systems backup procedure is subject to the United States Internal Revenue Service requirements set forth in IRS Publication 1075 (Rev.10-2007) and Attachment F entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".

6.2.3. County stipulates, covenants, and agrees that it will not access, use or disclose OAG Data beyond its limited authorization or for any purpose not necessary for the performance of its duties under this Agreement. Without OAG's approval (in its sole discretion), County will not: (i) use OAG Data other than in connection with providing the Agreement Services; (ii) disclose, sell, assign, lease, or otherwise provide OAG Data to third parties, including any local, state, or Federal legislative body; (iii) commercially exploit OAG Data or allow OAG Data to be commercially exploited; or (iv) create, distribute or use any electronic or hard copy mailing list of OAG Customers for purposes other than in connection with providing the Agreement Services. However, nothing in this agreement is intended to restrict County from performing its other authorized duties. For example, the duty to disseminate copies of court orders to requesting parties that necessarily includes data such as names and addresses. In the event that County fails to comply with this subsection, OAG may exercise any remedy, including immediate termination of this Agreement.

6.2.3.1. County agrees that it shall comply with all state and federal standards regarding the protection and confidentiality of OAG Data as currently effective, subsequently enacted or as may be amended. OAG Data accessed shall always be maintained in a secure environment (with limited access by authorized personnel both during work and non-work hours) using devices and methods such as, but not limited to: alarm systems, locked containers of various types, fireproof safes, restricted areas, locked rooms, locked buildings, identification systems, guards, or other devices reasonably expected to prevent loss or unauthorized removal of manually held data. County shall also protect against unauthorized use of passwords, keys, combinations, access logs, and badges. Whenever possible, computer operations must be in a secure area with restricted access. In situations such as remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection. This protection must include (where communication is through an external not-organization-controlled network [e.g. the Internet]) multifactor authentication that is compliant with NIST SP 800-63, Electronic authentication Guidance level 3 or 4, and shall be consistent with IRS Publication 1075 Section 4.7 Alternate Work Sites.

6.3. OAG Data Retention and Destruction, and Public Information Requests

6.3.1. Any destruction or purging of OAG Data shall be destroyed and/or purged in accordance with state and federal statutes, rules and regulations. Within ten (10) business days of destruction or purging, County will provide the OAG with a completed OAG-Child Support Division

"Certificate of Destruction for Contractors and Vendors" (Attachment H; a copy of which is attached hereto and included herein).

6.3.2. In the event of Agreement expiration or termination for any reason, County shall ensure the security of any OAG Data remaining in any storage component to prevent unauthorized disclosures. Within twenty (20) business days of Agreement expiration or termination, County shall provide OAG with a signed statement detailing the nature of the OAG Data retained, type of storage media, physical location(s), and any planned destruction date.

6.3.3. County expressly does not have any actual or implied authority to determine whether any OAG Data are public or exempted from disclosure. County is not authorized to respond to public information requests which would require disclosure of otherwise confidential information on behalf of the OAG. County agrees to forward to the OAG, by facsimile within one (1) business day from receipt all request(s) for information associated with the County's services under this Agreement. County shall forward via fax any information requests to:

Public Information Coordinator
Office of the Attorney General
Fax (512) 494-8017

6.4. Security Incidents

6.4.1. Response to Security Incidents

6.4.1.1. County shall respond to detected security incidents. The term "security incident" means an occurrence or event where the confidentiality, integrity or availability of OAG Data may have been compromised. County shall maintain an internal incident response plan to facilitate a quick, effective and orderly response to information security incidents. The incident response plan should cover such topics as:

6.4.1.1.1. Initial responders

6.4.1.1.2. Containment

6.4.1.1.3. Management Notification

6.4.1.1.4. Documentation of Response Actions

6.4.1.1.5. Expeditious confirmation of system integrity

6.4.1.1.6. Collection of audit trails and similar evidence

6.4.1.1.7. Cause analysis

6.4.1.1.8. Damage analysis and mitigation

6.4.1.1.9. Internal Reporting Responsibility

6.4.1.1.10. External Reporting Responsibility

6.4.1.1.11. OAG Contract Manager's and OAG CISO's name, phone number and email address.

6.4.2. Attachment G is County's current internal incident response plan. Any changes to this incident response plan require OAG approval (which approval shall not be unreasonably withheld) and may be made by Controlled Correspondence.

6.5. Notice

6.5.1. Within one (1) hour of concluding that there has been, any OAG Data security incident County shall initiate damage mitigation and notify the OAG Chief Information Security Officer ("OAG CISO") and the OAG Contract Manager, by telephone and by email, of the security incident and the initial damage mitigation steps taken. Current contact information shall be contained in the Plan.

6.5.2. Within twenty-four (24) hours of the discovery, County shall conduct a preliminary damage analysis of the security incident; commence an investigation into the incident; and provide a written report to the OAG CISO, with a copy to the OAG Contract Manager fully disclosing all information relating to the security incident and the results of the preliminary damage analysis. This initial report shall include, at a minimum: time and nature of the incident (e.g., OAG data loss/corruption/intrusion); cause(s); mitigation efforts; corrective actions; and estimated recovery time.

6.5.3. Each day thereafter until the investigation is complete, County shall: (i) provide the OAG CISO, or the OAG CISO's designee, with a daily oral or email report regarding the investigation status and current damage analysis; and (ii) confer with the OAG CISO, or the OAG CISO's designee, regarding the proper course of the investigation and damage mitigation.

6.5.4. Whenever daily oral reports are provided, County shall provide, by close of business each Friday, an email report detailing the foregoing daily requirements.

6.6. Final Report

6.6.1. Within five (5) business days of completing the damage analysis and investigation, County shall submit a written Final Report to the OAG CISO with a copy to the OAG Contract Manager, which shall include:

6.6.1.1. a detailed explanation of the cause(s) of the security incident;

6.6.1.2. a detailed description of the nature of the security incident, including, but not limited to, extent of intruder activity (such as files changed, edited or removed; Trojans), and the particular OAG Data affected; and

6.6.1.3. a specific cure for the security incident and the date by which such cure shall be implemented, or if the cure has been put in place, a certification to OAG that states the date County implemented the cure and a description of how the cure protects against the possibility of a recurrence.

6.6.2. If the cure has not been put in place by the time the report is submitted, County shall within thirty (30) calendar days after submission of the final report, provide a certification to OAG that states the date County implemented the cure and a description of how the cure protects against the possibility of a recurrence.

6.6.3. If County fails to provide a Final Report and Certification within forty-five (45) calendar days, or as otherwise agreed to, of the security incident, County agrees that OAG may exercise any right, remedy or privilege which may be available to it under applicable law of the State and any other applicable law. The exercise of any of the foregoing remedies will not constitute a termination of this Agreement unless OAG notifies County in writing prior to the exercise of such remedy.

6.7. Independent Right to Investigate

6.7.1. OAG reserves the right to conduct an independent investigation of any security incident, and should OAG choose to do so, County shall cooperate fully, making resources, personnel and

systems access available. If at all possible, OAG will provide reasonable notice to County that it is going to conduct an independent investigation.

6.8. Security Audit

6.8.1. Right to Audit, Investigate and Inspect the Facilities, Operations, and Systems Used in the Performance of Agreement Services.

6.8.1.1. County shall permit OAG, the State Auditor of Texas, the United States Internal Revenue Service, the United States Department of Health and Human Services and the Comptroller General of the United States to:

6.8.1.1.1. monitor and observe the operations of, and to perform security investigations, audits and reviews of the operations and records of, the County;

6.8.1.1.2. inspect its information system in order to access security at the operating system, network, and application levels; provided, however, that such access shall not interfere with the daily operations of managing and running the system; and

6.8.1.1.3. enter into the offices and places of business of County and County's subcontractors for a security inspection of the facilities and operations used in the performance of Agreement Services. Specific remedial measures may be required in cases where County or County's subcontractors are found to be noncompliant with physical and/or OAG data security protection.

6.8.1.2. When OAG performs any of the above monitoring, observations, and inspections, OAG will provide County with reasonable notice that conforms to standard business audit protocol. However prior notice is not always possible when such functions are performed by the State Auditor of Texas, the United States Internal Revenue Service, the United States Department of Health and Human Services and the Comptroller General of the United States. In those instances the OAG will endeavor to provide as much notice as possible but the right to enter without notice is specifically reserved.

6.8.1.3. Any audit of documents shall be conducted at County's principal place of business and/or the location(s) of County's operations during County's normal business hours and at OAG's expense. County shall provide on County's premises, (or if the audit is being performed of a County's subcontractor, the County's subcontractor's premises, if necessary) the physical and technical support reasonably necessary for OAG auditors and inspectors to perform their work.

