ATTORNEY GENERAL OF TEXAS
GREG ABBOTT
CHILD SUPPORT DIVISION

June 20, 2012

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

RE: Two Originals of FY13/14 State Case Registry and Local Customer Service Contract

Dear Ms. Hinojosa:

Attached are two originals of the renewal for the FY13/14 State Case Registry/Local Customer Service (SCR/LCS) Contract. Please have both originals signed where indicated.

Also attached is the Incident Response Plan, Attachment G (flagged), which is designed to provide a general reference to both OAG and county staff when a security incident may threaten the confidentiality of OAG data. You will need to submit a new Incident Response Plan even if no changes occurred since the previous contract. Pursuant to contract requirement § 6.4.1.1, please complete the Incident Response Plan and return it along with both signed originals to the following:

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

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

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

Sincerely,

Allen Broussard
Manager, Government Contracts

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

CONTRACT NO. 13-C0047

1. INTRODUCTION & PURPOSE

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

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

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

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

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

2. CONTRACT PERIOD

2.1. This Contract shall commence on September 1, 2012 and shall terminate on August 31, 2014, unless terminated earlier by provisions of this Contract.

3. REQUIREMENTS OF THE OAG AND THE COUNTY

3.1. State Case Registry Activities

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

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

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

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

3.1.1.2.2. family violence indicator, if applicable

3.1.1.2.3. name of each participant (last and first)

3.1.1.2.4. sex code for each participant

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

3.1.1.2.6. cause number

3.1.1.2.7. cause county code

3.1.1.2.8. start date of cause

3.1.1.2.9. order modification date

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

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

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

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

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

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

3.1.1.8. County shall ensure that the Family Violence Indicator (FVI) is updated on Registry Only cases in TXCSES Web within three (3) business days of a protective order being filed. If a Full Service case exists the county shall provide the local OAG field office with a copy of the protective order within three (3) business days of it being filed.

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

3.1.1.10. County shall ensure that payments on cases that have been redirected from the County registry to the TXSDU are paid to the TXSDU and that disbursements on such cases are no longer made by the County. The District Clerk or the Domestic Relations Office (as

applicable) shall send all erroneously received child support payments to the TXSDU within one day of receipt.

3.1.1.11. County agrees that all court orders must direct child support payments to the (TXSDU) in accordance with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations. Where the County identifies a pattern of court orders from a particular court or attorney that fail to comply with Section 154.004 of the Texas Family Code and 42 USC 654b of the Code of Federal Regulations, the County will notify the OAG of same.

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

3.2. LOCAL CUSTOMER SERVICE

3.2.1. County Customer Service Unit Resources and Services

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

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

3.2.1.2.1. These activities include but are not limited to:

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

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

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

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

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

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

3.2.3. Customer Service Unit Documentation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2.5. In the event of a failed transmission, or if a file is unable to be processed, County shall correct the problem and retransmit within one (1) business day of notification by the OAG.

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

3.3. ACCESSING OAG SYSTEMS

3.3.1. County Responsibilities

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

3.3.1.2. County must make necessary programming changes to its own automated child support system to accomplish the local customer service activities in this Contract. If the County employs a

Vendor for maintenance and changes to its automated child support system, County must coordinate efforts between the County Vendor and the OAG or its designated agent.

3.3.1.3. Should the County desire to retain their legacy case management system, whether in-house or vendor based, the County is required to maintain strict data synchronization with the OAG Systems. To accomplish this, the County must demonstrate sufficient resources and ability to receive and process into the County legacy system daily data updates from the OAG in ICD050 format.

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

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

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

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

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

3.4. OAG Responsibilities

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

4. REIMBURSEMENT

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

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

4.3. If the County approves the Summary and Reimbursement Voucher, the County signs the voucher and returns it to OAG for payment within ten (10) County business days. County's signature constitutes

approval of the voucher and certification that all services provided during the period covered by the voucher are included on the voucher. The OAG shall process the invoice for payment in accordance with the state procedures for issuing state payments and the Texas Prompt Payment Act.

4.3.1. County shall submit the invoice to:

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

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

4.4.1. OAG Rights Upon Loss of Funding

4.4.1.1. Legislative Appropriations

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

4.4.2. Provision of Funding by the United States

4.4.2.1. It is expressly understood that any and all of the OAG's obligations and liabilities hereunder are contingent upon the existence of a state plan for child support enforcement approved by the United States Department of Health and Human Services providing for the

statewide program of child support enforcement, pursuant to the Social Security Act, and on the availability of Federal Financial Participation for the activities described herein. In the event that such approval of the state plan or the availability of Federal Financial Participation should lapse or otherwise terminate, the OAG, in its discretion, may terminate this contract, either in whole or in part. In the event of such termination, the OAG will not be considered to be in default or breach under this contract, nor shall it be liable for any further payments ordinarily due under this contract, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination. The OAG shall make best efforts to provide reasonable written advance notice to Contractor of any such termination. In the event of such a termination, County shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. OAG shall be liable for payments limited only to the portion of work the OAG authorized in writing and which the County has completed, delivered to the OAG, and which has been accepted by the OAG. All such work shall have been completed, per the Contract requirements, prior to the effective date of termination.

4.5. Reimbursement Rates

4.5.1. State Case Registry

4.5.1.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated cost that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purpose of reference only the federal share on the effective date of this Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of new and modified Registry Only Court Orders (together with all required data elements) provided to the OAG during the calendar month multiplied by a per new and modified Registry Only Court Order fee of $12.81 plus the number of Registry Only Court Orders updated during the calendar month multiplied by a per Registry Only Court Order updated fee of $4.07 per Registry Only Court Order updated. Thus: [(Calendar Month new and modified Registry Only Court Orders provided x $12.81) + (Calendar Month Registry Only Court Orders updated x $4.07)] x Federal Share = OAG Liability.

4.5.2. Local Customer Service

4.5.2.1. The OAG shall be financially liable to the County for the federal share of the County's Contract associated cost. Federal share means the portion of the County's Contract associated cost that the federal Office of Child Support Enforcement reimburses the state as federal financial participation under Title IV-D; for purpose of reference only the federal share on the effective date of this Contract is 66%. The County agrees that for the purposes of this Contract all of the County's Contract associated costs for any given calendar month is equal to the number of inquiries on IV-D cases handled by County personnel during the calendar month, plus the number of inquiries on Registry Only cases (See Section 3.2.1 for the meaning of Registry Only cases) minus the Federal Disallowance Percentage, multiplied by a per inquiry fee of $4.19 per inquiry. For purpose of reference only the Federal Disallowance Percentage for SFY 2011 annualized is 19%. Thus: (Calendar Month IV-D Inquiries Handled by County Personnel) + (Calendar Month Registry Only Inquiries Handled by County Personnel - Federal Disallowance Percentage) x ($4.19) x (Federal Share) = OAG Liability.

4.6. Limitation of OAG Liability

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

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

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

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

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

4.6.6. Notwithstanding any other provision of this Contract, the maximum liability of the OAG under this Contract is **Forty Seven Thousand Six Hundred Dollars and No Cents ($47,600.00)**.

