Travis County Commissioners Court Agenda Request

Meeting Date: September 17, 2013
Prepared By/Phone Number: Sylvia Mendoza 512-854-7008
Elected/Appointed Official/Dept. Head: Estela P. Medina 854-7069
Commissioners Court Sponsor: Judge Biscoe

AGENDA LANGUAGE:
Consider and take appropriate action to approve the contract extension between the Office of Attorney General and the Travis County Domestic Relations Office for the Child Support Community Supervision services extended through February 28, 2014. The original contract date effective September 1, 2009 to August 31st 2013

BACKGROUND/SUMMARY OF REQUEST AND ATTACHMENTS:
The Travis County Domestic Relations Office has entered into a contract with the Office of Attorney General (OAG) to provide the OAG with community supervision services on Title IV-D cases for the purpose of enforcement of child support and medical support orders, a Title IV-D function.
The attached contract amendment one proposes to extend the currently expired contract through February 28, 2014.

STAFF RECOMMENDATIONS:
The Travis County Juvenile Probation Department respectfully recommends approval of the contract extension.

ISSUES AND OPPORTUNITIES:

FISCAL IMPACT AND SOURCE OF FUNDING:

REQUIRED AUTHORIZATIONS:

AGENDA REQUEST DEADLINE: All agenda requests and supporting materials must be submitted as a pdf to David Salazar at David.Salazar@co.travis.tx.us in the County Judge's office, by **Tuesdays at 5:00 p.m.** for the next week's meeting.

TRAVIS COUNTY JUVENILE PROBATION DEPARTMENT

2515 South Congress Avenue ~ Austin Texas 78704
Phone: (512)854-7000 Fax: (512)854-7097

ESTELA P. MEDINA
Chief Juvenile Probation Officer

TO: The Honorable Samuel T. Biscoe, County Judge
The Honorable Ron Davis, Commissioner Precinct 1
The Honorable Bruce Todd, Commissioner Precinct 2
The Honorable Gerald Daugherty, Commissioner, Precinct 3
The Honorable Margaret J. Gomez, Commissioner, Precinct 4

FROM: _____
Estela P. Medina
Chief Juvenile Probation Officer

RE: Approval of a contract between the Office of the Attorney General (OAG) and Travis County for Community Supervision Services through the Domestic Relations Office

DATE: September , 2013

Travis County Juvenile Probation Department respectfully requests that the attached contract extension for the existing Community Supervision Contract be placed before Commissioners Court for review and approval. Through this contract, the Domestic Relations Office supervises all OAG child support probationers in Travis County and is partially reimbursed for the costs of providing these services. The department is interested in continuing our partnership with the Office of the Attorney General. This contract amendment would extend the Contract with the Office of the Attorney General from September 1, 2009 through February 28, 2014.

The Domestic Relations Office has been supervising OAG child support probationers since 2005.

cc: Sylvia Mendoza
Scot Doyal
Chris Hubner

AMENDMENT ONE
TO
TRAVIS COUNTY
CONTRACT FOR SERVICES

Contract Number: 10-C0028

1.0 PURPOSE

The Office of the Attorney General ("OAG") and Travis County of the State of Texas ("County") do hereby agree to amend their original Agreement as executed initially effective September 1, 2009 to extend the termination date from August 31, 2013 to February 28, 2014.

2.0 AMENDMENT TO EXTEND TERMINATION DATE FROM AUGUST 31, 2013 TO FEBRUARY 28, 2014.

Effective August 30, 2013, Section 2.1 of the Agreement is revised to read as follows (deleted text is in strikethrough font; new text is in italics):

The Contract becomes effective on September 1, 2009 and ends on *February 28, 2014* ~~August 31, 2010 (the "initial term"). The contract shall be automatically renewed for three (3) one (1) year terms with the first one (1) year renewal term beginning on September 1, 2010, unless one party notifies the other in writing of its intention to not renew this Contract. Such renewal shall be subject to all specifications and terms and conditions of this Contract, with the sole and limited exception that the original date of termination may be extended pursuant to this provision. The parties agrees to be bound, for the initial term of the Contract and for any and all renewal terms which the OAG may elect to exercise, by the terms of this Agreement, including the County performance of the within described services at the rates specified herein.~~

3.0 ORIGINAL AGREEMENT

By the signing of this amendment, the parties hereto understand and agree that this amendment is hereby made a part of the Agreement identified in Section 1 of this amendment as though the amendment were set forth word for word therein.

Office of the Attorney General (OAG)	Travis County (County)
_____	_____
Name: Alicia G. Key	Name: The Honorable Samuel T. Biscoe
Title: Deputy Attorney General for Child Support	Title: County Judge, Travis County
Date: _____	Date: _____

State of Texas
CONTRACT FOR SERVICES

Contract Number: 10-C0028

1. INTRODUCTION

1.1. This Contract is entered into, by and between the Office of the Attorney General ("OAG") and Travis County ("County").

1.2. This Contract is authorized by Section 231.002 of the Texas Family Code.

1.3. The OAG and the County have entered into this Contract to provide the OAG with Community Supervision services on Title IV-D cases for the purpose of enforcement of child support and medical support orders, a Title IV-D function.

1.4. Definitions

1.4.1. Respondent. Non custodial persons in active IV-D full service cases who have been ordered by the Court to participate in the County Community Supervision program.

1.4.2. OAG Computer System. The Texas Child Support Enforcement System (TXCSES), a federally certified case management system for the IV-D program.

1.4.3. Allowable Cost. The actual amount of costs incurred that qualify for reimbursement under the federal financial participation provisions of Part D, Title IV of the federal Social Security Act (45 U.S.C. §§ 651 *et seq.*) and the Office of Management and Budget Circular A-87, "Cost Principles for State and Local Governments", published by the Executive Office of the President of the United States of America.

1.4.4. Case Status.

1.4.4.1. Reporting. Respondent has reported to the Community Supervision office according to the terms set forth in the order requiring Community Supervision.

1.4.4.2. Paying. Respondent has made a payment towards the court ordered monthly child support and/or medical support obligation.

1.4.5. Violation Report. The notification from the County to the OAG requesting revocation of Community Supervision for a specific Respondent and OAG child support case. Said notification shall specifically state each violation of the terms and conditions of Community Supervision.

1.4.6. Acceptable Activities. Specific activities performed by the County in an effort to collect child support and/or medical support for active cases in the Community Supervision caseload. Only activities deemed acceptable by the OAG will be considered for payment, as set forth in the Reimbursement Section below.

1.4.6.1. Intake Activities. The initial meeting with the Respondent following the rendition of the order requiring Community Supervision, including creation of the case file and establishment of reporting duties and expectations for the Respondent.

1.4.6.2. Respondent Report. All regularly scheduled and required reports from the Respondent according to the terms set forth in the order requiring Community Supervision, or in a manner deemed appropriate by the County Community Supervision Office.

1.4.6.3. Phone calls. Phone calls to or from the Respondent, and/or other individuals as appropriate, in an effort to collect court ordered child support and/or medical support.

1.4.6.4. Correspondence. Correspondence sent to the Respondent, and/or other individuals as appropriate, in an effort to collect court ordered child support and/or medical support.

1.4.6.5. Field Visits. Visits to the Respondent's home, place of business, or other location as deemed appropriate by the County Community Supervision Office, in an effort to collect court ordered child support and/or medical support.

1:4.6.6. Referral to other programs. Referral to other programs as deemed appropriate by the County Community Supervision Office designed to ensure the Respondent achieves and maintains a paying case status.

1.4.6.7. Violation Reports. Notification from the County Community Supervision Office to the appropriate OAG field office that the Respondent has not complied with the terms and conditions of the court ordered Community Supervision. Said notification may be in the form of an Affidavit, email, spreadsheet, or other forms as mutually agreed upon by the County and the OAG Regional Administrator and/or the OAG Senior Regional Attorney.

1.4.6.7.1. If no response has been received from the OAG regarding the initial Violation Report within ninety (90) days from the date of the first submittal, a second Violation Report may be submitted. The Second Violation Report shall be updated with all relevant information, shall be clearly identified as a Second Violation Report, and shall be forwarded to the OAG Senior Regional Attorney.

1.4.6.7.2. If no response has been received from the OAG regarding the Second Violation report with forty-five (45) days from the date of the second submittal, a third Violation Report may be submitted. The Third Violation Report shall be updated with all relevant information, shall be clearly identified as a Third Violation Report, and shall be forwarded via email or facsimile to:

Mara Friesen (or her successor in office)
Assistant Deputy Director for Field Legal Practice
Facsimile #: (512) 460-6733
Email Address: Mara.Friesen@cs.oag.state.tx.us.