6.8.1.4. County shall supply to the OAG and the State of Texas any data or reports rendered or available in conjunction with any security audit of County or County's subcontractors, if such data or reports pertain, in whole or in part, to the Agreement Services. This obligation shall extend to include any report(s) or other data generated by any security audit conducted up to one (1) year after the date of termination or expiration of the Agreement.

6.9. Remedial Action

6.9.1. Remedies Not Exclusive and Injunctive Relief

6.9.1.1. The remedies provided in this section are in addition to, and not exclusive of, all other remedies available within this Agreement, or at law or in equity. OAG's pursuit or non-pursuit of any one remedy for a security incident(s) does not constitute a waiver of any other remedy that OAG may have at law or equity.

6.9.1.2. If injunctive or other equitable relief is available, then County agrees that OAG shall not be required to post bond or other security as a condition of such relief.

6.10. Notice to Third Parties

6.10.1. Subject to OAG review and approval, County shall provide notice to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the security incident, with such notice to include: (i) a brief description of what happened; (ii) to the extent possible, a description of the types of personal data that were involved in the security breach (e.g., full name, SSN, date of birth, home address, account number, etc.); (iii) a brief description of what is being done to investigate the breach, mitigate losses, and to protect against any further breaches; (iv) contact procedures for those wishing to ask questions or learn additional data, including a telephone number, website, if available, and postal address; and, (v) instructions for accessing the Consumer Protection Identity Theft section of the OAG website. County and OAG shall mutually agree on the methodology for providing the notice. However, the notice method must comply with Section 521.053, Texas business and Commerce Code (as currently enacted or subsequently amended). Provided further that County must also comply with Section 521.053's "consumer reporting agency" notification requirements.

6.10.2. County shall be responsible for responding to and following up on inquiries and requests for further assistance from persons notified under the preceding section.

6.10.3. If County does not provide the required notice, OAG may elect to provide notice of the security incident. County and OAG shall mutually agree on the methodology for providing the notice. However, the notice method must comply with Section 521.053, Texas business and Commerce Code (as currently enacted or subsequently amended). Costs (excluding personnel costs) associated with providing notice shall be reimbursed to OAG by County. If County does not reimburse such cost within thirty (30) calendar days of request, OAG shall have the right to collect such cost. Additionally, OAG may collect such cost by offsetting or reducing any future payments owed to County.

6.11. Commencement of Legal Action

6.11.1. County shall not commence any legal proceeding on OAG's behalf outside the scope of the Agreement Services without OAG's express written consent. OAG shall not commence any legal proceedings on County's behalf without County's express written consent.

7. AMENDMENT

7.1. This Contract shall not be amended or modified except by written amendment executed by duly authorized representatives of both parties. Any alterations, additions or deletions to the terms of this Contract which are required by changes in federal or state law are automatically incorporated into this Contract without written amendment to this Contract and shall be effective on the date designated by said federal or state law.

8. TERMINATION OF CONTRACT

8.1. Termination

8.1.1. Either party to this Contract shall have the right to either terminate this Contract in its entirety or in part. However, a County continuing to contract to provide Local Customer Service services must also continue to contract to provide State Case Registry services. The Contract, or portion of the Contract, may be terminated by the terminating party notifying the other party in writing of

such termination and the proposed date of the termination no later than thirty (30) calendar days prior to the effective date of such termination.

8.2. Survival of Terms

8.2.1. Termination of this Contract for any reason shall not release the parties from any liability or obligation set forth in this Contract that is expressly stated to survive any such termination or by its nature would be intended to be applicable following any such termination.

9. TERMS AND CONDITIONS

9.1. Federal Terms and Conditions

9.1.1. Compliance with Law, Policy and Procedure

9.1.1.1. County shall perform its obligations hereunder in such a manner that ensures its compliance with OAG, policy, processes and procedure. It shall also comply with all state and federal laws, rules, regulations, requirements and guidelines applicable to County: (1) performing its obligations hereunder and to assure with respect to its performances hereunder that the OAG is carrying out the program of child support enforcement pursuant to Title IV, Part D of the federal Social Security Act of 1935 as amended; (2) providing services to the OAG as these laws, rules, regulations, requirements and guidelines currently exist and as they are amended throughout the term of this Contract County understands and agrees that from time to time OAG may need to change its policy, processes or procedures and that such change shall not entitle County to any increased cost reimbursement under this Contract; provided, however, that County may exercise its right to terminate the Contract in accordance with the Termination Section above. OAG shall provide County e-mail notice of any change in OAG policy, processes or procedures.

9.1.2. Civil Rights

9.1.2.1. County agrees that no person shall, on the ground of race, color, religion, sex, national origin, age, disability, political affiliation, or religious belief, be excluded from participation in, be denied the benefits of, be subjected to discrimination under, or be denied employment in the administration of, or in connection with, any program or activity funded in whole or in part with funds provided by this Contract. County shall comply with Executive Order 11246, "Equal Employment Opportunity" as amended by Executive Order 11375, "Amending Executive Order 11246 relating to Equal Employment Opportunity" and as supplemented by regulations at 41 C.F.R. Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." County shall ensure that all subcontracts comply with the above referenced provisions.

9.1.3. Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion from Participation in Contracts Exceeding $100,000.00.

9.1.3.1. County certifies by entering into this Contract, that neither it nor its principals are debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.

9.1.3.2. The certification requirement of this provision shall be included in all subcontracts that exceed $100,000.

9.1.4. Environmental Protection (Contracts in Excess of $100,000.00)

9.1.4.1. County shall be in compliance with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act (42 USC 1857(h)) Section 508 of the Clean Water Act (33 USC 1368) Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15). The requirements of this provision shall be included in all subcontracts that exceed $100,000.

9.1.5. Certain Disclosures Concerning Lobbying [Contracts in excess of $100,000]

9.1.5.1. Certain Counties shall comply with the provisions of a federal law known generally as the Lobbying Disclosure Acts of 1989, and the regulations of the United States Department of Health and Human Services promulgated pursuant to said law, and shall make all disclosures and certifications as required by law. County must submit at the time of execution of this Contract a Certification Regarding Lobbying (Attachment E). This certification certifies that the County will not and has not used federally appropriated funds to pay any person or organization for influencing or attempting to influence any officer or employee of any Federal agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal Contract, grant or any other award covered by 31 U.S.C. 1352. It also certifies that the County will disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award by completing and submitting Standard Form LLL.

9.1.5.2. The requirements of this provision shall be included in all subcontracts exceeding $100,000.

9.2. News Releases or Pronouncements

9.2.1. News releases, advertisements, publications, declarations, and any other pronouncements pertaining to this Contract by County, using any means or media, must be approved in writing by the OAG prior to public dissemination.

9.3. Date Standard

9.3.1. Four-digit year elements will be used for the purposes of electronic data interchange in any recorded form. The year shall encompass a two digit century that precedes, and is contiguous with, a two digit year of century (e.g. 1999, 2000, etc.). Applications that require day and Month information will be coded in the following format: CCYYMMDD. Additional representations for week, hour, minute, and second, if required, will comply with the international standard ISO 8601: 1988, "Data elements and interchange formats--Information interchange--Representation of dates and times."

9.4. Headings

9.4.1. The headings for each section of this Contract are stated for convenience only and are not to be construed as limiting.

9.5. Agreement Relating to Debts or Delinquencies Owed to the State

9.5.1. As required by §2252.903, Government Code, the County agrees that any payments due under this Contract shall be directly applied towards eliminating any debt or delinquency including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support.

9.6. Non-Waiver of Rights

9.6.1. Failure of a party to require performance by another party under this Contract will not affect the right of such party to require performance in the future. No delay, failure, or waiver of either party's exercise or partial exercise of any right or remedy under this Contract shall operate to limit, impair, preclude, cancel, waive or otherwise affect such right or remedy. A waiver by a party of any breach of any term of this Contract will not be construed as a waiver of any continuing or succeeding breach. Should any provision of this Contract be invalid or unenforceable, the remainder of the provisions will remain in effect.

9.7. No Waiver of Sovereign Immunity

9.7.1. The parties expressly agree that no provision of this contract is in any way intended to constitute a waiver by the OAG or the State of Texas of any immunities from suit or from liability that the OAG or the State of Texas may have by operation of law.

9.8. Severability

9.8.1. If any provision of this contract is construed to be illegal or invalid, such construction will not affect the legality or validity of any of its other provisions. The illegal or invalid provision will be deemed severable and stricken from the contract as if it had never been incorporated herein, but all other provisions will continue in full force and effect.