4.7. Assignment of Claims

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

5. CONTRACT MANAGEMENT

5.1. Written Notice Delivery

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

5.1.1.1. County

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

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

5.1.1.2. OAG

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

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

With copies to:

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

and

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

5.2. Controlled Correspondence

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

5.3. Inspections, Monitoring and Audits

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

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

5.4. Reimbursement of Audit Penalty

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

5.5. Remedies for Non-Performance

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

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

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

5.6. Training on OAG Systems

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

Larry Acevedo
Office of the Attorney General
Mail Code 053
PO Box 12017
Austin, TX 78711-2017
email address: CSD-TRN@texasattorneygeneral.gov

5.7. Assignment

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

5.8. Liaison

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

5.9. Subcontracting

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

5.10. Dispute Resolution Process for County Breach of Contract Claim

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

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

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

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

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

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

5.11. Reporting Fraud, Waste or Abuse

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

5.11.1.1. the Contract Manager

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

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

5.11.1.4. the OAG Ethics Advisor

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

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

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

5.11.2.1. the specific suspected misconduct

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

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

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

5.11.2.5. any documents which tend to support the allegations.

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

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

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

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

6. CONFIDENTIALITY AND SECURITY

6.1. Confidentiality and Security Provisions

6.1.1. General

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

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

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

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

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

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

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

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

6.1.1.9. County shall comply with all applicable statutory and regulatory provisions requiring that information be safeguarded and kept confidential. These statutes and regulatory provisions include but are not limited to 42 U.S.C. §§ 653 and 654; 45 CFR §§ 307.10, 307.11 and 307.13; 26 U.S.C. 6103 (IRC 6103); IRS Publication 1075 (Rev.8-2010) and § 231.108 of the Texas Family Code, each as currently written or as may be amended, revised or enacted. County shall also comply with OAG policy, processes and procedures concerning the safeguarding and confidentiality of information, and computer security (including any requirements set forth in Attachment F, entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information"). The requirements of these Confidentiality and Security Provisions shall be included in, and apply to, subcontracts and agreements the County has with anyone performing Agreement Services on County's behalf.

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

6.2. OAG Data Usage and Storage

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

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

6.2.2. OAG Data are not allowed on mobile/remote/portable storage devices; nor may storage media be removed from the facility used by County. Any exception to this prohibition must have OAG prior approval. Such approval may only be granted by Controlled Correspondence or Contract amendment. This prohibition does not apply to County Information Systems backup procedure. County Information Systems backup procedure is subject to the United States Internal Revenue Service requirements set forth in IRS Publication 1075 (Rev.8-2010) and Attachment F entitled "United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information".

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

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

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

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

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

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

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

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

6.4. Security Incidents

6.4.1. Response to Security Incidents

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

6.4.1.1.1. Initial responders

6.4.1.1.2. Containment

6.4.1.1.3. Management Notification

6.4.1.1.4. Documentation of Response Actions

6.4.1.1.5. Expeditious confirmation of system integrity

6.4.1.1.6. Collection of audit trails and similar evidence

6.4.1.1.7. Cause analysis

6.4.1.1.8. Damage analysis and mitigation

6.4.1.1.9. Internal Reporting Responsibility

6.4.1.1.10. External Reporting Responsibility

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

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

6.5. Notice

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

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

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

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

6.6. Final Report

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

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

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

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

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

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

6.7. Independent Right to Investigate

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

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

6.8. Security Audit

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

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

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

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

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

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

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

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

6.9. Remedial Action

6.9.1. Remedies Not Exclusive and Injunctive Relief

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

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

6.10. Notice to Third Parties

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

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

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

6.11. Commencement of Legal Action

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

7. AMENDMENT

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

8. TERMINATION OF CONTRACT

8.1. Termination

8.1.1. Either party to this Contract shall have the right to either terminate this Contract in its entirety or in part. However, a County continuing to contract to provide Local Customer Service services must also continue to contract to provide State Case Registry services. The Contract, or portion of the Contract, may be terminated by the terminating party notifying the other party in writing of such termination and the proposed date of the termination no later than thirty (30) calendar days prior to the effective date of such termination.

8.2. Survival of Terms

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

9. TERMS AND CONDITIONS

9.1. Federal Terms and Conditions

9.1.1. Compliance with Law, Policy and Procedure

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

9.1.2. Civil Rights

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

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

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

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

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

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

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

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

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

9.2. News Releases or Pronouncements

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

9.3. Date Standard

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

9.4. Headings

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

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

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

9.6. Certification Concerning Dealings with Public Servants

9.6.1. County, by signing this contract, certifies that it has not given nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this transaction.

9.7. Personnel Comportment

9.7.1. County and County subcontractor personnel and agents shall be courteous and professional in all communications during their performance of the requirements of this contract. Any actions deemed unprofessional must be remedied to the satisfaction of the OAG Contract Manager. The OAG reserves the right, in its sole discretion, to require the immediate removal and replacement of any County and/or County subcontractor personnel and agents deemed by the OAG to be discourteous, unprofessional, unsuitable or otherwise objectionable. Any replacement personnel assigned by County to perform services under this contract must have qualifications for the assigned position that equal or exceed those of the person being replaced.

9.8. Non-Waiver of Rights

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

9.9. No Waiver of Sovereign Immunity

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

9.10. Severability

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

9.11. Applicable Law and Venue

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

9.12. Entire Contract

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

9.13. Counterparts

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

9.14. Attachments

9.14.1. Attachment A: OAG Information Security Policy Manual

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

9.14.3. Attachment C: Child Support Online Login Policy

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

9.14.5. Attachment E: Certification Regarding Lobbying

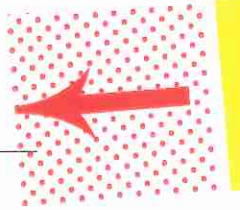
9.14.6. Attachment F: IRS Publication 1075 (Rev.8-2010)

9.14.7. Attachment G: Incident Response Plan

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

THIS CONTRACT IS HEREBY ACCEPTED

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



ATTACHMENT A

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

Office of the Attorney General
Information Technology Security Policy Manual

Version 4.3
April 5, 2011

Presented by:
Kathleen Donaho-Jaeger
CS Information Security Officer
Mike O'Connell
A&L Information Security Officer

Table of Contents

1. Information Security Policy

1.1. Attorney General Policy Statement

The Office of the Attorney General (OAG) is committed to protecting the information resources that are 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 Information Security Officers are 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 assets" that are used by or for the OAG throughout its life cycle. "Information assets" 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.[i]

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

To the extent there is any conflict between this policy and the Sensitive Personal Information Privacy Policy (found at https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php), the latter shall control.

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 assets.

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 Asset:
The term information asset 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 Technology Asset:
A subset of the term information asset 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 assets are protected from the effects of damage, destruction, and unauthorized or accidental modification, access or disclosure.

2.2. Management Responsibility

The protection of information assets 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. Information Security Officers (ISO)

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

directly to their respective IT Directors and indirectly to the IRM. It is the ISO'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 asset 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 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 asset;
- Determine the asset's 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.