1.4.6.8. Affidavit Preparation. Preparation of or review and signing of an affidavit requested by an OAG field office for a Motion to Revoke.

1.4.6.9. Court Activities. Preparation of case brief for revocation hearings and court appearances to testify or confer with the OAG, the Respondent, or the Court.

1.4.6.10. Locate Activities. Efforts by the County Community Supervision Office to locate a Respondent.

1.4.6.11. Classes. Any class or orientation meeting designed to enhance the collection of child support which the County Community Supervision Office requires a Respondent to attend.

1.4.6.12. Jail Review. Review by the County Community Supervision Office to determine a Respondent's incarceration release date.

1.4.6.13. Court Report. A written report filed with the court which advises the court that community supervision has been: (1) discharged because child support arrears have been paid in full, (2) terminated because the probationer is deceased, (3) terminated pursuant to the court's order, or (4) closed at the Office of the Attorney General's request.

1.4.6.14. Warrant/Capias Assistance. Assistance with the arrest of a Respondent in the community supervision office who has a warrant or capias pending due to a revocation request.

1.4.7. Active Caseload. All cases referred to the County for Community Supervision services, provided that the case is classified as "active full service" in the OAG computer system and that the case cannot be classified as Inactive pursuant to the Inactive Caseload Section below.

1.4.7.1. Maximum Active Caseload. The County shall maintain a maximum Active Caseload of no more than five hundred (500) Active Cases per month per full time employee whose job is in whole or in part assigned to specific County Community Supervision Office tasks. If the County exceeds the maximum allowable Active Caseload, the OAG will notify the OAG Regional Administrator and the OAG Senior Field Attorney to cease Community Supervision referrals until such time as the monthly Active Caseload falls below the maximum allowable Active Caseload.

1.4.8. Inactive Caseload.

1.4.8.1. All cases that are classified as "closed full service" cases and/or "registry only" cases in the OAG computer system.

1.4.8.2. All cases that are classified as "deferred full service" cases in the OAG computer system because the Respondent is incarcerated. Cases shall be included in the "Active" caseload in the month following the month the OAG computer system deferral is removed.

1.4.8.3. All cases in which the terms and conditions of Community Supervision, as set forth in the court order requiring Community Supervision, have been satisfied and supervision is no longer required by court order.

1.4.8.4. All cases in which a motion to revoke Respondent's Community Supervision has been filed. Cases shall be included in the "Active" caseload in the month following the month the Respondent's Community Supervision has been reinstated or the filing has been dismissed.

1.4.8.5. All cases in which the Respondent's Community Supervision has been revoked.

1.4.8.6. All cases in which the Respondent is deceased.

1.4.8.7. All cases in which the Respondent no longer resides in the State of Texas and has failed to make a payment for three consecutive months.

1.4.8.8. All cases in which the Court of Continuing Exclusive Jurisdiction has been transferred out of the County and the Respondent has failed to make a payment for three consecutive months or a new order has been rendered by the new Court of Continuing Exclusive Jurisdiction.

1.4.8.9. The County no longer has an obligation to provide monitoring and enforcement services as set forth in the County Obligations Section for cases classified as "Inactive".

1.5. Contract Provision Construction. This contract is the joint work product of the parties and in the event of any ambiguities no inferences shall be drawn for or against either party. The language used in this contract is deemed to be the language chosen by the parties hereto to express their mutual intent, and no rule of strict construction will be applied against any party, regardless of the actual author of the contract.

2. CONTRACT TERM

2.1. The Contract becomes effective on September 1, 2009 and ends on August 31, 2010 (the "initial term"). The contract shall be automatically renewed for three (3) one (1) year terms with the first one (1) year renewal term beginning on September 1, 2010, unless one party notifies the other in writing of its intention to not renew this Contract. Such renewal shall be subject to all specifications and terms and conditions of this Contract, with the sole and limited exception that the original date of termination may be extended pursuant to this provision. The parties agrees to be bound, for the initial term of the Contract and for any and all renewal terms which the OAG may elect to exercise, by the terms of this Agreement, including the County performance of the within described services at the rates specified herein.

2.2. Notice of Intent Concerning Non-Renewal and/or Renegotiation. In the event a party determines not to renew this Contract, said party shall notify the other party not later than June 1 concerning its intention to not renew the contract for the following year. No later than June 1, 2013, each party shall serve written notice to the other party concerning its intention to enter into or not enter into negotiations for a new Contract to take effect upon the expiration of this Contract.

3. REQUIREMENTS

3.1. County Obligations. At its sole discretion, the OAG will refer Respondents to the County Community Supervision program pursuant to this Contract. The County shall provide monitoring and enforcement services, as set forth below to maximize collection of child support and/or medical support obligations of Respondents.

3.1.1. The County shall provide monitoring and enforcement services for all Respondents in the County Community Supervision Active Caseload. The County shall monitor each Respondent in the Active Caseload as set forth in the table below. At the OAG's discretion and approval, the County may alter the monitoring schedule for a specific Respondent based on the individual circumstances of the Respondent.

3.1.1.1. The County shall maintain sufficient documentation of all Acceptable Activities performed on each case.

Case Status	Acceptable Activities
Intake	Intake activities as defined in the Definitions Section above
Paying	Document Status in Monthly Report
Not Paying	• Intake Activities • Respondent Report • Phone Call (incoming or outgoing) • Correspondence • Field Visit • Referral to Other Programs • First, Second and Third Violation Report • Affidavit Preparation • Court Activities • Locate Activities • Classes • Jail Review • Court Report • Warrant/Capias Assistance
Pending motion to revoke Community Supervision	• Affidavit Preparation • Court Activities • Court Report • Warrant/Capias Assistance
Closed IV-D Cases	• Court Report

3.1.1.2. If a respondent fails to make a child support payment for four (4) consecutive months from the Initial Intake date or the date of last payment, whichever occurs later, the County will be reimbursed for acceptable activities only if a violation report has been submitted on that case. If the County determines that a violation report is not appropriate for a specific case, the County may submit said case for reimbursement provided that the County performs an acceptable activity as set forth in the table above and provides the OAG with sufficient documentation to justify withholding the violation report.

3.1.2. Upon request of the OAG, the County shall provide to the OAG affidavits necessary to support a motion to revoke the Community Supervision of a Respondent. The County shall also ensure that County personnel are available to testify at, and to confer with OAG personnel in advance of and in preparation for, the hearing on the motion to revoke Community Supervision and to testify at any hearings, as necessary.

3.1.3. Standards and Business Rules. To ensure that all activities are IV-D monitoring and enforcement functions, the County, in coordination with the OAG Regional Administrator and/or the OAG Senior Regional Attorney, shall develop written standards and business rules for providing the Community Supervision services under this Contract. The document shall contain detailed procedures for fulfilling the County and OAG obligations, as set forth in the County Obligations Section and the OAG Obligations Section.

3.1.3.1. The County, working with the OAG Regional Administrator and/or Regional Senior Attorney, shall develop the written standards and business rules within two (2) months after the execution of this Contract, and shall submit to the OAG Contract Manager upon completion for approval. The OAG, working directly with the County, will review, revise and finalize the rules.

3.1.4. Performance Measures.

3.1.4.1. Minimum Performance Standards.

3.1.4.1.1. Monthly Collections Ratio. The County agrees that, at a minimum, it shall achieve a "collection-to-obligation" ratio of at least fifty-five percent (55%) for cases in the Active Caseload. The "collection-to-obligation" ratio shall be calculated monthly by dividing the sum total of the monthly court ordered child support and medical support collections for the Active Caseload by the sum total of the monthly child support and medical support obligations for the Active Caseload.

3.1.4.1.2. Annual Collections Ratio. The County agrees that, at a minimum, it shall achieve an annual average "collection-to-obligation" ratio of sixty-five percent (65%) for cases in the Active Caseload. The collection-to-obligation ratio shall be calculated by averaging the individual monthly collection ratios for the fiscal year.

3.1.4.2. Exceptional Performance Standards and Incentives. The County may qualify to receive monthly incentive payments of up to six dollars ($6.00) per Active Case for meeting or exceeding the Exceptional Performance Standards set forth in the table below. In order to qualify to receive an incentive payment, the County must:

- not be in an unsatisfactory performance status (see the Remedies for Non-Performance section below);
- meet the Exceptional Collections Standard of at least a seventy percent (70%) monthly collection-to-obligation ratio; and,
- achieve one or more of the three Exceptional Payment Consistency Standards.