9.9. Applicable Law and Venue

9.9.1. Applicable Law and Venue: County agrees that this Contract in all respects shall be governed by and construed in accordance with the laws of the State of Texas, except for its provisions regarding conflicts of laws. County also agrees that the exclusive venue and jurisdiction of any legal action or suit brought by County concerning this Contract is, and that any such legal action or suit shall be brought, in a court of competent jurisdiction in Travis County, Texas. OAG agrees that any legal action or suit brought by OAG concerning this Contract shall be brought in a court of competent jurisdiction in Hidalgo County. All payments under this Contract shall be due and payable in Travis County, Texas.

9.10. Entire Contract

9.10.1. This instrument constitutes the entire Contract between the parties hereto, and all oral or written contracts between the parties relating to the subject matter of this Contract that were made prior to the execution of this Contract have been reduced to writing and are contained herein.

9.11. Counterparts

9.11.1. This Contract may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

9.12. Attachments

9.12.1. Attachment A: OAG Information Security Policy Manual

9.12.2. Attachment B: OAG Automated Computer System Access - Statement of Responsibility

9.12.3. Attachment C: Child Support Online Login Policy

9.12.4. Attachment D: Data Integrity Procedures Changes to Case Information

9.12.5. Attachment E: Certification Regarding Lobbying

9.12.6. Attachment F: IRS Publication 1075 (Rev.10-2007)

9.12.7. Attachment G: Incident Response Plan

9.12.8. Attachment H: Certificate of Destruction for Contractors and Vendors

THIS CONTRACT IS HEREBY ACCEPTED

OFFICE OF THE ATTORNEY GENERAL	**HIDALGO COUNTY**
Alicia G. Key Deputy Attorney General for Child Support	The Honorable Rene Ramirez County Judge, Hidalgo County

ATTACHMENT A

ATTORNEY GENERAL OF TEXAS

GREG ABBOTT

Office of the Attorney General

Information Technology Security Policy Manual

Version 3.0
February 12, 2009

Presented by:
Dr. Walt H. Foultz
Chief Information Security Officer

Table of Contents

1. Information Security Policy

1.1. Attorney General Policy Statement

The Office of the Attorney General (OAG) is committed to data integrity. Every reasonable effort must be made to protect information that is entrusted to this agency. An effective data security protocol, supported by an appropriately rigorous security structure, is critical to the success of an information security program. The OAG's Chief Information Security Officer is responsible for managing and developing the information security program, which includes identifying and resolving all at-risk information system assets, as well as supporting the operational needs of the agency.

An effective information security program encompasses many activities requiring commitment and cooperation among both employees and management of the OAG. All information resources users must be involved in the success of this strategic effort.

1.2. Scope of Policy

This policy applies to all OAG "information resources" that are used by or for the OAG throughout its life cycle. "Information resources are the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.[1]

This policy also applies to all users of OAG information resources, and electronic data regardless of location.

To the extent there is any conflict between this policy and the Sensitive Personal Information Privacy Policy.

1.3. OAG Information Security Policy Purpose & Intent

The purpose and intent of this policy document is to familiarize users of OAG information resources with the need to protect these resources in a prescribed manner and in accordance with appropriate standards.

1.4. Definitions

Access:
The physical or logical capability to interact with, or otherwise make use of information resources

Business Continuity Planning:
The process of identifying mission critical data systems and business functions, analyzing the risks and probabilities of service disruptions and developing procedures to restore those systems and functions.

Control:
Any action, device, policy, procedure, technique, or other measure that improves security.

Encryption:
The conversion of plain text (human readable) information into a mathematical cipher or algorithm to create an electronic message that conceals the true meaning.

Information Resources:
The term is defined in Section 1.2 of this policy.

Information Resource Data:
Any data electronically produced, modified, transmitted, or stored while in electronic form.

Information Resources Asset:
A subset of the term information resources that refers to computing hardware such as a laptop computer, desktop PC, network server, or computer software.

2. Management Security Controls

2.1. State Agency Head - Attorney General

The Attorney General, as the state agency head, is responsible for establishing and maintaining an information security and risk management program.[ii] It is the responsibility of the Attorney General to ensure that the agency's information resources are protected from the effects of damage, destruction, and unauthorized or accidental modification, access or disclosure.

2.2. Management Responsibility

The protection of information resources is a management responsibility. Managing information security within the OAG requires commitment and support on the part of executive, technical and program management. All managers must be involved in the security and awareness program, and be familiar with and enforce OAG policies and procedures among their staff and employees.

2.3. Information Resources Manager (IRM)

The IRM is the agency executive who must approve the information technology assets and services necessary to conduct the information security program, as well as use executive authority where necessary to enable the success of the information security program.

2.4. Chief Information Security Officer (CISO)

The CISO reports to the IRM. It is the CISO's duty and responsibility to:

- Manage, develop and coordinate the development of the OAG information security program and all other information security policies, standards and procedures.

- Collaborate with IT divisions, information resources owners and executive management in the development of procedures to ensure compliance with external information security requirements.

- Develop training materials on information security for employees and all other authorized users, and collaborate with agency training staff to establish a standardized agency-wide information security training program.

- Develop and implement incident reporting and incident response processes and procedures to address any security incident/breach, violation of policy or complaint.

- Serve as the official agency point of contact for all information security inquiries and audits.

- Develop and implement an ongoing risk assessment program, including recommending methods for, and overseeing of, vulnerability detection and testing.

- Monitor security legislation, regulations, advisories, alerts and vulnerabilities, and communicate accordingly with IT divisions, data owners and executive management.

- Review agency information systems and provide written reports that identify potential security risks and recommended solutions as appropriate.

- Provide annual report to executive management on security program and risk mitigation.

- Collaborate with IT personnel, the Records Management Officer, and legal counsel to preserve data in accordance with appropriate data preservation and litigation hold procedures.

2.5. Information Security Officers (ISO).

A full-time ISO will be assigned to oversee the Administrative and Legal Divisions (A&L), while another full-time ISO will be assigned to oversee the Child Support Divisions (CS). The A&L ISO and CS ISO will report directly to the CISO.

These ISOs will function as the representatives of the CISO and will oversee the daily security activities within their supported division operations. The A&L ISO and CS ISO will review all information security procedures and recommend changes as appropriate.

2.6. Information Resource Owner

An information resource owner is defined as a person responsible for a business function and for determining controls and access to information resources supporting that business function.[iii] The state agency head or his or her designated representative(s) shall review and approve ownership of information resources and their associated responsibilities.[iv] For the OAG Information Resource Owners are typically Division Chiefs.

Where information resources are used by more than one division, the owners shall reach a consensus as to the designated owner with responsibility for the information resources and advise the A&L or CS ISO of their decision.[v]

The information owner or his or her designated representatives(s), with the CISO's concurrence, are responsible for and authorized to:

- Approve access to, and formally assign custody of, an information resource;
- Determine the information resources' value;
- Specify data control requirements and convey them to users and custodians;
- Specify appropriate controls, based on risk assessment, to protect the agency's information resources from unauthorized modification, deletion or disclosure. Controls shall extend to information resources outsourced by the agency in accordance with the Department of Information Resources' (DIR) information security policy;
- Confirm that controls are in place to ensure the accuracy, authenticity and integrity of electronic data;
- Ensure compliance with applicable controls;
- Assign custody of information technology assets and provide appropriate authority to implement security controls and procedures; and
- Review access lists based on documented security risk management decisions.

2.7. Information Custodian

An information custodian is defined as any person or group who is charged with the physical possession of information technology assets.[vi] Custodians are the technical managers that provide the facilities, controls and support services to owners and users of information. Custodians of information technology assets, including entities providing outsourced information resources services to state agencies, must:

- Implement the controls specified by the owner(s);

- Provide physical and procedural safeguards for the information resources;
- Assist owners in understanding and evaluating the cost-effectiveness of controls and monitoring;
- Administer access to the information resources; and
- Implement appropriate monitoring techniques and procedures for detecting, reporting and investigating incidents.