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

2.7. Information Technology User

All authorized users of OAG information technology assets (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. Each division's ISO 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 IRM and appropriate IT Director. (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 ISO's 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, which may be found at https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php).

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 IRM and appropriate IT Director of the actual or suspected security incident. The ISO 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:

1. Management Group:
   - Membership includes: The affected division's ISO and IT Director.
   - May include: IRM.
   - Responsibilities: Manage CSIRT operations (ISO), manage overall incident response, document activities, and produce appropriate reports. Also responsible to communicate internally to executive management.

2. 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.

3. 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 appropriate ISO, 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 prior to implementation.

4.5. Acceptable Use of OAG Information Technology Assets

State information technology assets 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, found at https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php.

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

4.6. Access to OAG Information Technology 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 appropriate ISO 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 appropriate ISO 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 IDs) 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 assets.

4.12. Automatic Suspension / Deletion of User ID's

Mainframe, LAN and Remote Access User IDs will be monitored for usage to protect system security, and any unused user IDs 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 ISOs 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 Technology 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 and approved by the appropriate ISO.

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 ISO 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 assets 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 assets. 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 assets. All use of e-mail must be in accordance with OAG policies and procedures regarding the use of information assets.

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 both the appropriate IT Director and ISO.

5.13. Wireless Systems

Wireless networks or routers may not be used without the prior authorization of both the appropriate IT Director and ISO. All wireless connectivity (Wi-Fi) to OAG networks must be in accordance with current IT architectural direction, Information Technology 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 assets 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 both the appropriate IT Director and ISO.

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 both the appropriate IT Director and ISO.

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 using techniques approved by the appropriate ISO.

5.20. Internal Electronic Investigations

All internal electronic investigations must be authorized by, and conducted under the supervision of, the appropriate ISO 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 found at http://www2.dir.state.tx.us/security/policy/Pages/policy.aspx. 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 appropriate IT Director and IRM. 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 appropriate IT Director and ISO.

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 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 appropriate ISO 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 appropriate ISO 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 technology 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 and approved by the IRM, appropriate IT Director, appropriate ISO, 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 the appropriate IT Director and approved by the appropriate ISO prior to implementation. If immediate changes to procedures are required to meet an emergency situation, A&L and/or CS ISO, 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 **4.2** of the **OAG Information Security Division Security Policy Manual.**

The OAG Information Security Division 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: April 5, 2011
Mike O'Connell, A&L Information Security Officer

OWNER: _____ DATE: April 5, 2011
Kathleen Donaho-Jaeger, CSD Information Security Officer

EXECUTIVE SPONSOR: _____ DATE: April 5, 2011
Diane B. Smith, Deputy for Administration and Information Resources 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).

ATTACHMENT B

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

Statement

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

General Information:

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

Statements:

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

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

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

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

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

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

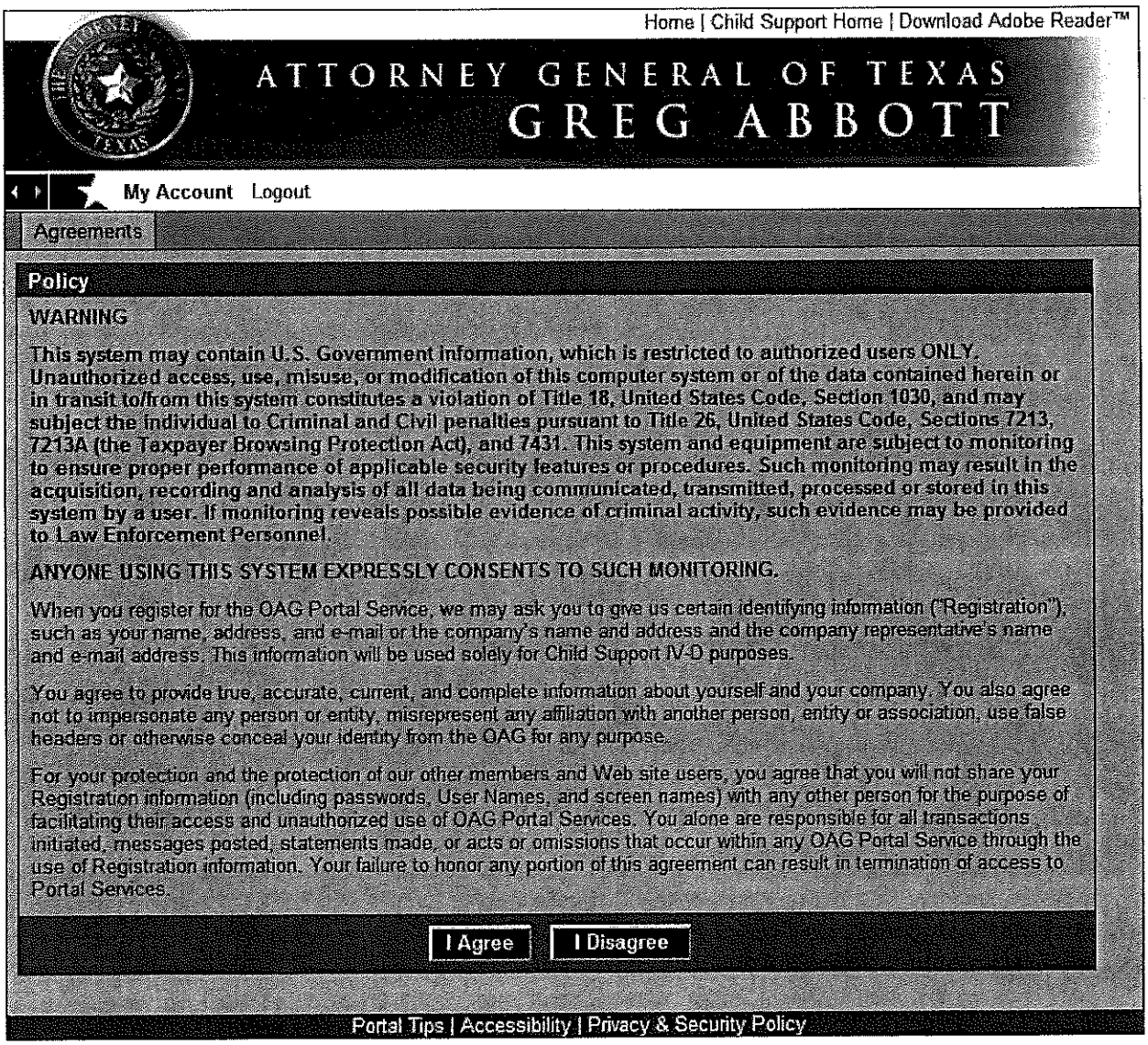
I also understand that failure to observe the above conditions may constitute a "breach of computer security" as defined in the TEXAS PENAL CODE, CHAPTER 33, Section 33.02 (b), and that such an offense may be classified as a felony. Similar federal statutes may also be applicable.