INCENTIVE BONUS	EXCEPTIONAL COLLECTIONS STANDARD	EXCEPTIONAL PAYMENT CONSISTENCY STANDARD
First Increment: One Dollar ($1.00) per Active Case in the month reviewed	Achieve a "collection-to-obligation" ratio of at least seventy percent (70%) in the month reviewed	Forty percent (40%) or more of the Active Caseload received a payment towards the child support and/or medical support obligation for at least three (3) consecutive months, ending with the month reviewed
Increment Two: Two Dollars ($2.00) per Active Case in the month reviewed	Achieve a "collection-to-obligation" ratio of at least seventy percent (70%) in the month reviewed	Thirty-five percent (35%) or more of the Active Caseload received a payment towards the child support and/or medical support obligation for at least six (6) consecutive months, ending with the month reviewed
Increment Three: Three Dollars ($3.00) per Active Case in the month reviewed.	Achieve a "collection-to-obligation" ratio of at least seventy percent (70%) in the month reviewed	Thirty percent (30%) or more of the Active Caseload received a payment towards the child support and/or medical support obligation for at least nine (9) consecutive months, ending with the month reviewed

3.1.4.3. The OAG, at its discretion, may reduce or waive any performance standards and measurements.

3.1.5. Remedies for Non-Performance.

3.1.5.1. The OAG shall evaluate the County's performance against the performance measure outlined in the Performance Measure Section and other requirements of this Contract.

3.1.5.2. Failure by the County to meet the minimum performance measure for three (3) consecutive months in the Performance Measure Section or any of the requirements of this Contract may result in a finding of unsatisfactory performance. The OAG Contract Manager will communicate to the County in writing any finding of unsatisfactory performance.

3.1.5.3. If the OAG validates the finding of unsatisfactory performance, the County shall 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. Once the Corrective Action Plan is accepted by the OAG Contract Manager, the County shall implement the Plan.

3.1.5.4. If the County does not return to satisfactory status within forty-five (45) calendar days after approval of the corrective action plan, then the OAG may withhold payments due to the County under this Contract until the County is once again performing satisfactorily. If the County has not either returned to satisfactory status within sixty (60) calendar days after receiving notice that an unsatisfactory performance finding has been validated, or commenced corrective action and thereafter proceeded diligently to complete such correction, then the OAG may terminate this Contract (in accordance with the Termination of the Contract Section below) without payment to the County for any costs incurred by the County from the time that the OAG may have commenced withholding payments due to the County being in an unsatisfactory performance status. Where payments have been withheld and are to resume, due to the County 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.

3.2. OAG Obligations.

3.2.1. The OAG is solely responsible for obtaining the requisite court order that requires the Respondent to participate in the County Community Supervision program and for filing any subsequent motions to revoke or modify the Respondent's Community Supervision status.

3.2.2. For each case in the Active Caseload, the OAG will:

3.2.2.1. direct the Respondent to meet with the County upon conclusion of the court proceeding that requires the Respondent to participate in the County Community Supervision program in order to conduct the initial Intake Activities as set forth in the Definitions Section above

3.2.2.2. provide the County with a copy of the court order requiring the Respondent to participate in the County Community Supervision program

3.2.2.3. provide the County with a copy of any court orders which modify or terminate the terms and conditions of the Respondent's Community Supervision obligations

3.2.2.4. acknowledge receipt of affidavits provided by the County

3.2.2.5. notify the County whenever a motion to revoke, modify or terminate the terms and conditions of the Respondent's Community Supervision obligations has been filed

3.2.2.6. notify the County of scheduled dates and times of all hearings to revoke, modify or terminate the terms and conditions of the Respondent's Community Supervision obligations

3.2.2.7. notify the County of the results of all hearings to revoke, modify or terminate the terms and conditions of the Respondent's Community Supervision

3.2.3. The OAG will respond within a reasonable time to any County recommendations for revocation of a Respondent's Community Supervision. Responses will be in writing and will occur no later than 15 business days of the County's request. If no response is received by the County within 15 business days, the recommendation is deemed rejected.

3.2.4. The OAG will file requisite motions to modify or terminate the terms and conditions of Community Supervision for a Respondent if OAG case closure is warranted for any reason. Motions will be filed prior to case closure on the OAG's computer system.

3.2.4.1. The OAG will provide to designated County employees access to appropriate case and payment information residing on the OAG computer system. The OAG will work with the County to maintain any existing County access to the OAG computer system and will provide appropriate training to the designated County employees on its use. The County is responsible for obtaining the necessary hardware, software, internet service provider, and phone lines for the connection to the OAG computer system, and for all costs associated with obtaining and maintaining same said connection.

4. FINANCIAL MATTERS

4.1. Maximum Liability of the OAG. Notwithstanding any other provision of this Agreement, the maximum liability of the OAG for reimbursable expenses under the terms of this Agreement is One Million Six Hundred Ninety-Seven Thousand Two Hundred Forty-Eight Dollars ($1,697,248.00).

4.2. Reimbursement.

4.2.1. The OAG shall reimburse the County for the federal share of the County's Contract associated allowable costs subject to the limitations set forth in this Contract. Federal share means the portion of the County's Contract associated allowable costs that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purposes of reference only the federal share on the effective date of this Contract is sixty-six percent (66%). The Cost Principles for "State and Local Governments" as defined in OMB Circular A-87 shall apply to costs reimbursed under this Contract. The County and OAG agree that, for the purposes of this Contract, all of the County's Contract associated allowable costs for any given calendar month is equal to the caseload that was in existence on the last day of that month multiplied by a per case fee of Thirty-Eight Dollars ($38.00), provided that, for each case, an Acceptable Activity, as described in the County Obligations Section, was performed by the County during the calendar month.

4.2.2. Except as described in the County Obligations Section above, the OAG is not financially liable to the County for any work associated with "Inactive" cases.

4.2.3. The OAG shall be liable only for Contract associated costs incurred after the effective date of this Contract and before termination of this Contract.

4.2.4. The OAG may decline to reimburse Contract associated 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.

4.2.5. The 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 the County agree has resulted in an overpayment to the County, provided that such sums cannot be offset and deducted from any amount owing but unpaid to the County.

4.2.6. The County agrees that:

4.2.6.1. The reimbursement for the County's performance of its responsibilities under this Contract represents the only reimbursement that can be charged to the OAG;

4.2.6.2. No other reimbursement for tasks, functions or activities that are incidental or ancillary to the performance of the County's responsibilities under this Contract shall be sought from the OAG, nor shall the failure of the OAG to pay for such incidental or ancillary services and deliverables entitle the County to cease performing its responsibilities due under this Contract; and,

4.2.6.3. The County shall not be entitled to payment for any task required by this Contract unless and until it has been performed and/or delivered to the OAG in accordance with the terms of this Contract and no partial or progress payments shall be made except as mutually agreed upon by the County and the OAG.

4.2.7 Implementation of New Reporting Requirements

The OAG will reimburse County for certain implementation costs associated with the reporting requirements set forth in the Reporting Section below.

4.2.7.1 Implementation Cost Reimbursement

4.2.7.2 The OAG shall reimburse the County for costs incurred, up to five thousand dollars ($5,000), for system programming charges necessary to comply with the reporting requirements imposed by this contract. Prior to incurring any cost under this Subsection, County must have obtained OAG's written approval as to the reprogramming. County shall invoice the OAG for costs actually paid in the preceding month. The invoice must be submitted no later than two months after the month in which the County paid for the programming costs. The invoice must detail the programming time spent on the reporting requirement and the actual cost of same. The invoice shall have attached to it copies of bills paid by the County for the allowable programming. The invoice shall contain such additional information and documentation as the OAG may require and shall be submitted in the manner and/ or on the forms reasonably specified by the OAG. The invoice shall be submitted to the address set forth in the Reimbursement Process Section below. The OAG shall process a properly prepared invoice for payment in accordance with the State procedures for issuing state payments and the Texas Prompt Payment Act.

4.3. Reimbursement Process.

4.3.1. The OAG shall determine the monthly fee based on the number of Active Cases as of the last day of the calendar month to which the County has performed an Acceptable Activity during the calendar month and the results of the Exceptional Performance Review.