2.8. Information System User

All authorized users of OAG information resources (including, but not limited to, OAG personnel, temporary employees, contractors, sub-contractors, auditors, consultants or agents), shall formally acknowledge that they will comply with the OAG's security policies and procedures or they shall not be granted access to the information technology assets. The CISO will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to OAG information technology assets.[vii] Users also have the responsibility to report all suspected violations of OAG information security policies to their Division Chief and the ISO responsible for their division. The ISO will then report the suspected violation to the CISO. (See section 3.4)

Users of OAG information technology assets shall have no expectation of privacy for information contained within or processed by an OAG information technology asset. Electronic files created, sent, received by, or stored on, OAG information technology assets that are owned, leased, administered, or otherwise under the custody and control of the OAG are not private and may be accessed by OAG IT employees at any time without knowledge of the information technology asset user or owner. Electronic file content may be accessed by appropriate personnel, including, but not limited to, information security personnel, records management personnel and legal counsel.[viii]

3. Operational Security Controls

3.1. Risk Management Framework

The OAG employs a risk-based information security strategy, which provides a method to eliminate or mitigate identified risk to an organization in order to maximize the positive effects of information security activities while minimizing costs to the organization.

3.2. Risk Assessment

It is the responsibility of the CISO to regularly assess the risk to all OAG electronic data, systems, networks and information technology operations, and report the results of the assessment to OAG executive management and other appropriate personnel.

3.3. Asset Management

Management of OAG equipment including laptops, PDAs, and other IT equipment is an asset control and physical security issue and not within the scope of this Information Technology Security policy. For policy regarding those items, refer to the OAG's general Policies and Procedures as well as the Special High-Risk Items Policy.

3.4. Disaster Recovery & Business Continuity

The OAG is charged with providing a comprehensive disaster recovery plan and business continuity procedure for all essential Data Center and field operations. This activity will be supported in part by the Information Security Division (ISD).

3.5. Outsourced Data Center Operations & Security Responsibility

As a requirement of House Bill 1516 by the 79th Legislature, OAG information technology systems will be consolidated at the DIR Consolidated Data Centers (CDC).

While DIR and their contractor will supply much of the required services and activities to protect OAG data, systems and networks, the OAG still has responsibility for ensuring the safety of OAG data.[ix]

4. Personnel Security Policy

4.1. Statement of Responsibility

OAG personnel are required to sign a Statement of Responsibility acknowledging that they agree to comply with all applicable information security policies, protocols and procedures as set forth in the OAG Information Security Policy Manual. This statement of responsibility will remain a part of the employee's file.

4.2. Reporting of Security Incidents

A security incident is defined as an event which results, or may result in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.[x]

Employees and all other users shall immediately report all actual or suspected security incidents to their Division Chief and the appropriate ISO. The ISO will promptly notify the CISO of the actual or suspected security incident. The CISO shall report any security incidents that affect critical systems and/or that could be propagated to other state systems outside the OAG to DIR within twenty-four hours.[xi]

4.3. Computer Security Incident Response Team (CSIRT)

The OAG Computer Security Incident Response Team (CSIRT) is responsible for the detection, triage, response, communication and management of all information security incidents. The CSIRT will:

- Provide a single point of contact at OAG for managing all reported OAG information resource electronic attacks, whether suspected or actual;
- Identify and analyze what has occurred, including impact and threat;
- Research and recommend solutions and mitigation strategies;
- Share response options, recommendations, incident information and lessons learned with appropriate entities; and
- Coordinate response efforts.

The CSIRT is comprised of three separate groups that include both permanent IT personnel certified in CSIRT operations, and ad hoc personnel based on the nature of the incident:

- Management Group:
  - Membership includes: CISO and the affected division's ISO and IT Director.
  - May include: IRM.
  - Responsibilities: Manage CSIRT operations (CISO), manage overall incident response, document activities, and produce appropriate reports. Also responsible to communicate internally to executive management.
- Technology Group:
  - Membership includes: Director of impacted network and Director of impacted infrastructure and/or application.
  - May include subject matter experts (SMEs) from specific disciplines.
  - Responsibilities: Analyze event, recommend possible courses of action, and coordinate selected response.
- Legal Group:
  - Membership includes: Attorney(s) from, or assigned by, the General Counsel Division, and the Records Management Officer.
  - May include: Law enforcement investigators.
  - Responsibilities: Produce draft of external communications; function as team's legal representative for guidance regarding evidence gathering and other possible legal issues and activities.

4.4. Information Security Violations

Violations of information security policy could result in a security breach. For this reason, violations of information security policy will be investigated by the appropriate IT personnel. If the violation is found to be deliberate in nature, an official Information Security Violation Report (ISVR) will be issued by the CISO, with an informational copy provided to the Records Management Officer. Additionally, such violations will be reported to the employee's Division Chief and the Human Resources Director for corrective action. Any corrective action involving

use of information technology resources must be documented and reviewed by the appropriate ISO and/or the CISO prior to implementation.

4.5. Acceptable Use of OAG Information Resources

State information resources will be used primarily for official State purposes. Software for browsing the Internet is provided to authorized users to conduct official State business. Compliance with this policy will be electronically monitored. Any personal use must be in accordance with the OAG's policy regarding the Unauthorized Use of Government Time, Property, Services, and Facilities.

Violations may result in disciplinary action, up to and including termination of employment. The unauthorized use of OAG Information Resources will be considered as a relevant factor in evaluating the performance of OAG employees.

4.6. Access to OAG Information Systems and Assets

Access to OAG information technology assets must be strictly controlled and monitored to provide users with only the minimum level of system access necessary to allow them to perform assigned business tasks. When access by the user requires the use of a password, or other security measure, those security measures must be kept confidential by the intended user. Remote access to OAG information systems and assets must be accomplished only through the use of an OAG-approved remote access software application.

4.7. User Identification

Except for public users of systems where such access is authorized by the CISO or other appropriate IT personnel, each system user shall be assigned a unique personal identifier or user identification (User ID) to allow system access.

4.8. Personal Software, Hardware and Modems

Personal software may not be loaded onto any OAG computer, nor may personally-owned hardware, including modems and wireless routers, be connected to OAG information systems. Any hardware or software required for a business purpose of the agency must be approved for use by the CISO and must be obtained through the appropriate ITS Division.

4.9. Security Awareness Program

The OAG will provide an ongoing Information Security Awareness training program to educate employees and all other personnel with access to OAG data and information systems about data security and the protection of OAG information resources. This training will include the establishment of security awareness and familiarization with OAG security policies and procedures through both New Employee Orientation and ongoing refresher training.

4.10. Warning Statements

System identification screens will be provided at the time of initial logon to the mainframe or LAN/WAN. These screens will provide the following warning statements:

- Unauthorized use is prohibited.

- Usage may be subject to security testing and monitoring.
- Misuse may be subject to disciplinary action.
- No expectation of privacy is to be anticipated by the user.

4.11. Termination of Employment

Computer user identifications (User ID's) for employees that have voluntarily terminated employment with the OAG must be removed from the computer system immediately following termination. For involuntary terminations, the ID should be removed prior to, or at the same time the employee is notified of the termination in order to protect OAG data and information resources.

4.12. Automatic Suspension / Deletion of User ID's

Mainframe, LAN and Remote Access User ID's will be monitored for usage to protect system security, and any unused user ID's will be subject to automatic suspension after 30 days, and deletion after 60 days without notice to the user, unless an exception has been approved in accordance with this policy.

4.13. Positions of Special Trust

The CISO will establish procedures for reviewing information resource functions to determine which positions require special trust or responsibilities. These include, but are not limited to:

- Network and system administrators;
- Users with access to information systems that process or contain federal tax information;
- Users with access to child support systems and data that may include federal tax information;
- Users with access to financial and accounting systems or networks;
- Any user with agency-wide access to data and information systems; and
- Any user required to undergo a background check as a prerequisite to employment or grant of system access.

5. Technical Security Controls

5.1. System Security Policy

The following policies cover specific issues as they relate to the security of information systems and data within the OAG, and are governed by the procedures outlined in the OAG Information Security Procedures Manual.

5.2. System Administrators

System administrators are responsible for adding, removing or modifying user accounts as employees change roles within the agency. This activity must be accomplished in a timely manner to ensure only authorized personnel have access to OAG systems and information. Changes to user accounts may be subject to independent audit review.

5.3. System Developers

All production software development and software maintenance activities performed by in-house staff must adhere to agency security policies, standards, procedures, and other systems development conventions including appropriate testing, training and documentation.

5.4. Information Asset Protection

OAG data and information technology assets will be protected from unauthorized access, use, modification or destruction through the deployment of protective measures. The design, acquisition and use of all protective measures must be reviewed with the appropriate ISO and approved by the CISO.

5.5. Vendor Access to OAG Systems

Access to OAG systems and data by vendors (including contractors, sub-contractors, auditors, consultants or agents) must be appropriately controlled depending on the work to be performed, sensitivity levels of the data involved, work location, and other relevant considerations. All requests for vendor access must be coordinated with and approved by the appropriate IT department and CISO prior to access being granted.