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

By agreeing to this statement I certify that I:

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

I Agree | I Disagree


Home | Child Support Home | Download Adobe Reader™
ATTORNEY GENERAL OF TEXAS
GREG ABBOTT
My Account Logout
Agreements
Policy
WARNING
This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.
ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.
When you register for the OAG Portal Service, we may ask you to give us certain identifying information ("Registration"), such as your name, address, and e-mail or the company's name and address and the company representative's name and e-mail address. This information will be used solely for Child Support IV-D purposes.
You agree to provide true, accurate, current, and complete information about yourself and your company. 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
Portal Tips | Accessibility | Privacy & Security Policy

Data Integrity Procedures Changes to Case Information

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

- Name
- Date of Birth
- Home address

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

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

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

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

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

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

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

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

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

PERIOD: September 1, 2012 to August 31, 2014

Certification for Contracts, Grants, Loans and Cooperative Agreements

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

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

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

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

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

_____ _____

Signature Date

_____

Title

_____

Organization

The agency should include the Exhibit 7 language for either General Services or Technology Services, as appropriate and include the language below to the greatest extent possible, applicable to the specific situation.

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

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) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available 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 this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

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

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) 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.

(6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) 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 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 five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future 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) 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 this 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 $1,000.00 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 $1,000.00 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. The penaltiesare prescribed by IRC Sections 7213A and 7431.

(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 so 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.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

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.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

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

(2) 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.

(3) 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.

(4) 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.

(5) 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.

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

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

(8) 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.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS:

(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) 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.

(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.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting

unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION:

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

County of Hidalgo, Texas

DRP

Disaster Recovery Plan

Assigned to the following Organizational Units:
Information Technology Department

Assigned to the following Geographic Locations:
The County of Hidalgo, Texas

STROHL SYSTEMS

Printed on: 6/5/2007

Table of Contents

Table of Contents

Plan Overview
Disaster Recovery Plan

6/5/2007

Report Description:
This report describes the plan's purpose, objectives, assumptions and strategies on which the plan is based.

Scope

In Hidalgo County, Texas the Chief Information Officer's role is to provide a centralized point of contact for all countywide information systems, infrastructure and application resources. The IT Department provides some level of support to all county departments and because all these resources are interconnected and interdependent, it is the IT Department's role to take the lead on any issue relating to technology and to facilitate any and all resources.

This is the Disaster Recovery Plan for applications, systems and appliances that are critical to the operation of the information technology resources on a county wide level. This plan also identifies departments that run separate yet critical applications and systems.

The County has IT policies in place, which mandate that any department that runs data servers or critical applications keep the application properly backed up and also develop a disaster recovery plan for these applications. Besides the countywide systems maintained by the IT Department and covered in this plan, the following departments maintain data systems:

County Auditor's Office (Appendix A)
SAGE Financial
Miscellaneous department specific applications

Head Start Agency (Appendix B)
Head Start MIS
Miscellaneous department specific applications

Urban County (Appendix C)
Urban County Finance Program
Miscellaneous department specific applications

Tax Assessor Collector (Appendix D)
Automated Tax Collection System
Miscellaneous department specific applications

Health and Human Services Department (Appendix E)
Client/Medical Records System
Miscellaneous department specific applications

Assumption

The Disaster Recovery Plan is built around a "Worst Case" scenario. The "Worst Case" scenario assumes an impact has occurred and access to primary operational facilities is not possible.

Purpose

The plan lists the critical applications, equipment and devices that are critical. It lists response teams, roles and responsibilities, key personnel contact information, task lists, equipment lists , dependencies and recovery time objectives (RTOs)

Plan Overview
Disaster Recovery Plan
6/5/2007

Objective

The primary objectives of the Recovery Plan are to provide a plan of action for Hidalgo County to:
- Identify and respond to the potential disaster through the appropriate contacts.
- Make a management decision whether the situation warrants a disaster declaration.
- Establish recovery procedures and operations of IT at a pre-determined Alternate Facility.
- Restore critical applications and data at a pre-determined Alternate Facility within 72 hours after the declaration of a disaster.

This Plan seeks to minimize:
- The number of decisions that must be made following an outage.
- The dependence on the participation of any specific person or group of people in the recovery process.
- The need to develop, test and debug new procedures, programs or systems during recovery.
- The exposure to Hidalgo County resulting from a disaster impacting their ability to perform their critical business functions.

Strategies Used

The primary and secondary strategies to be applied in the Application Recovery Plan are as follows:

Strategy One - Worst Case:

1. Upon "Disaster Declaration" notification, all Application Recovery Team members will be notified and assembled at a prespecified "Recovery Team" assembly location.
2. Review of critical application RTO and RPO requirements
3. Delegation to Application Recovery Team those task items to be completed based upon extent of impact and variables of situation.
4. Communication with all affected departmental business units, vendors, Command Center, etc.
5. On-going support to all affected departmental areas as long as required until full restoration back to normal operations.

Strategy Two - Application Failure:

1. Upon "Application Failure", work in conjunction with the IT Department to bring back on-line the "most critical" application first.
2. Assist departmental business functions affected by outage with review of data restores, record balancing, record reconciliation, etc

Report Description:

This report lists each task alphabetically with its subtasks. The task will still be listed even if it has no subtasks assigned.

Task ID TSK01
Description Electrical Grid
Task Name Power grid that supplies electricity for county IT distribution facilities.

Subtasks:

Seq #		
1	Electric Grid - Response	Response
2	Electric Grid - Response	Notify response team
3	Electric Grid - Response	Report to site
4	Electric Grid - Response	Contact facilities manager of issue (Buildings and Grounds Department/Daniel Flores 956-318-2646)
5	Electric Grid - Response	Assess damage and possiblity of recovery
6	Electric Grid - Response	Verify that alternate power is on
7	Electric Grid - Response	If alternate power is unavailable begin DRP procedures for affected applications
8	Electric Grid - Response	Begin recovery process
9	Electric Grid - Response	Obtain alternate hardware if necessary
10	Electric Grid - Response	Test application

Task ID TSK02
Description Internet, PRIs and Special Circuits
Task Name Communication lines for Network LAN/WAN

Subtasks:

Seq #		
1	Communicaton - Response	Response
2	Communicaton - Response	Notify response team
3	Communicaton - Response	Report to site
4	Communicaton - Response	Contact vendor of issue
5	Communicaton - Response	Assess damage and possibility of recovery
6	Communicaton - Response	Verify that alternate site is ready
7	Communicaton - Response	Route data to alternate site
8	Communicaton - Response	Begin recovery process
9	Communicaton - Response	Test equipment access to circuit
10	Communicaton - Response	Obtain alternate hardware if necessary
11	Communicaton - Response	Test equipment
12	Communicaton - Response	Bring equipment online

Task ID TSK03
Description Network LAN/WAN
Task Name This encompasses all countywide network and telecommunciation equipment, including routers, switches, firewalls, data circuits, servers and related applications. The network is designed to be modular and a specific site crash will not mean an entire system failure.