4.3.2. The OAG shall forward a Summary and Reimbursement Invoice to the County for review and approval.

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

Allen Broussard, Contract Manager, or his successor in office
Mail Code: 062
Office of the Attorney General
P.O. Box 12017
Austin, Texas 78711-2017

4.3.4. If the County does not approve the Summary and Reimbursement Invoice, it shall return the Invoice to the OAG within ten (10) County work days of receipt, detailing the basis of any disputed item along with supporting documentation. The OAG shall review the returned Invoice. If the dispute is resolved in the County's favor, the OAG shall make payment in the amount requested by the County. If the dispute is not resolved in the County's favor, the OAG shall make payment in accordance with the Invoice originally sent to the County and forward a letter of explanation to the County.

4.4. Audit and Investigation.

4.4.1. The County understands that acceptance of funds under this Contract acts as acceptance of the authority of the OAG, the State Auditor of Texas, the United States Department of Health and Human Services and the Comptroller General of the United States to conduct an audit or investigation in connection with those funds. The County agrees to cooperate fully in the conduct of the audit or investigation. The County shall grant access to all books, records and documents pertinent to this Contract to the OAG, the State Auditor of Texas, the United States Department of health and Human Services and the Comptroller General of the United States for the purposes of inspecting, auditing or copying such books, records and documents. The County shall ensure that the requirements of this provision including, but not limited to, the authority of the OAG, the State Auditor of Texas, the United States Department of Health and Human Services and the Comptroller General of the United States to conduct an audit or investigation concerning funds received indirectly by subcontractors through the County and the requirement to cooperate in the conduct of such audit or investigation shall in included in all subcontracts.

4.4.2. In order to comply with the monitoring and auditing requirements governing this Contract, the fiscal duty officer duly appointed by the County shall submit a Certification of Local Expenditures Report that certifies local expenditures made by the County for contract services for the period October through September of the fiscal year. This figure includes direct services in support of the program, allocated costs, and the costs of indirect services provided by the County in support of the contracted program. This Certification is due no later than six months following the fiscal year end of the County for which the expenditures are certified. Attachment Seven (7) is included as an example form.

4.5. Financial Terms.

4.5.1. Buy Texas. In accordance with §2155.4441, Texas Government Code, the County shall, in performing any services under this Contract, purchase products and materials produced in

Texas when they are available at a comparable price and in a comparable period of time to products and materials produced outside Texas.

4.5.2. Legislative Appropriations. 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 United States below). The OAG will not be in default for nonpayment under this Contract if such appropriated funds or federal funds are not available to the OAG for payment of the OAG's obligations under this Contract. In such event the OAG will promptly notify the County, and the Contract shall terminate (subject to the post termination responsibilities outlined in the Termination of the Contract Section) simultaneous with the termination of either appropriated funds or federal funds. Upon such occurrence, OAG shall discontinue payment hereunder.

4.5.3. Provision of Funding by the United States. 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 shall promptly notify the County of such fact in writing. Upon such occurrence, the OAG shall discontinue payment hereunder and the Contract shall be terminated subject to the post termination responsibilities outlined in the Termination of the Contract Section.

4.5.4. Antitrust and Assignment of Claims. – Pursuant to 15 U.S.C. §1, et seq., and Tex. Bus. & Comm. Code §15.01, et seq., the County affirms that it has not violated the Texas antitrust laws or federal antitrust laws and has not communicated its bid for this Contract directly or indirectly to any competitor or any other person engaged in such line of business. The 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. Controlled Correspondence. In order to track and document requests for decisions and/or information pertaining to this Contract, and the subsequent response to those requests, the OAG and the County shall use Controlled Correspondence. The OAG shall manage the Controlled Correspondence for this Contract. For each Controlled Correspondence document, the OAG shall assign a tracking number and the document shall be signed by the appropriate Party's Contract Manager. The Controlled Correspondence process may be used to document refinements and interpretations of the provisions of this Contract. Controlled Correspondence may also be used to document the cost impacts of proposed changes. However, Controlled Correspondence shall not be used to change pricing or alter the terms of this Contract. Controlled Correspondence shall not be the basis of a claim for equitable adjustment of pricing. Any changes that involve the pricing or the terms of this Contract must be by a Contract amendment. Controlled Correspondence documents shall be maintained by both Parties in on-going logs.

5.2. Notices

5.2.1. Written Notice Delivery. 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 (except as provided in the Discretionary Termination Section below). 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.

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

The Honorable Sam Briscoe (or successor in office)
Travis County Judge
PO Box 1748
Austin, TX 78767

with copies to (registered or certified mail with return receipt is not required for copies):

Cecelia Burke, Director (or successor in office)
Travis County Domestic Relations Office
PO Box 1495
Austin, TX 78767

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

Alicia Key (or successor in office)
Deputy Attorney General for Child Support
Office of the Attorney General
P.O. Box 12017 (Mail Code 033)
Austin, Texas 78711-2017

with copies to (registered or certified mail with return receipt is not required for copies):

Joe Fiore, Managing Attorney, or successor in office
Legal Counsel Section
P. O. Box 12017 (Mail Code 044)
Austin, Texas 78711-2017

5.3. Contract Managers. The County and the OAG shall designate Contract Managers for this Contract. The Contract Managers shall be the initial point of contact for all other matters. The Contract Managers shall be named in writing at the time of execution of this Contract. Subsequent changes in Contract Managers shall be communicated by the respective parties in writing per the notice procedures established by the Notices Section above.

5.4. Reporting. The County shall provide a monthly report to the OAG which shall include, for each Active Case:

- OAG Case Number
- Respondent Name
- Community Supervision Intake Date
- Community Supervision Expiration Date
- Last Payment Date (Month & Year)
- Reporting Type
- Reporting Status

- One Acceptable Activity performed in the preceding calendar month
- Violation Report Request Date

5.4.1. The report shall be submitted during the first ten (10) calendar days of each month. The report format and its implementation shall be as agreed upon by the County and the OAG. The County shall electronically transmit the required report.

5.4.2. The new reporting requirements in this contract must be in place and working within ninety (90) days after execution of this contract. The reimbursement process under Section 4.2 cannot be initiated until the OAG reports are in place and working.

5.5. Subcontracting. The County shall not subcontract any portion of the IV-D services to be performed under this Contract without the prior written approval of the OAG. All subcontracts, if any, entered into by the County shall be written and competitively advertised. Any subcontract entered into by the County shall be subject to the requirements of this Contract. The County agrees to be responsible to the OAG for the performance of any subcontractor and remains bound to perform the duties described in any subcontract regardless of whether the subcontractor breaches in its performance. The County understands and acknowledges that the OAG is in no manner liable to any subcontractor of the County.

5.6. Reporting Fraud, Waste or Abuse. The 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:

- the Contract Manager;
- the Deputy Director for Contract Operations, Child Support Division;
- the Director, Child Support Division;
- the Deputy Director, Child Support Division;
- the OAG Ethics Advisor;
- the Director of the OAG Office of Special Investigations;
- the OAG's Agency Integrity Program (AIP) Hotline (866-552-7937) or the AIP E-mailbox (AIP@oag.state.tx.us);
- the State Auditor's Office hotline for fraud (1-800-892-8348); or the Texas State Auditor's Special Investigation Unit, (512) 936-9500

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

- the specific suspected misconduct;
- the names of the individual(s)/entity(ies) involved;
- the date(s)/location(s) of the alleged activity(ies);
- the names and all available contact information (phone numbers, addresses) of possible witnesses or other individuals who may have relevant information; and,
- any documents which tend to support the allegations.

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

5.6.1.1.1. 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.

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

5.6.1.1.3. Abuse, being distinct from fraud, encompasses illegal acts or violations of policy or provisions of contracts or grant agreements. When abuse occurs, no law, regulation or provision of a contract or grant agreement is necessarily violated. Rather, the conduct of an individual falls short of behavior that is expected to be reasonable and necessary business practice by a prudent person. An example of abuse would be misuse of the power or authority of an individual's position.

5.7. Cooperation with the OAG. The County must ensure that it cooperates with the OAG and other state or federal administrative agencies, at no charge to the OAG, for purposes relating to the administration of this Contract. The County agrees to reasonably cooperate with and work with the OAG's contractors, subcontractors, and third party representatives as requested by the OAG.

5.8. Dispute Resolution Process for County Breach of Contract Claim.

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

5.8.2. A County 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.

5.8.3. 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 immediately preceding subsection.

5.8.4. 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.

5.8.5. 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.

5.8.6. 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.

6. CONFIDENTIALITY AND SECURITY PROVISIONS

6.1. General

6.1:1. Both the OAG and the 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.