5.6. Classification of Electronic Data and Assets

OAG electronic data and the information technology assets used to process, transmit, and store it should be assigned an appropriate classification level to assist in the proper safeguarding of the data. As higher classification levels require the agency to incur greater costs in order to safeguard data, care should be taken to accurately classify assets. Assets of varying classifications that are co-mingled in a single database or file system shall be classified at the highest level of the information contained in the data.

For the limited purposes of this policy, the OAG has two classifications of electronic data:

- **CONFIDENTIAL AND SENSITIVE** - This classification includes data that may be deemed confidential or protected by Texas or federal laws and/or administrative rules, and sensitive information, which if subject to a security breach, could compromise the agency's business functions or the privacy or security of agency employees, clients, or partners. Information in this category may only be provided to external parties in accordance with OAG policies and procedures.

- **UNCLASSIFIED** - This refers to all data that does not meet the requirements for CONFIDENTIAL AND SENSITIVE as described herein, as designated by the originating source of the data and/or the originator of any derivative data with guidance from 1 TAC § 202.1(3); DIR Classification Guidance, and any other applicable regulation or law.

- The default classification for all electronic data is CONFIDENTIAL AND SENSITIVE.

5.7. Data Destruction

OAG data should only be destroyed in accordance with the applicable records retention schedule, or upon the receipt of proper authorization from the State Library and Archives Commission. OAG data contained on magnetic or optical media must be removed from the media prior to the media being transferred out of the control of the authorized user, or the media must be physically destroyed in accordance with the appropriate document destruction guidelines applicable to that information.

5.8. Configuration Management

Configuration management (CM) is the process of managing the effects of changes or differences in configurations of an information system or network through the implementation of strict protocols and testing in order to reduce the risk of changes resulting in a compromise to data security, confidentiality, integrity, or availability. All systems will be configured and maintained only in accordance with approved IT and Information Security configuration management (CM) guidelines.

5.9. Change Management

Change management refers to the safeguards and procedures established for making modifications to OAG systems and networks. All such modifications must be processed through the appropriate change control procedure, with any OAG systems residing at a Consolidated Data Center (CDC) additionally being subject to the DIR and its contractor change management process.

5.10. Data Integrity

Data integrity refers to ensuring that data remains complete and unchanged during the course of any electronic processing, transfer, storage, or retrieval. To promote data integrity, individual users of OAG information resources must follow data integrity procedures applicable to their level of user access to OAG data, and take adequate precautions to safeguard against the loss of OAG data, including but not limited to:

- Performing regular backups of OAG data as may be appropriate;
- Taking physical and procedural safeguards to avoid the accidental loss, destruction or unauthorized modification of OAG data;
- Ensuring proper and routine use of virus protection software/anti-malware; and
- Coordinating with and seeking assistance from IT personnel as may be appropriate to safeguard OAG data.

5.11. Voice/Phone Mail

The OAG's voice or phone mail systems use agency information resources. Accordingly, each user is responsible for ensuring that use of these services is in compliance with applicable law, policy and procedures. All requests for changes, modifications, or termination of voicemail services must be initiated through the ITS Division.

5.12. E-Mail

Electronic mail (e-mail) is a form of communication that uses agency information resources. All use of e-mail must be in accordance with OAG policies and procedures regarding the use of information resources.

Upon the OAG's implementation of an agency-approved email encryption process, employees may not send CONFIDENTIAL AND SENSITIVE OAG data in the body of an email or as an email attachment across unsecured connections such as the Internet, unless it is encrypted using a process approved by ITS Division and the CISO.

5.13. Wireless Systems

Wireless networks or routers may not be used without the prior authorization of the IRM and the CISO. All wireless connectivity (Wi-Fi) to OAG networks must be in accordance with current IT architectural direction, the Information Security Policy, and OAG policies and procedures relating to the use of mobile telecommunications devices.

5.14. Copyright

Generally, the reproduction of copyrighted information is a violation of federal law. Therefore, OAG information resources should not be used to reproduce copyrighted information. Unauthorized copies of software shall not be loaded or executed on OAG information technology assets. Regular audits will be conducted to search for unauthorized software installed on machines.

5.15. Personal Software, Shareware and Freeware

Personal software, shareware and freeware may not be loaded or otherwise used on OAG systems unless there is a business necessity for the use of such programs, and their installation and use is specifically approved by the IRM and the CISO.

5.16. Data Encryption

All OAG laptops must have encrypted hard drives to safeguard data in the event the device is lost or stolen. Those divisions who choose to employ data encryption for transmission or storage of CONFIDENTIAL AND SENSITIVE data shall adopt the 256 bit Advanced Encryption Standard (AES), or 128 bit Single Sockets Layer (SSL/TLS) as a minimum. No encryption will be used without the prior approval of the IRM and the CISO.

5.17. Portable and Mobile Devices

All laptops and other mobile telecommunications devices (PDAs, Network capable Cell Phones, BlackBerry's, etc.) must be approved for use and supplied by the appropriate ITS Division. Only OAG laptops installed with full-disk encryption, anti-malware safeguards, and secure connectivity are authorized for use with OAG data and networks.

5.18. Malware Protection Software

All workstations and laptops must use approved malware protection software and configurations, regardless of whether they are connected to OAG networks or are used as a standalone device. Additionally, each file server attached to the OAG network and each e-mail gateway must utilize

OAG IT-approved e-mail malware protection software and/or hardware. Users shall not alter, disable, bypass, or adjust any settings or configurations for OAG malware protection software in any manner.

5.19. Intrusion Detection

Intrusion detection techniques will be deployed wherever possible in order to safeguard against unauthorized attempts to access, manipulate, or disable OAG networks. Intrusion detection activities may be conducted only by specially-trained personnel within the OAG's Information Security Division using techniques approved by the CISO.

5.20. Internal Electronic Investigations

All internal electronic investigations must be authorized by, and conducted under the supervision of, the CISO unless otherwise approved by the First Assistant Attorney General. No other investigation is authorized on OAG systems or networks. Any unauthorized electronic investigation or monitoring discovered on OAG systems or networks will be reviewed by the Information Security Division and may result in disciplinary action up to and including termination of employment.

5.21. Screen Savers

To reduce the likelihood of unauthorized access to OAG data, systems and networks, all OAG workstations, including laptop computers, must be configured to activate password-protected screensavers after no more than fifteen minutes of user inactivity. An employee should not leave his or her workstation unless the password-protected screensaver has been activated or, if possible, the workstation has been secured by a locked door.

5.22. User Passwords

Systems that use passwords shall follow the standards on password usage prescribed by DIR. This document specifies minimum criteria and provides guidance for selecting additional password security criteria. Disclosure of an individual's password or use of an unauthorized password or access device may result in disciplinary action up to and including termination of employment.

5.23. Administrator Passwords

All system administrators will maintain and use both a standard user password and a system administrator password ("super user" password). The system administrator password will be used only for system administrator activities. All common applications and system activities (email, calendar, etc.) must be accessed by the system administrator only with their standard user password.

5.24. System Log On & Re-Boot

All OAG workstations, including laptop computers, must be connected to the OAG network at least once weekly in order to receive appropriate application updates and security patches. Additionally, all systems must be re-booted (shut down and restarted) at least once a week to ensure these updates and patches are installed appropriately.

5.25. System Settings

All OAG systems are specifically configured to ensure that users have the appropriate ability to perform assigned tasks. Users shall not modify, change or attempt to change any system settings. If additional user access, permissions or system setting changes are required, then a request for the modification must be approved by the user's manager and submitted to the appropriate IT Division for handling.

5.26. Control of Peripherals

A peripheral device is any device attached to a computer in order to expand its functionality, such as USB flash drives, CD burners, or PCMCIA card slots. The ability to use peripheral devices may be controlled on some OAG systems; users are not authorized and should not attempt to change control settings in order to use peripheral devices on these systems. Adding or deleting peripherals on these systems may only be accomplished by IT personnel.

5.27. Security Breaches

A security breach is defined as any event which results in loss, disclosure, unauthorized modification, or destruction of information resources. Users shall immediately report all actual or suspected security breaches to their Division Chief and the ISO responsible for their division. The responsible ISO will promptly report the suspected or actual security breach to the CISO. Depending on the nature of the information involved, additional procedures may be required in accordance with the Sensitive Personal Information Privacy Policy.

5.28. Dial-up Access

For dial-up access to OAG systems other than access authorized for the public, information security protocols shall be employed to positively and uniquely identify authorized users and authenticate user access to the requested system. All modems used for dial-up access to OAG systems must be authorized by the IRM and CISO.