Subtasks:

Seq #		
1	Network - Response	Response
2	Network - Response	Notify response team
3	Network - Response	Report to site
4	Network - Response	Contact application vendor of issue
5	Network - Response	Participate in damage assessment
6	Network - Response	If at alternate site, route all data through working infrastructure
7	Network - Response	Verify/Test access to equipment and application
8	Network - Response	Assess damage and possibility of recovery
9	Network - Response	Begin recovery process
10	Network - Response	Obtain alternate hardware if necessary
11	Network - Response	Test equipment for readiness and accuracy
12	Network - Response	Test equipment access to network infrastructure
13	Network - Response	Bring equipment online

Task ID TSK04
Description Tyler Technologies Criminal Justice System (AbleTerm)
Task Name Countywide application, all main infrastructure and equipment hosted at a central site.

Subtasks:

Seq #		
1	Criminal Justice - Response	Response
2	Criminal Justice - Response	Notify response team
3	Criminal Justice - Response	Report to site for instructions
4	Criminal Justice - Response	Contact application vendor of issue.
5	Criminal Justice - Response	Participate in damage assessment
6	Criminal Justice - Response	Verify/Test access to equipment and application
7	Criminal Justice - Response	Assess damage and possibility of recovery
8	Criminal Justice - Response	Begin recovery process
9	Criminal Justice - Response	Obtain backup media from remote site
10	Criminal Justice - Response	Reload data to main or redundant server.
11	Criminal Justice - Response	Obtain alternate hardware if necessary
12	Criminal Justice - Response	Test data for readiness and accuracy
13	Criminal Justice - Response	Test Server access to network infrastrusture
14	Criminal Justice - Response	Bring application server online

Task ID TSK05
Description VOIP County Telephone System (ShoreTel)
Task Name Countywide telephone system, this system is designed in a modular architecture. All geographic sites are independent of each other, yet the system will pool all resources for countywide use. A failure at a site will not constitute a system wide collapse.

Subtasks:

Seq #		
1	Shoretel - Response	Response
2	Shoretel - Response	Notify response team
3	Shoretel - Response	Report to site
4	Shoretel - Response	Contact application vendor of issue
5	Shoretel - Response	Participate in damage assessment
6	Shoretel - Response	If at alternate site, route all telephone traffic thru working infrastructure
7	Shoretel - Response	Verify/Test access to equipment and application
8	Shoretel - Response	Assess damage and possiblity of recovery
9	Shoretel - Response	Begin recovery process
10	Shoretel - Response	Obtain backup media from remote site
11	Shoretel - Response	Obtain alternate hardware if necessary
12	Shoretel - Response	Test equipment for readiness and accuracy
13	Shoretel - Response	Test equipment access to network infrastructure
14	Shoretel - Response	Bring application server online

Task ID TSK06
Description SAGE Financial
Task Name This is the countywide financial system application. It hosts the Financial Administration, Human Resources/Payroll and Purchasing modules.

Subtasks:

Seq #		
1	Sage - Response	Response
2	Sage - Response	Notify response team
3	Refer to Auditor's Office Disaster Recovery Plan (Appendix A)	(Appendix A)

Task ID TSK07
Description DataNAS
Task Name Central data file server for the users of the county. All user work documents and application backup data is stored on these servers. Currently there are two of these servers.

Subtasks:

Seq #		
1	DataNAS - Response	Response
2	DataNAS - Response	Notify response team
3	DataNAS - Response	Report to site
4	DataNAS - Response	Contact application vendor of issue
5	DataNAS - Response	Participate in damage assessment
6	DataNAS - Response	Verify/Test access to equipment and application
7	DataNAS - Response	Assess damage and possiblity of recovery
8	DataNAS - Response	Begin recovery process
9	DataNAS - Response	Obtain backup media from remote site
10	DataNAS - Response	Obtain alternate hardware if necessary
11	DataNAS - Response	Test equipment for readiness and accuracy
12	DataNAS - Response	Test equipment access to network infrastructure
13	DataNAS - Response	Bring application server online

Task ID TSK08
Description Web Services
Task Name Countywide web servers and applications.

Subtasks:

Seq #		
1	Web - Response	Response
2	Web - Response	Notify response team
3	Web - Response	Contact application vendor of issue
4	Web - Response	Participate in damage assessment
5	Web - Response	Verify/Test access to equipment and application
6	Web - Response	Assess damage possibility and recovery
7	Web - Response	Begin recovery process
8	Web - Response	Obtain backup media from remote site
9	Web - Response	Obtain alternate hardware if necessary
10	Web - Response	Test equipment for readiness and accuracy
11	Web - Response	Test equipment access to network infrastructure
12	Web - Response	Bring application server online

Task ID TSK09
Description Email Services
Task Name Countywide email services

Subtasks:

Seq #		
1	Email - Response	Response
2	Email - Response	Notify response team
3	Email - Response	Contact application vendor of issue
4	Email - Response	Participate in damage assessment
5	Email - Response	Verify/Test access to equipment and application
6	Email - Response	Assess damage possibility and recovery
7	Email - Response	Begin recovery process
8	EMail - Response	Obtain backup media from remote site
9	Email - Response	Obtain alternate hardware if necessary
10	Email - Response	Test equipment for readiness and accuracy
11	Email - Response	Test equipment access to network infrastructure
12	Email - Response	Bring application server online

Task ID TSK10
Description BAAP
Task Name Budget Request Application is a stand alone client based application.

Subtasks:

Seq #		
1	BAAP - Response	Notify response team
2	BAAP - Response	Begin recovery process
3	BAAP - Response	Obtain backup media from remote site
4	BAAP - Response	Reload data on client
5	BAAP - Response	Test data for accuracy
6	BAAP - Response	Bring application online

Task ID TSK11
Description TAAP
Task Name Time and Attendance Application: Is a countywide application hosted off a central server. This application works in conjunction with the SAGE Financial application. A disruption in the SAGE application will directly affect TAAP.

Subtasks:

Seq #		
1	TAAP - Response	Response
2	TAAP - Response	Notify response team
3	TAAP - Response	Report to site
4	TAAP - Response	Contact application vendor of issue
5	TAAP - Response	Participate in damage assessment
6	TAAP - Response	Verify/Test access to equipment and application
7	TAAP - Response	Assess damage and possibility of recovery
8	TAAP - Response	Begin recovery process
9	TAAP - Response	Obtain backup media from remote site
10	TAAP - Response	Obtain alternate hardware if necessary
11	TAAP - Response	Test equipment for readiness and accuracy
12	TAAP - Response	Test peripheral equipment communication
13	TAAP - Response	Test equipment access to network infrastructure
14	TAAP - Response	Bring application server online

Task ID TSK12
Description Head Start Family Information System (HSFIS)
Task Name is a data collection system used to track all family and child information.

Subtasks:

Seq #		
1	HSFIS - Restoration	Response
2	HSFIS - Response	Notify response team
3	Refer to Head Start Program Disaster Recovery Plan (Appendix B)	(Appendix B)

Task ID TSK13
Description Urban County Finance Program
Task Name Urban County financial system application.