6.1.2. The OAG recognizes that the 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). The OAG also recognizes that the 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.

6.1.3. Under this Contract, the County has view-only access to OAG computer systems.

6.1.4. The 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 the County by or on behalf of OAG, or (ii) which the County accesses from OAG systems in connection with provisions of the Contract Services. OAG Data does not include data and information originated by the County in the performance of its duties. Upon request by the OAG, the County shall execute and deliver any documents that may be necessary or desirable under any law to preserve or enable the OAG to enforce its rights with respect to OAG Data. Tex. Govt. 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.

6.1.5. 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.

6.1.6. The 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 the County's request, to access, use or disclose OAG Data, as well as any special conditions and limitations applicable to each authorization. The 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 monthly, the OAG shall send the County a list of users authorized to access the OAG computer system and the 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. The County shall notify the OAG of the authorized personnel that should have access rights to OAG Data and information in the method prescribed by the OAG. The County will immediately notify the OAG when an individual's access to OAG systems is no longer relevant. The OAG, in its sole discretion, may deny or revoke an individual's access to OAG Data and information and any of its systems.

6.1.7. The 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. The County shall certify to the OAG that such reviews have been conducted and that in the County's opinion the aforesaid employees are deemed trustworthy. The County may request the OAG

to perform such reviews. In such instances, the County shall provide the OAG with any required information, consent and authorization to perform the reviews and the OAG shall perform the reviews at its own expense.

6.1.8. All references to "Contract Services" shall include activities within the scope of this Contract.

6.1.9. The 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. 2-2007) and § 231.108 of the Texas Family Code, each as currently written or as may be amended, revised or enacted. The 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 One (1), 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 Contract Services on the County's behalf.

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

6.2. OAG Data Usage and Storage.

6.2.1. The County agrees to maintain physical security for OAG Data by maintaining an environment designed to prevent loss or unauthorized removal of data. The 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. The 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 Contract Services shall 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 Two (2)), signed the acknowledgment (and the 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 Three (3)), read and signed the IRS Information Notification Form (Attachment Four (4)), and any Agency-required Online Login Policy (Attachment Five (5)).

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 the 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.2-2007) and Attachment One (1) entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".

6.2.3. The 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 Contract. Without the OAG's approval (in its sole discretion), the County will not: (i) use OAG Data other than in connection with providing the Contract 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 Contract Services. However, nothing in this Contract is intended to restrict the 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 the County fails to comply with this subsection, the OAG may exercise any remedy, including immediate termination of this Contract.

6.2.4. The 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. The 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.

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

6.3.1. Within ninety (90) calendar days of this Contract's execution, the County and the OAG shall develop a detailed schedule for the retention and possible destruction of OAG Data. The schedule will be based upon the Contract Services being performed and the County's limited authorization to access, use, and disclose OAG Data.

6.3.2. 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, the County will provide the OAG with a signed statement(s) containing the date of destruction or purging, description of OAG Data destroyed or purged, and the method(s) used.

6.3.3. In the event of Contract expiration or termination for any reason, the County shall ensure the security of any OAG Data remaining in any storage component to prevent unauthorized disclosures. Within twenty (20) business days of Contract expiration or termination, the County shall provide the 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.

The County expressly does not have any actual or implied authority to determine whether any OAG Data are public or exempted from disclosure. The County is not authorized to respond to public information requests which would require disclosure of otherwise confidential information on behalf of the OAG. The 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 Contract. The County shall forward 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. The County shall respond to detected security incidents. The term "security incident" means an occurrence or event where the confidentiality of OAG Data may have been compromised. The 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:

1. Initial Responders
2. Containment
3. Management Notification
4. Documentation of Response Actions
5. Expeditious Confirmation of System Integrity
6. Collection of Audit Trails and Similar Evidence
7. Cause Analysis
8. Damage Analysis and mitigation
9. Internal Reporting Responsibility
10. External Reporting Responsibility
11. OAG Contract Manager's and OAG CISO's Name, Phone Number and Email Address

~~Attachment Six (6) is the 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.

6.4.2. Notice

6.4.2.1. Within one (1) hour of concluding that there has been any OAG Data security incident, the 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 Incident Response Plan.

6.4.2.2. Within twenty-four (24) hours of the discovery, the 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.

6.4.2.3. Each day thereafter until the investigation is complete, the 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.

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

6.4.3. Final Report

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

6.4.3.1.1. A detailed explanation of the cause(s) of the security incident;

6.4.3.1.2. 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,

6.4.3.1.3. 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 the OAG that states the date the County implemented the cure, a description of how the cure protects against the possibility of a recurrence, and that the County's security program is operating with the effectiveness required to assure that the security, confidentiality and integrity of OAG Data are protected.

6.4.3.2. If the cure has not been put in place by the time the report is submitted, the County shall, within five (5) business days after submission of the final report, provide a certification to the OAG that states the date the County implemented the cure, a description of how the cure protects against the possibility of a recurrence, and that the County's security program is operating with the effectiveness required to assure that the security, confidentiality and integrity of OAG Data are protected.

6.4.3.3. If the County fails to provide a Final Report or Certification within fifteen (15) calendar days of the security incident, the County agrees that the 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 Contract unless the OAG notifies the County in writing prior to the exercise of such remedy.

6.4.4. Independent Right to Investigate

6.4.4.1. The OAG reserves the right to conduct an independent investigation of any security incident, and should the OAG choose to do so, the County shall cooperate fully, making resources, personnel and systems access available. If at all possible, the OAG will provide reasonable notice to the County that it is going to conduct an independent investigation.

6.4.5. Security Audit

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

6.4.5.1.1. The County shall permit the 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:

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

6.4.5.1.1.2. 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;

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

6.4.5.1.2. When the OAG performs any of the above monitoring, observations, and inspections, the OAG will provide the 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.

6.4.5.1.3. Any audit of documents shall be conducted at the County's principal place of business and/or the location(s) of the County's operations during the County's normal business hours and at the OAG's expense. The County shall provide on the 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.

6.4.6. Remedial Action

6.4.6.1. Remedies Not Exclusive and Injunctive Relief

6.4.6.1.1. The remedies provided in this section are in addition to, and not exclusive of, all other remedies available within this Contract, or at law or in equity. The 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 the OAG may have at law or equity.

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

6.4.6.2. Notice to Third Parties

6.4.6.2.1. Subject to OAG review and approval, the 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. The County and the OAG shall mutually agree on the methodology for providing the notice.

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

6.4.6.2.3. If the County does not provide the required notice, the OAG may elect to provide notice of the security incident. The County and the OAG shall mutually agree on the methodology for providing the notice. Costs (excluding personnel costs) associated with providing notice shall be reimbursed to the OAG by the County. If the County does not reimburse such cost within thirty (30) calendar days of request, the OAG shall have the right to collect such cost. Additionally, the OAG may collect such cost by offsetting or reducing any future payments owed to the County.

6.4.7. Commencement of Legal Action

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

6.4.8. Survival of Provisions

6.4.8.1. Perpetual Survival and Severability

6.4.8.1.1. OAG rights and privileges applicable to OAG Data, including the confidentiality and security thereof, shall survive expiration or any termination of this Contract, and shall be perpetual.

7. AMENDMENT

This Contract shall not be amended or modified except by written amendment executed by duly authorized representatives of the OAG and the County.

8. TERMINATION OF THE CONTRACT

8.1. Discretionary Termination. The parties to this Contract shall have the right, in each party's sole discretion and at its sole option, to terminate this Contract by notifying the other party hereto in writing of such termination at least one hundred and eighty (180) calendar days prior to the effective date of such termination. Such notice of termination shall comply with the notice provisions in the Notices Section above, and shall state the effective date of such termination. Additionally, a copy of any such notice by the County shall be sent by registered or certified mail with return receipt requested, addressed to:

Office of the Attorney General
Joseph Fiore (or his successor in office), Mail Code 044
Managing Attorney, Contracts Attorneys, Legal Counsel Division
5500 East Oltorf
Austin, TX 78741

8.2. Termination for Default. If the County fails to provide the Contracted Services according to the provisions of this Contract, or fails to comply with any of the terms or conditions of this Contract, the OAG may, upon written notice of default to the County, terminate the Contract. Termination is not an exclusive remedy, but will be in addition to any other rights and remedies provided in equity, by law or under this Contract.