5.29. Purchasing/Development Pre-Approval

All OAG purchases, acquisitions, or developments of information technology services, equipment or software must be reviewed and pre-approved by the appropriate ISO, and the IRM, in consultation with the CISO, to determine whether the purchase may negatively impact OAG information technology security. All purchases of information technology security products, or products with information technology security functionality or impact, must be approved by the IRM and either the A&L and/or CS ISO or CISO prior to the issuance of a purchase order.

5.30. Contract Security Provisions

All third-party contracts must contain appropriate language to ensure the security of OAG information to which the third-party may have access, even if such access is limited to encrypted data. This language must state in clear and unambiguous terms the security requirements placed on the third-party involved, and their responsibilities for security under the contract. It must also clearly state OAG's authority to audit their security procedures for appropriateness during the length of the contract.[xii]

All contracts to which the OAG is a party and that affect OAG information technology security must be reviewed and approved by the CISO prior to execution in order to ensure that appropriate security controls are included.

5.31. System Development, Acquisition and Testing

Data and network security requirements must be considered and addressed in all phases of the development or acquisition of new information processing systems. Before being placed into use, all new systems must be properly tested in order to ensure compatibility with OAG information systems and the OAG computing environment. During system testing, test functions shall be kept either physically or logically separate from production functions in order to safeguard OAG data and information systems.

6. Exception, Waiver and Modification

6.1. Waivers and Exceptions

Waivers and exceptions to the existing information security policies and procedures are strongly discouraged because they may pose an unacceptable risk to protected OAG data and systems. Prior to implementation, all exceptions or waivers of existing security policies or procedures must be reviewed by appropriate information technology security and IT personnel, approved by the CISO, and reported to the Records Management Officer.

- A waiver is a variance of a control standard that is limited to a specific period of time and to a specific system in order to allow IT personnel to perform an approved change or modification to OAG systems.

- An exception is an indefinite variance from a control standard supported by a valid and ongoing business justification.

6.2. Modification or Significant Changes to Procedures

All changes in the procedures to protect OAG IT systems and data must be reviewed by appropriate IT personnel and approved by the A&L ISO and/or CS ISO as appropriate and the CISO prior to implementation. If immediate changes to procedures are required to meet an emergency situation, A&L and/or CS ISO, CISO and the Records Management Officer must be informed as soon as possible thereafter.

6.3. Executive Management Waiver

Not withstanding any provisions to the contrary contained herein, waivers, exceptions and modifications to the information security policies and procedures may be authorized in writing at the discretion of the First Assistant Attorney General.

7. Document Acceptance and Release Notice

This is Version **3.0** of the **OAG Information Security Technology Security Policy Manual.**

The OAG Information Security Technology Security Policy Manual is a managed document. Changes will be issued only as a complete replacement document. Recipients should remove superseded versions from circulation. This document is authorized for release after all signatures have been obtained.

Please submit all requests for changes to the owner/author of this document.

OWNER: _____DATE: February 12, 2009
Dr. Walt H. Foultz, Chief Information Security Officer

SPONSOR: _____DATE: February 12, 2009
Gary Buonacorsi, Information Resource Manager

8. References

[i] Tex. Gov't Code § 2054.003(7).

[ii] 1 TAC §202.20.

[iii] 1 TAC § 202.1

[iv] 1 TAC § 202.21.

[v] 1 TAC § 202.21.

[vi] 1 TAC § 202.21.

[vii] 1 TAC § 202.27.

[viii] *See generally*, 1 TAC Chapter 202.

[ix] 1 TAC § 202.21.

[x] 1 TAC § 202.1.

[xi] 1 TAC §202.26.

[xii] 1 TAC §202.25(6)(B).

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

Signature Request Form

Please route form in accordance with signature approval list below.

Date: February 12, 2009

Policy name: Information Technology Security Policy Manual

(Description of Attachment)
Security policy for all OAG "information resources" as such term is defined in Texas Government Code section 2054.003(7) that is used by or for the OAG, throughout its life cycle. This policy also applies to all users of OAG information assets and electronic data regardless of location.

Attachments: Information Technology Security Policy Manual (Version 3.0)

Prepared by ITS Division

Gary Bumgarner by email attached 2/12/09
Division Chief

February 12, 2009
Date

PLEASE FORWARD BY *DATE*

✓ Approved __Approved with Comments/Edits __Not Approved

Vers. 3.0 ✓

[signature]
General Counsel Division

2/12/09
Date

04142008 v3.0

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

PLEASE FORWARD BY *DATE*

✓Approved __Approved with Comments/Edits __Not Approved

Version 3.0

Jonathan F. Zuba
Deputy Attorney General for Legal Counsel

2/12/2009
Date

PLEASE FORWARD BY *DATE*

✓Approved __Approved with Comments/Edits __Not Approved

Deputy for Administration

2/13/09
Date

__Approved __Approved with Comments/Edits __Not Approved

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

First Assistant Attorney General

Date 2/13/09

STATEMENT OF RESPONSIBILITY

_____ Name

_____ Position

_____ Agency, Division, or Company

_____ Social Security Number

In general, all information that is used in or by the Office of the Attorney General is to be disseminated on a "need-to-know" basis. Confidential information is to be held in the strictest confidence and may not be disclosed except as provided in the Attorney General's disclosure policy. Sensitive information may only be created, modified, or deleted by authorized personnel. Special provisions must be made for the preservation of essential information.

Any computer system passwords I receive or devise are confidential. They are not to be disclosed to anyone! I am responsible for all computer transactions performed by my identification code (ID) which is authenticated by my password(s).

My failure to comply with the security policies of the agency may result in disciplinary action including termination of employment. Failure to observe the above conditions or any attempt to circumvent the computer security by using or attempting to use any transaction, software, files, resources, or password that I am not authorized to use may constitute a "breach of computer security" as defined in the TEXAS PENAL CODE, CHAPTER 33, Section 33.02, and that such an offense is a Class A Misdemeanor. Similar federal statutes may also be applicable.

Copyrighted material, including but not limited to commercial computer software, which maybe made available to me for use by the Office of the Attorney General is protected by copyright laws and is not to be copied for any reason without written permission from the owner of the copyright.

(Continued on next page)
This document is not part of the preceding policy document but is required by that policy document to be signed and placed in your employee records. Signature lines appear on the next page.

State-owned information resources, including but not limited to data processing and related equipment, but not including telephones (covered under separate policy), are to be used only for official state purposes. I will not review or modify information that is outside the scope of my current job assignment.

The use or installation of any software or hardware not owned by the Office of the Attorney General is expressly forbidden unless explicitly authorized in writing. In the event that authorization is granted, installation of such software or the connection of such hardware is to be performed by authorized employees of the Office of the Attorney General.

By signing this statement I certify that I

- agree to abide by all written conditions imposed by the Office of the Attorney General as regards information security;
- understand my above-mentioned responsibilities;
- have received information security training; and
- have received, read, and understood the Employee's Information Security Manual.

SIGNATURE _____ DATE_____

NOTICE: The user statement of responsibilities form is not the beginning of a negotiation with the user. It is a statement by the user that he/she has been trained and therefore understands his/her responsibilities in the protection of OAG information assets. This form is **not** modifiable by the user. Any modifications by the user, other than providing the requested information, shall make the form null and void and shall be cause to discontinue said employees access to OAG information assets.

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

Statement

OFFICE OF THE ATTORNEY GENERAL: AUTOMATED COMPUTER SYSTEM ACCESS STATEMENT OF RESPONSIBILITY

General Information:

All information maintained in the files and records of the Child Support Division are privileged and confidential. The unauthorized use or release of the information can result in criminal prosecution and civil liability. Only authorized personnel may add, modify and/or delete information.

Statements:

I understand that the information concerning any person, customer or client that may come to my knowledge while using the computer system of the TxCSDU or TXCSES or any other OAG computer shall be held in strictest confidence and may not be disclosed except as used exclusively for purposes directly connected with the administration of programs under Title IV-A, IV-D and XIX of the federal Social Security Act and the OAG Confidentiality Policy and Procedures.

Notwithstanding the above, I understand that I may not disclose to any individual or agency any federal tax return or return information. I further understand that it is unlawful to offer or receive anything of value in exchange for federal tax return or return information. Such unauthorized disclosure or exchange is punishable by fine up to $5,000, or imprisonment up to 5 years, or both, under Internal Revenue Code 7213 and 7213 A. Accessing federal tax information without a "need to know" is a federal misdemeanor punishable by not more than one year imprisonment, or a $1000 fine or both, plus costs of prosecution. under 7213 A, Internal Revenue Code. I also understand that I may be civilly liable for damages of not less than $1000 per violation, together with costs of prosecution under Section 7431 of the Internal Revenue Code.