Subtasks:

Seq #		
1	Urban County - Response	Response
2	Urban County - Response	Notify response team
3	Refer to Urban County Disaster Recovery Plan (Appendix C)	(Appendix C)

Task ID TSK14
Description Automated Tax Collection System
Task Name Tax Collection System

Subtasks:

Seq #		
1	Tax - Response	Response
2	Tax - Response	Notify response team
3	Refer to Tax Office Standard Operation Procedure (Appendix D)	(Appendix D)

Task ID	TSK15
Description	Health Dept. Systems
Task Name	Health Department Medical/Client Record System - TWICES System (Client record system) - SDI System (Medical Billing System)

Subtasks:

Seq #		
1	Health - Response	Response
2	Health - Response	Notify response team
3	Refer to Health Department Disaster Recovery Plan (Appendix E)	(Appendix E)

Plan Personnel Contact Directory

Disaster Recovery Plan

6/5/2007

Report Description:
This report lists the numbers and email addresses for each person assigned to this plan organized by person name.

Employees:

Vivian Barrera	*Title*	Technician II
	Work Phone	956-292-7010
	Work Phone Extension	6002
	Work Email	vivian@co.hidalgo.tx.us
	Cell Phone	956-566-9891
	Home Email	viv1372@yahoo.com
Juan Deleon	*Title*	Technician IV
	Work Phone	956-292-7010
	Work Phone Extension	6004
	Work Email	juan@co.hidalgo.tx.us
	Home Phone	956-207-9204
	Pager	956-268-0139
Ruben Flores	*Title*	Admin Asst I
	Work Phone	956-292-7010
	Work Phone Extension	6018
	Work Email	ruben.flores@co.hidalgo.tx.us
	Home Phone	956-605-8175
Carlos Garcia	*Title*	Technician V
	Work Phone	956-292-7010
	Work Phone Extension	6008
	Work Email	charlie@co.hidalgo.tx.us
	Home Phone	956-207-9397
	Pager	956-268-0149
Maria Gonzalez	*Title*	Technician III
	Work Phone	956-292-7010
	Work Phone Extension	6013
	Work Email	maria.gonzalez@co.hidalgo.tx.us
	Cell Phone	956-650-9014
	Home Phone	956-650-9641
	Home Email	mgonz_7@yahoo.com
	Pager	956-286-0160
Charles Graham	*Title*	Application Developer II
	Work Phone	956-292-7010
	Work Phone Extension	6010
	Work Email	charles.graham@co.hidalgo.tx.us
	Cell Phone	956-884-1138
	Pager	956-268-0236
Luis Izaguirre	*Title*	Technician I
	Work Phone	956-292-7010
	Work Phone Extension	6015
	Work Email	luis.izaguirre@co.hidalgo.tx.us
	Cell Phone	956-522-7112
	Home Phone	956-581-1216
	Home Email	lisag_79@hotmail.com
	Pager	956-268-0139

Employees:		
Edna Kirby	*Title*	Technical Assistant
	Work Phone	956-292-7010
	Work Phone Extension	6017
	Work Email	edna.kirby@co.hidalgo.tx.us
Lisette Parker	*Title*	Technical Assistant
	Work Phone	956-292-7010
	Work Phone Extension	6014
	Work Email	lisette.parker@co.hidalgo.tx.us
	Cell Phone	956-222-4988
	Home Email	lisette.parker@msn.com
	Pager	956-268-0144
Cruz Quintana	*Title*	Telecomm Manager
	Work Phone	956-292-7000
	Work Phone Extension	6006
	Work Email	cruz.quintana@co.hidalgo.tx.us
	Cell Phone	956-784-2062
	Home Phone	956-207-9941
	Pager	956-268-0151
Renan Ramirez	*Title*	Chief Information Officer
	Work Phone	956-292-7010
	Work Phone Extension	6011
	Work Email	renan@co.hidalgo.tx.us
	Cell Phone	956-457-0792
	Home Phone	956-289-7444
	Home Email	renanville@yahoo.com
	Pager	956-268-0111
Stan Ramos	*Title*	Technician III
	Work Phone	956-292-7010
	Work Phone Extension	6005
	Work Email	stan.ramos@co.hidalgo.tx.us
	Cell Phone	956-454-5724
	Home Phone	956-383-0577
	Pager	956-268-0038
Oralia Regino	*Title*	Application Developer II
	Work Phone	956-292-7010
	Work Phone Extension	6009
	Work Email	oralia.regino@co.hidalgo.tx.us
	Home Phone	956-618-3909
	Home Email	o_bermudez@yahoo.com
	Pager	956-268-0104
Mike Robledo	*Title*	Info System Admin
	Work Phone	956-292-7010
	Work Phone Extension	6012
	Work Email	mike@co.hidalgo.tx.us
	Pager	956-268-0067

Employees:

Griselda Salazar	*Title*	Admin Asst II
	Work Phone	956-292-7010
	Work Phone Extension	6001
	Work Email	gris.salazar@co.hidalgo.tx.us
	Cell Phone	956-457-2356
	Home Phone	956-624-5126
	Home Email	grisslzr@yahoo.com
Carlos Trevino	*Title*	Multimedia Coordinator
	Work Phone	956-292-7010
	Work Phone Extension	6019
	Work Email	carlos.trevino@co.hidalgo.tx.us
	Cell Phone	714-809-4800
	Home Email	jcarlost@aol.com
	Pager	956-268-0014
Nazleth Vela	*Title*	Technician II
	Work Phone	956-292-7010
	Work Phone Extension	6007
	Work Email	nazleth.vela@co.hidalgo.tx.us
	Pager	956-268-5591

Customer Reps:

Hidalgo County Judge		
Juan D. Salinas	*Title*	Hidalgo County Judge
	Work Phone	956-318-2600
	Work Fax	956-318-2699
Commissioner Precinct 1		
Sylvia Handy	*Title*	Commissioner
	Work Phone	956-968-8733
	Work Fax	956-968-1417
Commissioner Precinct 2		
Hector 'Tito' Palacios	*Title*	Commissioner
	Work Phone	956-787-1891
	Work Fax	956-787-4683
Commissioner Precinct 3		
Joe M. Flores	*Title*	Commissioner
	Work Phone	956-585-2375
	Work Fax	956-585-2375
Commissioner Precinct 4		
Oscar Garza Jr.	*Title*	Commissioner
	Work Phone	956-383-3112
	Work Fax	956-381-5905

Customer Reps:

Justice of the Peace - Pct.1		
Gilbert Saenz	*Title*	Judge
	Work Phone	956-447-3995
	Work Fax	956-447-9522
Jesus Morales	*Title*	Judge
	Work Phone	956-447-3995
	Work Fax	956-447-9522
Justice of the Peace - Pct.2		
Bobby Contreras	*Title*	Judge
	Work Phone	956-687-5088
	Work Fax	956-687-4990
Rosa Trevino	*Title*	Judge
	Work Phone	956-687-5088
	Work Fax	956-687-4990
Justice of the Peace - Pct. 3		
Luis Garza	*Title*	Judge
	Work Phone	956-519-8422
	Work Fax	956-519-1796
Ismael Ochoa	*Title*	Judge
	Work Phone	956-519-8422
	Work Fax	956-519-1796
Justice of the Peace - Pct. 4		
Charlie Espinoza	*Title*	Judge
	Work Phone	956-380-4473
	Work Fax	956-380-4029
Mary Alice Palacios	*Title*	Judge
	Work Phone	956-380-4473
	Work Fax	956-380-4029
Justice of the Peace - Pct. 5		
E. Speedy Jackson	*Title*	Judge
	Work Phone	956-262-3300
	Work Fax	956-262-4413
Constable - Pct. 1		
Celestino Avila Jr.	*Title*	Constable
	Work Phone	956-447-3775
	Work Fax	956-447-8614
Constable - Pct. 2		
Gilbert Alaniz	*Title*	Constable
	Work Phone	956-783-4664
	Work Fax	956-783-4664

Customer Reps:		
Constable - Pct. 3		
Lazaro Gallardo Jr.	*Title*	Constable
	Work Phone	956-581-6800
	Work Fax	956-519-4245
Constable - Pct. 4		
Andres 'Andy' Rios	*Title*	Constable
	Work Phone	956-383-8560
	Work Fax	956-383-8565
Constable - Pct. 5		
Eduardo 'Walo' Bazan	*Title*	Constable
	Work Phone	956-262-4200
	Work Fax	956-262-2919
County Court Law 1		
Rodolfo Gonzalez	*Title*	Judge
	Work Phone	956-318-2375
	Work Fax	956-318-2373
County Court Law 2		
Jaime Palacios	*Title*	Judge
	Work Phone	956-318-2380
	Work Fax	956-318-2384
County Court Law 4		
Fred Garza, Jr.	*Title*	Judge
	Work Phone	956-318-2390
	Work Fax	956-318-2396
County Court Law 5		
Arnaldo Cantu	*Title*	Judge
	Work Phone	956-318-2460
	Work Fax	956-318-2463
County Court Law 6		
Albert Garcia	*Title*	Judge
	Work Phone	956-289-7400
Criminal Auxiliary Court A		
Homer Salinas	*Title*	Judge
	Work Phone	956-289-7420
	Work Fax	956-289-7429
Criminal Auxiliary Court B		
Fidencio Guerra	*Title*	Judge
	Work Phone	956-318-2362

Customer Reps:

Master Court 1		
J.M Ramirez	*Title*	Judge
	Work Phone	956-318-2398
	Work Fax	956-318-2455
Master Court 2		
Maria Socorro Leos	*Title*	Judge
	Work Phone	956-318-2452
	Work Fax	956-318-2454
Child Protective Court		
Ricardo Flores	*Title*	Judge
	Work Phone	956-318-2672
Juvenile Justice Court		
Maxine L. Longoria	*Title*	Judge
	Work Phone	956-381-0744
	Work Fax	956-381-0730
Adult Probation		
Joe Lopez	*Title*	Director
	Work Phone	956-661-4600
	Work Fax	956-661-4700
Auto License		
Arnaldo Morin	*Work Phone*	956-318-2158
	Work Fax	956-318-2191
Boot Camp		
Homer Salinas	*Title*	Judge
	Work Phone	956-380-3311
	Work Fax	956-380-3324
Budget Office		
Valde Guerra	*Title*	Budget Officer
	Work Phone	956-292-7025
	Work Fax	956-292-7034
Building and Grounds		
Daniel Flores	*Title*	Director
	Work Phone	956-318-2646
	Work Fax	956-318-2648
Auditor's Office		
Ray Eufracio	*Title*	County Auditor
	Work Phone	956-318-2511
	Work Fax	956-318-2577

Customer Reps:		
County Clerk		
Arturo Guajardo, Jr.	*Title*	County Clerk
	Work Phone	956-318-2100
	Work Fax	956-318-2105
Law Library		
Angie Z. Chapa	*Title*	Law Librarian
	Work Phone	956-318-2155
	Work Fax	956-381-4269
District Clerk		
Laura Hinojosa	*Title*	District Clerk
	Work Phone	956-318-2200
	Work Fax	956-318-2251
Drainage District		
Godfrey Garza, Jr.	*Title*	District Manager
	Work Phone	956-292-7080
	Work Fax	956-292-7089
Elections		
Teresa R. Navarro	*Title*	Elections Administrator
	Work Phone	956-318-2570
	Work Fax	956-318-2569
Fire Department		
Victor Fonseca, Jr.	*Title*	Fire Marshall
	Work Phone	956-318-2656
	Work Fax	956-318-2697
Human Resources/Civil Service		
Esther A. Cortez	*Title*	Director
	Work Phone	956-318-2660
	Work Fax	956-318-2669
Indigent Defense		
Isidro 'Sid' Sepulveda	*Title*	Director
	Work Phone	956-318-2367
	Work Fax	956-318-2893
Urban County		
Diana Serna	*Title*	Executive Director
	Work Phone	956-787-8127
Jaime Ortega	*Title*	Facility Coordinator
	Work Phone	956-787-8127
Maribel Lopez	*Title*	Network Coordinator
	Work Phone	956-787-8127
Nydia Vega	*Title*	Administrative Coordinator
	Work Phone	956-787-8127

Customer Reps:

Tax Office

Armando Barrera	*Title*	Tax Assessor Collector
	Work Phone	956-318-2157
Fernando Cantu	*Title*	Account Reports Specialist
	Work Phone	956-318-2157

Health Department

Eduardo Olivarez	*Title*	Chief Admin. Officer
Rigo Hinojosa		

Vendor Reps:

Total Technologies

John Mathis		
	Title	President
	Work Phone	281-448-7676
	Email	mmurphy@totaltec.com
Lee Warren		
	Work Phone	281-448-7676
Kelly Green		
	Work Phone	281-448-7676

Information Design, Inc.

John Green		
	Work Phone	303 792- 2990
Jim Grimm		
	Work Phone	303-792-2990

Calence

Cathi Whelan		
	Work Phone	512-691-2043

Lava Concepts

Technical Support		
	Work Phone	956-648-9559

County Information Resources Agency - CIRA

Gayle Latham		
	Work Phone	512-478-8753

Tyler Technologies

Dawson Tyler		
	Work Phone	469-585-8361

Vendor Reps.		
IPSwitch Technical Support		
	Work Phone	706-312-3500
Dell Customer Support		
	Work Phone	1800-981-3355
AT&T Customer Service		
	Work Phone	1800-332-4387
Reliant Energy Yesenia Zamarron		
	Work Phone	713-497-3082
Excel Meridian - Technical Support Technical Support		
	Work Phone	1800-995-1014

Report Description:
This report lists all the characteristics of every Application organized by application name.