The OAG may exercise any other right, remedy or privilege which may be available to it under applicable law of the State and any other applicable law or proceed by appropriate court action

to enforce the provisions of this Contract, or to recover damages for the breach of any agreement being derived from this Contract. The exercise of any of the foregoing remedies will not constitute a termination of this Contract unless the OAG notifies the County in writing prior to the exercise of such remedy. The County will remain liable for all covenants under the aforesaid agreement. The County and the OAG will each be responsible for the payment of its own legal fees, and other costs and expenses, including attorney's fees and court costs, incurred with respect to the enforcement of any of the remedies listed herein.

8.3. Change in Federal or State Requirements. If federal or state laws, rules or regulations, or other federal or state requirements or guidelines are amended or judicially interpreted so that either party cannot reasonably fulfill this Contract and if the parties can not agree to an amendment that would enable substantial continuation of the Contract, the parties shall be discharged from any further obligations under this Contract.

8.4. Rights Upon Termination. In the event that the contract is terminated for any reason, or upon its expiration, the OAG shall retain ownership of all associated work products and documentation with any order that results from or is associated with this contract in whatever form that they exist.

8.5. Post Termination Responsibilities. Both the OAG and the County agree that upon any termination of this Contract, a smooth transfer of responsibility for the Contract Services being provided under this Contract is in the best interest of the public being served. The OAG and the County therefore agree to develop and implement a reasonable transition plan designed to achieve an efficient transfer of responsibility, either to the OAG or another entity, in a timely manner, and to cooperate fully throughout the post termination period until such transition is complete. The plan shall be in writing and shall, at a minimum, specify the procedures and schedule: for the County Community Supervision Office to be relieved of its responsibility to oversee the court ordered Community Supervision Program; and for the transfer of case files and other relevant information. The plan shall also specify any interim measures deemed necessary to ensure compliance with federal and state law, rules, regulations, requirements and guidelines. The plan shall be completed no later than ninety (90) calendar days after the execution of this Contract. The termination of services under this Contract, whether pursuant to the Termination of Contract Section or any other section of this Contract, shall be governed by and follow the approved transition plan.

8.6. Survival of Terms. Termination of this Contract for any reason shall not release the County 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. The County shall comply with all federal and state laws, rules, regulations, requirements and guidelines applicable to the County: (1) performing its obligations hereunder and to assure, with respect to its performances hereunder, that the OAG is fully and completely meeting obligations imposed by all laws, rules, regulations, requirements, and guidelines upon the OAG in carrying out the IV-D program pursuant to Chapter 231 of the Texas Family Code and Title IV, Part D, of the 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. Notwithstanding anything to the contrary in this Contract, the OAG reserves the right, in its sole discretion, to unilaterally amend this Contract

throughout its term to incorporate any modifications necessary for the OAG's or the County's compliance with all applicable state and federal laws, rules, regulations, requirements and guidelines.

9.1.2. Civil Rights. The 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 the 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 available under this Contract. The 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". The 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. The County certifies by entering into this Contract, that it is not debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency. The certification requirement of this provision shall be included in all subcontracts that exceed $100,000.

9.1.4. Records Retention. The County shall retain all financial records, supporting documents, statistical records, and any other records or books relating to the performances called for in this Contract. The 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 and litigation matters are resolved, whichever period is longer.

9.1.5. Environmental Protection. The County shall be in compliance with all applicable standards, orders, or requirements issued pursuant to the mandates of the Clean Air Act (42 U.S.C. Section 7401 et seq.) and the Federal Water Pollution Control Act, as amended, (33 U.S.C. 1251 et seq.). The certification requirement of this provision shall be included in all subcontracts that exceed $100,000.

9.1.6. Lobbying Disclosure. The County 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. The County must sign and return the Certification Regarding Lobbying (Attachment Eight (8)); attached hereto and incorporated herein). 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. The certification requirement of this provision shall be included in all subcontracts that exceed $100,000.

9.1.7. Copyrights and Publications. The County understands and agrees that where activities supported by this Contract produce original books, manuals, films, or other original material (hereinafter referred to as "the works"), the County may copyright the works subject to the reservation by the OAG and/or the United States Department of Health and Human Services, Administration for

Children and Families of a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for State and/or Federal Government purposes:

- the copyright in the works developed under this Contract, and
- any rights of copyright to which the County purchases ownership with funding from this Contract.

The County may publish, at its expense, the results of the Contract performance with prior OAG review and approval of that publication. Any publication (written, visual, or sound) shall include acknowledgment of the support received from the OAG and the United States Department of Health and Human Services, Administration for Children and Families. One (1) copy of any such publication must be provided to the OAG. The OAG reserves the right to require additional copies before or after the initial review. All copies shall be provided free of charge.

9.2. General Responsibilities

9.2.1. Independent Contractor. It is expressly understood and agreed by the parties hereto that the County is an independent contractor that shall have exclusive responsibility for any and all claims, demands, causes of action of every kind and character which may be asserted by any third party occurring from, in any way incident to, arising out of or in connection with the activities to be performed by the County hereunder. It is further expressly understood and agreed that any County personnel employed or retained to carry out the terms of this Contract are deemed to be employees and/ or agents of the County for purposes of retirement benefits, health insurance, all types of leave and any and all other purposes.

9.2.2. No Implied Authority. Any authority delegated to the County by the OAG is limited to the terms of this Contract. The County shall not rely upon implied authority and specifically is not delegated authority under this Contract to:

(1) Make public policy;
(2) Promulgate, amend, or disregard OAG Child Support program policy; or
(3) Unilaterally communicate or negotiate, on behalf of the OAG, with any member of the U.S. Congress or any member of their staff, any member of the Texas Legislature or any member of their staff, or any federal or state agency. However, the County is required to cooperate fully with the OAG in communications and negotiations with federal and state agencies, as directed by the OAG.

9.2.2.1. Force Majeure. The OAG shall not be responsible for performance of the Contract should it be prevented from performance by an act of war, order of legal authority, act of God, or other unavoidable cause not attributable to the fault or negligence of the OAG.

The County shall not be liable to the OAG for non-performance or delay in performance of a requirement under this Contract if such non-performance or delay is due to one of the following occurrences, which occurrence must not be preventable through the exercise of reasonable diligence, be beyond the control of the County, can not be circumvented through the use of alternate sources, work-around plans, or other means and occur without its fault or negligence: fire; flood; lightning strike; weather damage; earthquake; tornado; hurricane; snow or ice storms; equipment break down; acts of war, terrorism, riots, or civil disorder; strikes and disruption or outage of communications, power, or other utility.

In the event of an occurrence under the Force Majeure Section, the County will be excused from any further performance or observance of the requirements so affected for as long as such circumstances prevail and the County continues to use commercially reasonable efforts to recommence performance or observance whenever and to whatever extent possible without delay. The County shall immediately notify the OAG Contract Manager by telephone (to be confirmed in writing within five (5) calendar days of the inception of such occurrence) and describe at a reasonable level of detail the circumstances causing the non-performance or delay in performance.

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

9.2.4. Debts or Delinquencies Owed to Texas – 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.

9.3. Special Terms and Conditions

9.3.1. Permits. The County shall be responsible, at the County's expense, for obtaining any and all permits or licenses required by city, county, state, or federal rules, regulations, law, or codes.

9.3.2. Electrical Items. All electrical items must meet all applicable OSHA standards and regulations, and bear the appropriate listing from UL, FMRC, or NEMA.

9.3.3. Date Standard. 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."

9.3.4. Offshoring. All work to be performed under this Contract shall be performed within the United States and its territories.

9.3.5. Terminated Contracts. By executing this Contract, the County certifies that it has not had a contract terminated or been denied the renewal of any contract for non-compliance with policies or regulations of any state or federally funded program within the past five years nor is it currently prohibited from contracting with a governmental agency.

9.3.6. Non-Waiver of Rights. 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.

9.4. No Waiver of Sovereign Immunity. 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.

9.5. Severability. 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.

9.6. Applicable Law and Venue. The 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. The County also agrees that the exclusive venue and jurisdiction of any legal action or suit brought by the 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. The OAG agrees that any legal action or suit brought by the OAG concerning this Contract shall be brought in a court of competent jurisdiction in Travis County.

9.7. Entire Agreement. This instrument constitutes the entire Contract between the parties hereto, and all oral or written agreements between the parties hereto 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.