I also understand that I may not release information to any committee or legislative body (federal, state, or local) that identifies by name or address any such applicant or recipient of services. Use of such information by a local government or component thereof for any other purpose, including but not limited to, collecting a fee is prohibited.

I understand that I may not perform any work, review, update or otherwise act to obtain information upon my own, or any relative's, friend's, or business associate's child support case, regardless if the case is open or closed. My failure to comply with the OAG Confidentiality Policy will result in immediate termination of my computer access. I also understand that a violation will be reported to my supervisor or other appropriate personnel in my agency for disciplinary action, which may include termination and/or referral for prosecution.

In addition, if applicable, I understand that the computer password(s) I receive or devise is confidential, and must not be disclosed to anyone. I understand that it is my responsibility to safeguard such password(s) by not allowing it to be viewed by anyone. I understand that I am responsible for computer transactions performed through misuse of my password(s).

I agree I will not load unauthorized software, personal computer programs, shareware or freeware of any kind onto the OAG computer equipment without the express written approval of the Office of the Attorney General, Information Resource Manager or designee, or the contract manager or designee. I understand that use of a password not issued or devised specifically for me is expressly prohibited and is a violation of state and federal law.

I also understand that failure to observe the above conditions may constitute a "breach of computer security" as defined in the TEXAS PENAL CODE, CHAPTER 33, Section 33.02 (b), and that such an offense may be classified as a felony. Similar federal statutes may also be applicable.

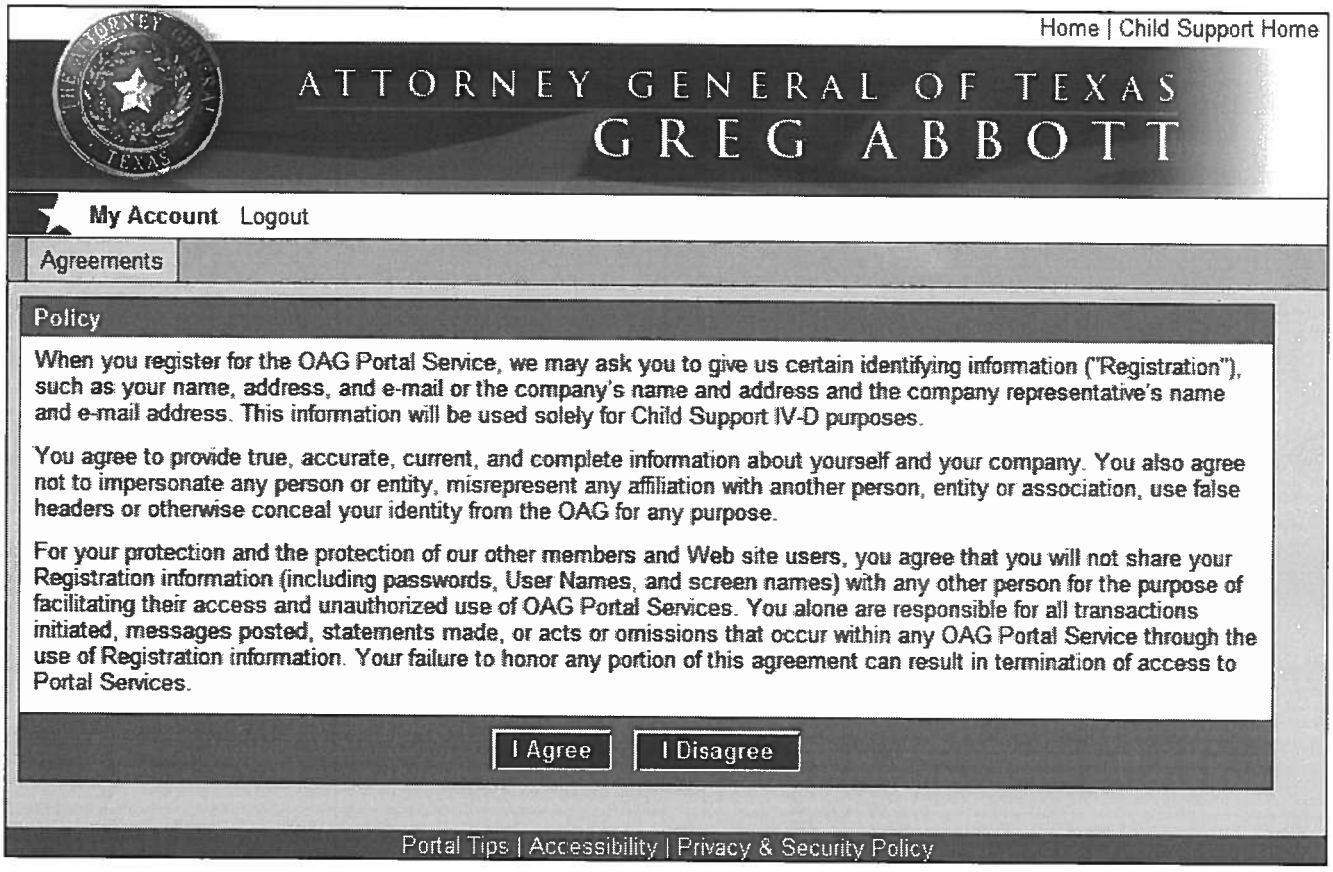
I certify that I understand that any copyrighted material, including but not limited to commercial computer software, which may be made available to me for use by the OAG is protected by copyright laws and is not to be copied for any reason without written permission from the owner of the copyright and the OAG.

By agreeing to this statement I certify that I:

- agree to abide by all written conditions imposed by the OAG regarding information security;
- understand my responsibilities as described above;
- have received, read and understand the OAG security information policy manual; and
- if applicable, I have read all applicable software licenses and agree to abide by all restrictions.

I Agree | I Disagree

ATTACHMENT C



ATTACHMENT D

Data Integrity Procedures Changes to Case Information

Before updating member/ case information, such as home address, phone number, etc., verify the caller's identity. Ask the caller for the following identifiers:

- Name
- Date of Birth
- Home address

If there is any doubt about the caller's identity after these identifier's have been obtained, ask for the children names and date of birth.

When pertinent information is unavailable on registry-only (RO) cases, county staff are prevented from verifying a caller's identity. Once all attempts to verify the caller's identity have been exhausted, instruct the caller to take one of the following actions in order to have the member/case information updated on TXCSESWeb:

- **Mail:**
- a copy of a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county address

- **FAX:**
- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county FAX number

- **E-mail the information** to be updated with a scanned copy of the proof/verification information to be updated (ie., home address, SSN card, drivers license, etc.) to the county email address

- **In Person (District Clerk Office or Domestic Relations Office):**
- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)

- **Visit the local child support office** that is assigned to work the RO case and provide:
- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)

ATTACHMENT E

CERTIFICATION REGARDING LOBBYING
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES
FORM F

PROGRAM: CHILD SUPPORT ENFORCEMENT PROGRAM PURSUANT TO TITLE IV-D OF THE SOCIAL SECURITY ACT OF 1935 AS ADMINISTERED BY THE OFFICE OF THE ATTORNEY GENERAL OF TEXAS

PERIOD: September 1, 2010 to August 31, 2012

Certification for Contracts, Grants, Loans and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid by, or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an office or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub grants, and contracts under grants, loans, and cooperative agreements) and that all sub recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

_____ _____

Signature Date

_____

Title

_____

Organization

ATTACHMENT F

United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information

#.1. PERFORMANCE

#.1.1. In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

#.1.2. All work will be done under the supervision of the contractor or the contractor's employees.

#.1.3. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

#.1.4. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

#.1.5. The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

#.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

#.1.7. All computer systems processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

#.1.8. No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

#.1.9. The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

#.1.10. The agency will have the right to void the contract if the contractor fails to provide the safeguards described above. (NOTE TO DRAFTER: Include any additional safeguards that may be appropriate.)

#.2. CRIMINAL/CIVIL SANCTIONS

#.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

#.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

#.2.3. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information

#.3. INSPECTION

#.3.1. The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

ATTACHMENT G

_____ COUNTY

INCIDENT RESPONSE PLAN

Adopted _____, 2010

_____ County
Incident Response Plan

Overview

Pursuant to the 2009 SCR/LCS Contract # _____, § 6.4.1.1, this Incident Response Plan is designed to provide a general guidance to county staff, both technical and managerial, to:

- enable quick and efficient recovery in the event of security incidents which may threaten the confidentiality of OAG Data;
- respond in a systematic manner to incidents and carry out all necessary steps to handle an incident;
- prevent or minimize disruption of mission-critical services; and,
- minimize loss or theft of confidential data.