9.8. Originals and Counterparts. 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.

9.9. Attachments.

9.9.1. Attachment One. "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information"

9.9.2. Attachment Two. OAG Information Security Policy Manual

9.9.3. Attachment Three. OAG Statement of Responsibility

9.9.4. Attachment Four. IRS Notification Form

9.9.5. Attachment Five. Online Login Policy

9.9.6. Attachment Six. County Internal Incident Response Plan

9.9.7. Attachment Seven. Certification of Local Expenditures Report

9.9.8. Attachment Eight. Certification Regarding Lobbying

AGREED TO AND ACCEPTED:

OFFICE OF THE ATTORNEY GENERAL

Alicia Key

Alicia Key
Deputy Attorney General for Child Support

11-2-09

Date

TRAVIS COUNTY

Samuel T. Briscoe

The Honorable Samuel Briscoe
County Judge, Travis County

10-27-09

Date

#.1. PERFORMANCE 38
#.2. CRIMINAL/CIVIL SANCTIONS 39
#.3. INSPECTION 40

ATTACHMENT ONE

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 NIST SP 800-53. 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.

#.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.

#.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 TWO

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 4
   1.1. Attorney General Policy Statement 4
   1.2. Scope of Policy 4
   1.3. OAG Information Security Policy Purpose & Intent 4
   1.4. Definitions 4
2. Management Security Controls 5
   2.1. State Agency Head - Attorney General 5
   2.2. Management Responsibility 5
   2.3. Information Resources Manager (IRM) 5
   2.4. Chief Information Security Officer (CISO) 5
   2.5. Information Security Officers (ISO) 6
   2.6. Information Resource Owner 7
   2.7. Information Custodian 7
   2.8. Information System User 8
3. Operational Security Controls 8
   3.1. Risk Management Framework 8
   3.2. Risk Assessment 8
   3.3. Asset Management 9
   3.4. Disaster Recovery & Business Continuity 9
   3.5. Outsourced Data Center Operations & Security Responsibility 9
4. Personnel Security Policy 9
   4.1. Statement of Responsibility 9
   4.2. Reporting of Security Incidents 9
   4.3. Computer Security Incident Response Team (CSIRT) 9
   4.4. Information Security Violations 10
   4.5. Acceptable Use of OAG Information Resources 11
   4.6. Access to OAG Information Systems and Assets 11
   4.7. User Identification 11
   4.8. Personal Software, Hardware and Modems 11
   4.9. Security Awareness Program 11
   4.10. Warning Statements 11
   4.11. Termination of Employment 12
   4.12. Automatic Suspension / Deletion of User ID's 12
   4.13. Positions of Special Trust 12
5. Technical Security Controls 12
   5.1. System Security Policy 12
   5.2. System Administrators 12
   5.3. System Developers 13
   5.4. Information Asset Protection 13
   5.5. Vendor Access to OAG Systems 13
   5.6. Classification of Electronic Data and Assets 13
   5.7. Data Destruction 14
   5.8. Configuration Management 14

5.9. Change Management 14
5.10. Data Integrity 14
5.11. Voice/Phone Mail 14
5.12. E-Mail 15
5.13. Wireless Systems 15
5.14. Copyright 15
5.15. Personal Software, Shareware and Freeware 15
5.16. Data Encryption 15
5.17. Portable and Mobile Devices 15
5.18. Malware Protection Software 15
5.19. Intrusion Detection 16
5.20. Internal Electronic Investigations 16
5.21. Screen Savers 16
5.22. User Passwords 16
5.23. Administrator Passwords 16
5.24. System Log On & Re-Boot 16
5.25. System Settings 17
5.26. Control of Peripherals 17
5.27. Security Breaches 17
5.28. Dial-up Access 17
5.29. Purchasing/Development Pre-Approval 17
5.30. Contract Security Provisions 17
5.31. System Development, Acquisition and Testing 18
6. Exception, Waiver and Modification 18
6.1. Waivers and Exceptions 18
6.2. Modification or Significant Changes to Procedures 18
6.3. Executive Management Waiver 18
7. Document Acceptance and Release Notice 19
8. References 20

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."

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 obtain items in accordance with signature approval list below.

Date: February [illegible], [illegible]

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 [illegible] that is used by or for the OAG, throughout its life cycle. This policy also applies to all users of OAG information resources and electronic data, regardless of location.

Attachments: Information Technology Security Policy Manual (Version 1.0)

Prepared by ITS Division

[illegible] February [illegible]

Division Chief Date

PLEASE FORWARD TO: [illegible]

X Approved _Approved with Comments/Edits _Not Approved

[illegible]

[illegible] [illegible]

General Counsel Division Date

[illegible]

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

PLEASE FORWARD BY *DATE*

✓ Approved __Approved with Comments/Edits __Not Approved

Version 3.0

Jonathan F. Mitchell
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

ATTACHMENT THREE

OFFICE of the ATTORNEY GENERAL
GREG ABBOTT
CHILDSUPPORT DIVISION

AUTOMATED COMPUTER SYSTEM ACCESS – STATEMENT OF RESPONSIBILITY

Name:	Agency Employed By:
Position:	Work Location (Address, City, Country):
Phone:	
FAX:	

If given access to the automated computer system maintained by the Office of the Attorney General of Texas, I agree to the following:

1. All information maintained in the files and records of the Office of the Attorney General of Texas (OAG), Child Support Division are privileged and confidential.
2. Information that I obtain about anyone while using the computer system of the OAG must be held in strictest confidence and may not be disclosed except as used exclusively for purposes directly connected with the administration of programs under Titles IV-A, IV-D, IV-E and XIX of the federal Social Security Act and in accordance with the OAG Confidentiality Policy and Procedures.
3. Only authorized personnel may view, add, modify and/or delete information.
4. I may not perform any work, review, update or otherwise act to obtain information about my own, or any relative's, friend's, or business associate's child support case, even if the case is closed.
5. The computer password(s) I receive or devise are confidential, and must not be disclosed to anyone.
6. I am responsible for computer transactions performed through misuse of my password(s).
7. Use of a password not issued or devised specifically for me is expressly prohibited and is a violation of Texas and United States law.
8. I will not load unauthorized software, personal computer programs, shareware or freeware of any kind onto the OAG computer equipment.
9. Copyrighted material, including 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.
10. United States federal tax return or return information may not be disclosed to any individual or agency.
11. It is unlawful to offer or receive anything of value in exchange for United States federal tax return or return information.

CIVIL AND CRIMINAL PENALTIES

I acknowledge that if I fail to observe this agreement, the following civil and criminal penalties apply:

1. A violation will be reported to appropriate personnel for disciplinary action, including termination and referral for prosecution.
2. 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 United States federal statutes may also be applicable.
3. Unauthorized disclosure or exchange of federal tax information is punishable by fine up to $5,000, or imprisonment up to 5 years, or both, under United States Internal Revenue Code 7213 and 7213 A
4. 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, United States Internal Revenue Code.
5. I may be civilly liable for damages of not less than $1000 per violation for unauthorized disclosure of federal tax information, together with costs of prosecution under Section 7431 of the United States Internal Revenue Code.

SIGNATURE: _____ DATE: _____

FAX completed form to **HelpDesk** at FAX number **512-460-6027**

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

First Assistant Attorney General

Date 2/13/09

WARNING
DISCLOSURE LIMITATIONS

Unauthorized disclosure, printing, or publishing of any Federal return or return information, or any information therefrom, is punishable by fine up to $5,000 or imprisonment up to 5 years, or both, together with costs of prosecution. See Sec. 7213 of the Internal Revenue Code (IRC) and 18 U.S.C. Sec. 1905. A person authorized to access IRS return or return information can be prosecuted under the federal "Anti-Browsing" Law, see IRC Sec, 7213A, if the information was accessed without a need to know. The offense constitutes a federal misdemeanor punishable by not more than 1 year in prison, or a $1,000 fine, or both, plus cost of prosecution. In addition, IRC Sec. 7431 provides for civil damages of not less than $1,000 per violation for unauthorized disclosure of such information, together with costs of prosecution.

It is unlawful for any person willfully to offer any item of material value in exchange for any return or return information and to receive as a result of such solicitation any such return or return information. Such action is punishable by fine up to $5,000 or imprisonment up to 5 years, or both, together with costs of prosecution. See Sec, 7213 of the IRC and 18 U.S.C. Sec. 1905. Section 6103 (1) (8) of the IRC permits the SSA to disclose tax return information to IV-D agencies subject to the same restrictions on disclosure above.

I acknowledge that I am aware of the above civil and criminal liabilities.