The plan identifies and describes the roles and responsibilities of the Incident Response Team and outlines steps to take upon discovery of unauthorized access to confidential data. The Incident Response Team is responsible for putting the Plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to any threat to confidential data. The Team's mission is to prevent a serious loss of information assets or public confidence by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Team is responsible for investigating suspected security incidents in a timely manner and reporting findings to management and the appropriate authorities as appropriate.

Incident Response Team Roles and Responsibilities

Position	Roles and Responsibilities
Chief Information Security Officer (CISO)	• Immediately report incident directly to OAG CISO and OAG Contract Manager • Determine nature and scope of the incident • Contact members of the Incident Response Team • Determine which Team members play an active role in the investigation • Escalate to executive management as appropriate • Contact other departments as appropriate • Monitor and report progress of investigation to OAG CISO • Ensure evidence gathering and preservation is appropriate • Prepare and provide a written summary of the incident and corrective action taken to OAG CISO
Information Technology Operations Center	• Central point of contact for all computer incidents • Notify CISO to activate Incident Response Team • Complete Incident Identification form (Attachment One) and Incident Survey (Attachment Two) and forward to County CISO
Information Privacy Office	• Document the types of personal information that may have been breached • Provide guidance throughout the investigation on issues relating to privacy of customer and employee personal information • Assist in developing appropriate communication to impacted parties • Assess the need to change privacy policies, procedures and/or practices as a result of the breach
Network Architecture	• Analyze network traffic for signs of external attack • Run tracing tool and event loggers • Look for signs of firewall breach • Contact external internet service provider for assistance as appropriate • Take necessary action to block traffic from suspected intruder • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Operating Systems Architecture	• Ensure all service packs and patches are current on mission-critical computers • Ensure backups are in place for all critical systems • Examine system logs of critical systems for unusual activity • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Business Applications	• Monitor business applications and services for signs of attack • Review audit logs of mission-critical servers for signs of suspicious activity • Contact the Information Technology Operations Center with any information relating to a suspected breach • Collect pertinent information regarding the incident at the request of the CISO
Internal Auditing	• Review systems to ensure compliance with information security policy and controls • Perform appropriate audit test work to ensure mission-critical systems are current with service packs and patches • Report any system control gaps to management for corrective action • Complete Incident Eradication Form (Attachment Four) and forward to County CISO

Incident Contact List

OAG Contact Information

Position	Name	Phone Number	Email address
OAG Chief of Information Security Officer	Walt Foultz	512-936-1320	walt.foultz@oag.state.tx.us
OAG SCR/LCS Contract Manager	Allen Broussard	512-460-6373	allen.broussard@cs.oag.state.tx.us

County Contact Information

Position	Name	Phone Number	Email address
Chief of Information Security Officer			
County SCR/LCS Contract Manager			
Information Technology Operations Center			
Information Privacy Office			
Network Architecture			
Operating Systems Architecture			
Business Applications			
Internal Auditing			

Incident Identification

Date Updated: _____

General Information

Incident Detector's Information:

Name: _____
Title: _____
Phone: _____
Email: _____
Detector's Signature: _____

Date and Time Detected: _____
_____
Location Incident Detected From: _____
_____
Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other _____
- Probe
- Hoax

Incident Location: _____

Site: _____

Site Point Of Contact: _____ _____

Phone: _____ _____

Email: _____

How was the Intellectual Property Detected: _____

_____

_____

_____

_____

_____

Additional Information: _____

_____

_____

_____

_____

Incident Survey

Date Updated: _____

Location(s) of affected systems: _____

Date and time incident handlers arrived at site: _____

Describe affected information system(s): _____

Is the affected system connected to a network? YES NO

Is the affected system connected to a modem? YES NO

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.):

Incident Containment

Date Updated: _____

Isolate Affected Systems:

CISO approved removal from network? YES NO

If YES, date and time systems were removed: _____

If NO, state reason: _____

_____

_____

Backup Affected Systems:

Successful backup for all systems? YES NO

Name of person(s) performing backup: _____

_____

Date and time backups started: _____

Date and time backups complete: _____

Incident Eradication

Date Updated: _____

Name of person(s) performing forensics on systems:

_____

_____

_____

_____

_____

_____

Was the vulnerability identified: YES NO

Describe: _____

_____

_____

_____

_____

_____

Office of the Attorney General – Child Support Division **ATTACHMENT H**

Certificate of Destruction for Contractors and Vendors

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Contact Name	Title	Company Name and Address	Phone

You may attach an inventory of the media if needed for bulk media disposition or destruction.

Media Type		Media Title / Document Name
☐ HARD COPY	☐ ELECTRONIC	
Media Description (Paper, Microfilm, Computer Media, Tapes, etc.)		
Dates of Records		

Document / Record Tracking Number	OAG Item Number	Make / Model	Serial Number

Item Sanitization						
	☐	CLEAR	Who Completed?		Who Verified?	
	☐	PURGE	Phone		Phone	
	☐	DESTROY	DATE Completed			
Sanitization Method and/or Product Used						
Final Disposition of Media	☐	Reused Internally		☐	Destruction / Disposal	
	☐	Reused Externally		☐	Returned to Manufacturer	
	☐	Other:				

Comments:

If any OAG Data is **retained**, indicate the type of storage media, physical locations(s), and any planned destruction date.

Description of OAG Data Retained and Retention Requirements:

Proposed method of destruction for OAG approval:		
	Type of storage media?	
	Physical location?	
	Planned destruction date?	

Within five (5) days of destruction or purging, provide the OAG with a signed statement containing the date of clearing, purging or destruction, description of OAG data cleared, purged or destroyed and the method(s) used.

Authorized approval has been received for the destruction of media identified above and have met all OAG Records Retention Schedule requirements including state, federal and/or internal audit requirements and are not pending any open records requests.

Records Destroyed by:		Records Destruction Verified by:	
Signature	Date	Signature	Date

Be sure to enter name and contact info for who completed the data destruction and who verified data destruction in the fields above.

Send the signed Certificate of Destruction to:

OAG: Child Support Division, Information Security Office, PO Box 12017, Austin, TX 78711-2017

Office of the Attorney General – Child Support Division
Certificate of Destruction for Contractors and Vendors

INSTRUCTIONS FOR CERTIFICATE OF DESTRUCTION

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

IRS Publication 1075 directs us to the FISMA requirements and NIST guidelines for sanitization and disposition of media used for federal tax information **(FTI).** These guidelines are also required for sensitive or confidential information that may include personally identifiable information **(PII)** or protected health information **(PHI).** NIST 800-88, Appendix A contains a matrix of media with minimum recommended sanitization techniques for clearing, purging, or destroying various media types. This appendix is to be used with the decision flow chart provided in NIST 800-88, Section 5.

There are two primary types of media in common use:

- **Hard Copy**. Hard copy media is physical representations of information. Paper printouts, printer and facsimile ribbons, drums, and platens are all examples of hard copy media.
- **Electronic (or soft copy).** Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in NIST SP 800-88, Appendix A.

1. For media being reused within your organization, use the **CLEAR** procedure for the appropriate type of media. Then validate the media is cleared and document the media status and disposition.

2. For media to be reused outside your organization or if leaving your organization for any reason, use the PURGE procedure for the appropriate type of media. Then validate the media is purged and document the media status and disposition. Note that some **PURGE** techniques such as degaussing will typically render the media (such as a hard drive) permanently unusable.

3. For media that will not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

4. For media that has been damaged (i.e. crashed drive) and can not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

5. If immediate purging of all data storage components is not possible, data remaining in any storage component will be protected to prevent unauthorized disclosures. Within twenty (20) business days of contract expiration or termination, provide OAG with a signed statement detailing the nature of OAG data retained type of storage media, physical location, planned destruction date, and the proposed methods of destruction for OAG approval.

6. Send the signed Certificate of Destruction to:

OAG: Child Support Division
Information Security Office
PO Box 12017
Austin, TX 78711-2017

FAX to: 512-460-6070

or send as an email attachment to:

Kathleen.Donaho-Jaeger@cs.oag.state.tx.us

Final Distribution of Certificate	Original to:	Kathleen Donaho-Jaeger, Information Security Officer 512-460-6021
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. CSD Contract Manager