Name (please print)_____ Date_____

Signature_____ SSN_____

Please check the appropriate box below that indicates your current Employment Status or your affiliation with the Attorney General of Texas agency:

☐	Child Support Full-Time Equivalent (FTE) Staff	☐	External Entity Staff (e.g., DHS, TWC, County, etc.)
☐	Child Support Part-Time Staff	☐	Intern
☐	Contractor/Vendor Staff	☐	Temporary Staff
☐	County Enforcement Staff	☐	Volunteer

For Field staff, please follow your local or Regional procedures when submitting this form for processing. For State Office staff, please forward completed form to: Brenda Staehr, Child Support Division, Procedures and Training Section, Mail Code 053, P.O. Box 12017, Austin, Texas 78711-2017.

Child Support Online
Account Services Employer Home
Login Request Password Account Request Request User ID

Login

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 FIVE

Child Support Online

Account Services Employer Home

Login Request Password Account Request Request User ID

Login

Policy

When you register for the OAG Portal Service, we may ask you to give us certain identifying information ("Registration").

You agree to provide true, accurate, current and complete information about yourself. You also agree not to impersonate any person or entity, misrepresent any affiliation with another person, entity or association, use false headers or otherwise conceal your identity from the OAG for any purpose.

For your protection and the protection of our other members and Web site users, you agree that you will not share your Registration information (including passwords, User Names, and screen names) with any other person for the purpose of facilitating their access and unauthorized use of OAG Portal Services. You alone are responsible for all transactions initiated, messages posted, statements made, or acts or omissions that occur within any OAG Portal Service through the use of Registration information. Your failure to honor any portion of this agreement can result in termination of access to Portal Services.

I Agree | I Disagree

ITS Department

Security Incident Response Plan For OAG Data

Version: Draft .00.01.01

Prepared by:

Shannon Clyde
Information Security Manager

Last Update: November 06, 2007

A. REVISION HISTORY

Contributors	Date	Reason For Changes	Version
Shannon Clyde	October 01, 2007	Initial Draft	00.01.00
Shannon Clyde	November 06, 2007	Final Author Draft - corrected Security Analyst contact information - corrected table of content reference	00.01.01

B. TABLE OF CONTENTS

A. REVISION HISTORY 2
B. TABLE OF CONTENTS 3
C. INTRODUCTION 4
1.0 Objectives and Scope 4
2.0 Audience 4
3.0 Keywords Defining Requirements 4
4.0 Requirement Priorities 5
5.0 Document Change Management 5
D. INCIDENT RESPONSE CONTACT INFORMATION 6
1.0 Office of Attorney General (OAG) Contacts 6
2.0 Travis County Contacts 6
E. OAG DATA INCIDENT MANAGEMENT REQUIREMENTS 7
1.0 General Requirements 7
2.0 Responsibility for Notifications and Reports 7
3.0 Notification Requirements 7
4.0 Reporting Requirements 8

C. INTRODUCTION

1.0 Objectives and Scope

The Travis County ("County") Information and Telecommunications Systems Department (ITS) Security Incident Response Plan for Office of the Attorney General (OAG) Data supplements the Travis County ITS Department Incident Response Standards and Procedures.

This Security Incident Response Plan is intended to provide the specific requirements that must be met to comply with SFY 2010 Community Supervision Contract # 10-C0028, §6.4.1.

2.0 Audience

Those who need to participate in the ITS Incident Response efforts involving OAG Data including Community Supervision staff, ITS Department staff and those who need to interact with the incident management efforts involving OAG Data.

3.0 Keywords Defining Requirements

The following keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are utilized within this document to indicate requirement levels and are to be interpreted as described below:

SHALL: This word, or the terms "REQUIRED" or "MUST", means that the definition is an absolute requirement of the specification.

SHALL NOT: This phrase, or the phrase "MUST NOT", means that the definition is an absolute prohibition of the specification.

SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications must be understood and the case carefully weighed before implementing any behavior described with this label.

MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation that does

include the option, though perhaps with reduced functionality. In the same vein, an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides.)

4.0 Requirement Priorities

Requirements that use the key word MUST or SHALL have the highest priority.

Those described as RECOMMENDED, as indicated by the use of the key word SHOULD, have a secondary priority to those requirements using the key words SHALL or MUST.

Those described as OPTIONAL, as indicated by the use of the key word MAY, have a tertiary priority. All first priority requirements represent core functionality critical to the project and must be met.

As many secondary priority requirements should be met if allotted time, human resources and funding permit.

Tertiary priorities should be completed only after all first and secondary priorities have been met.

5.0 Document Change Management

Requests for changes to this document should be made in writing to the Information Security Manager or the Chief Information Officer.

D. INCIDENT RESPONSE CONTACT INFORMATION

1.0 Office of Attorney General (OAG) Contacts

Position	Name	Phone Number	Email address
OAG Chief of Information Security Officer	Walt Foultz	512-936-1320	Walt.Foultz@OAG.State.TX.US
OAG Community Supervision Contract Manager	Allen Broussard	512-460-6373	Allen.Brousard@CS.OAG.State.TX.US

2.0 Travis County Contacts

Position	Name	Phone Number	Email address
Chief Information Officer	Joe Harlow	512-854-9372	Joe.Harlow@co.travis.tx.us
ITS Department Information Security Manager	Shannon Clyde	512-854-7846	Shannon.Clyde@co.travis.tx.us
ITS Department Sr. Information Security Analyst	David Stanton	512-854-4024	David.Stanton@co.travis.tx.us
ITS Department Help Desk		512-854-9175	ITS.Helpdesk@co.travis.tx.us
County Contract Manager			
County Community Supervision Contract Manager			

E. OAG DATA INCIDENT MANAGEMENT REQUIREMENTS

1.0 General Requirements

County shall respond to security incidents involving OAG Data in accordance with ITS Department Incident Management Standards and Procedures and specific OAG requirements as stated within this Incident Response Plan for OAG Data.

2.0 Responsibility for Notifications and Reports

The Information Security Officer or designate is responsible for the data collection, document creation, and delivering of the required notices and reports identified within this plan.

3.0 Notification Requirements

3.1. Initial Incident Notification to OAG

3.1.1. OAG Notification Time Frame, Recipients, Method

The OAG CISO and the OAG Contract Manager must be notified by telephone and electronic mail ***within one (1) hour of determination that OAG Data is involved in the incident.***

3.1.2. OAG Notification Content

Content of the notification must include:

Notice of incident

Description of Affected Information System

Initial damage assessment and potential scope of incident

Containment/Eradication/Recovery steps taken to date

Any changes in County contact information

4.0 Reporting Requirements

4.1. Initial Written Report to OAG

4.1.1. Initial OAG Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a written report to the OAG CISO and the OAG Contract Manager by electronic mail ***within twenty-four (24) hours of determination that OAG Data is involved in the incident.***

4.1.2. Report Content

Disclosure of all information relating to the incident

Results of preliminary damage analysis

Time, nature of incident; mitigation efforts; corrective actions; estimated recovery time

4.2. Daily Status Report to OAG:

4.2.1. Daily OAG Status Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a *daily* oral status report to the OAG CISO or designate and an electronic mail message follow up to the OAG CISO and the OAG Contract Manager

4.2.2. Report Content

Current damage analysis

Status of containment, eradication, recovery efforts

4.3. Final Report to OAG:

4.3.1. Final OAG Report Time Frame, Recipients, Method

The Information Security Manager or designate must provide a final written report by electronic mail to the OAG CISO and the OAG Contract Manager *within five (5) days of the completion of the final damage analysis and the completion of the eradication/recovery phases but prior to incident closure.*

4.3.2. Report Content

Cause of security incident

Nature of security incident

Description of cure, effective date, description of how cure protects from recurrence

Certification Statement: County's security program is operating with the effectiveness required to assure that the confidentiality and integrity of OAG Data are protected

ATTACHMENT SEVEN

SFY 200___
Certification of Local Expenditures
Bexar County Children First, Contract #_____

County of _____, Fiscal Year 200___

From _____ To _____

Actual Local Expenditures for FY 200___

Description	Total	Percent Allocation	Allocated Total
Salaries and Fringe Benefits	$		
Travel	$		
Operating Expenses	$		
Indirect Cost	$		
Other (Please Describe)	$		
Fiscal Year Total	$		

Verification

I DO SOLEMNLY SWEAR THAT the foregoing Financial Statement filed herewith is in all things true and correct, and fully shows all information required to be reported pursuant to Contract # _____.

_____
Signature of Affiant

SWORN AND SUBSCRIED BEFORE ME BY _____ this

_____ day of _____, 200____, to certify which, witness my hand and seal.

Notary Public in and for

_____ County, Texas