Budget Application Program

Application Profile

Application ID	APP0000016
Application Name	Budget Application Program
Description	Budget Application Program (BAP)- Budget Preparation
Business Function	Budget Preparation
Application Type	Departmental
Application Owner	Oralia Regino (EMP0000004)
BIA Last Updated	5/14/2007 12:00:00PM

Application Characteristics

Operating System	Window XP
Program Languages	Visual Basic for Applications
Desktop Data Storage	C:\Budget Backup\

Application Configuration

Backup Detail

Application Backup	Daily

Enterprise Recovery Information

Criminal Justice Information System (AbleTerm)

Application Profile

Application ID	APP0000002
Application Name	Criminal Justice Information System (AbleTerm)
Description	County wide application, all main infrastructure and equipment hosted at a central site.
Business Function	Criminal Tracking System
Application Type	Departmental
Application Owner	Vivian Barrera (EMP0000015)

Application Characteristics

Application Configuration

Backup Detail

Application Backup	Nightly - Data Center

Enterprise Recovery Information

DataNAS - 10.1.1.150

Application Profile

Application ID	APP0000019
Application Name	DataNAS - 10.1.1.150
Description	Network storage server for County Clerks.
Business Function	Data Storage
Application Type	Enterprise
Application Owner	Juan Deleon (EMP0000008)
Vendor Org	Tyler Technologies (VND0000007)
BIA Last Updated	5/17/2007 12:00:00PM

Application Characteristics

Operating System	Proprietary
Location	Hidalgo County Courthouse (LOC0000001)
Desktop Data Storage	na
External File Requirements	na

Application Configuration

IP Address/Range	10.1.1.150
Data Sensitivity	Highly Sensitive-Customer

Backup Detail

Application Backup	Daily
Backup Source Code	Nightly - Data Center
Backup Type	Raw Data
Media	Cartridge Tape
Backup Frequency	Daily Incremental, Weekly Full
Schedule	Yes

Enterprise Recovery Information

Internal Vendor	Juan Deleon (EMP0000008)
RPO (Hours)	24.00
RTO (Hours)	24.00

DataNAS - 10.1.1.200

Application Profile

Application ID	APP0000024
Application Name	DataNAS - 10.1.1.200
Description	Network storage server for Hidalgo County
Business Function	Data Storage
Application Type	Enterprise
Application Owner	Stan Ramos (EMP0000005)
Vendor Org	Excel Meridian - Technical Support (VND0000013)
BIA Last Updated	5/14/2007 12:00:00PM

Application Characteristics

Operating System	Proprietary
Location	Hidalgo County Courthouse (LOC0000001)
Desktop Data Storage	na
External File Requirements	na

Application Configuration

License Req's	1CH40915
IP Address/Range	10.1.1.200
Data Sensitivity	Highly Sensitive-Customer

Backup Detail

Backup Available	Yes
Application Backup	Weekly
Backup Source Code	N/A
Backup Type	Raw Data
Media	Data Cartrige
Backup Frequency	Weekly Full
Schedule	Yes
Backup Password	Yes

Enterprise Recovery Information

Internal Vendor	Stan Ramos (EMP0000005)
RPO (Hours)	24.00
RTO (Hours)	24.00

Electrical Grid

Application Profile

Application ID	APP0000021
Application Name	Electrical Grid
Description	Power grid that supplies electricity for county IT distribution facilities.
Application Type	Enterprise
Application Owner	Renan Ramirez (EXEC000001)

Application Characteristics

Application Configuration

Backup Detail

Enterprise Recovery Information

Head Start Family Information System

Application Profile

Application ID	APP0000023
Application Name	Head Start Family Information System
Description	is a data collection system used to track all family and child information
Application Type	Departmental

Application Characteristics

Application Configuration

Backup Detail

Enterprise Recovery Information

IMail - Services

Application Profile

Application ID	APP0000018
Application Name	IMail - Services
Description	Sharing of Calendar
Business Function	Email Services
Application Type	Enterprise
Application Owner	Carlos Garcia (EMP0000007)
Vendor Org	IPSwitch (VND0000008)

Application Characteristics

Operating System	Microsoft Windows 2000 Server
Location	Hidalgo County Administration Bldg. (LOC0000004)
Internet Accessible	Yes
Can Co-Exist	Yes

Application Configuration

License Req's	SL4-0000183154
Protocol Req's	TCP/IP, SMTP, POP
Port Req's	80, 110, 25, 443
IP Address/Range	68.88.107.134, 68.88.107.135
Data Sensitivity	Highly Sensitive-Customer
Min. Client Req's	MS Internet Explorer, Outlook Express, Outlook

Backup Detail

Backup Available	Yes
Backup Type	Raw Data
Media	Disk Drive
Backup Frequency	Other

Enterprise Recovery Information

Internet, PRIs and Special Circuits

Application Profile

Application ID	APP0000020
Application Name	Internet, PRIs and Special Circuits
Description	Communication lines for Network LAN/WAN
Application Type	Enterprise
Application Owner	Renan Ramirez (EXEC000001)

Application Characteristics

Application Configuration

Backup Detail

Enterprise Recovery Information

Network LAN/WAN

Application Profile

Application ID	APP0000015
Application Name	Network LAN/WAN
Description	Countywide network and telecommunication
Business Function	Provide access to network resources.
Application Type	Enterprise
Application Owner	Juan Deleon (EMP0000008)
Vendor Org	Calence (VND0000001)
BIA Last Updated	5/17/2007 12:00:00PM

Application Characteristics

Operating System	Cisco ISO
Program Languages	NA
Location	Hidalgo County Courthouse (LOC0000001)
Desktop Data Storage	NA
External File Requirements	NA

Application Configuration

Protocol Req's	All protocols
Port Req's	10/100 ports
IP Address/Range	10.100.101.1 -10.100.146.254
Known Bottlenecks	Users

Backup Detail

Backup Available	Yes
Backup Password	Yes

Enterprise Recovery Information

External Vendor	Calence (VND0000001)
Internal Vendor	Juan Deleon (EMP0000008)
RPO (Hours)	4.00
RTO (Hours)	4.00

Sage Financial

Application Profile

Application ID	APP0000003
Application Name	Sage Financial
Description	The SAGE system is the county's financial application system.
Business Function	Financial System
Application Type	Departmental
Application Owner	Renan Ramirez (EXEC000001)

Application Characteristics

Application Configuration

Backup Detail

Backup Available	Yes
Application Backup	Nightly - Data Center
Backup Source Code	Nightly - Data Center

Enterprise Recovery Information

External Vendor	Information Design, Inc. (VND0000003)

Time & Attendance Program

Application Profile

Application ID	APP0000014
Application Name	Time & Attendance Program
Description	Hidalgo County's Time and Attendance Program (TAAP)
Business Function	Time and Attendance
Application Type	Departmental
Application Owner	Charles Graham (EMP0000013)
Vendor Org	Lava Concepts (VND0000005)
BIA Last Updated	5/17/2007 12:00:00PM

Application Characteristics

Operating System	Windows 2000
Program Languages	C Sharp
Location	Hidalgo County Administration Bldg. (LOC0000004)
Internet Accessible	Yes
Can Co-Exist	Yes
Desktop Data Storage	40mb
External File Requirements	n/a

Application Configuration

Storage Req's	n/a
License Req's	n/a
Protocol Req's	tcp/ip
Port Req's	80
IP Address/Range	10.100.100.x
Data Sensitivity	Internal Use Only
Min. Client Req's	0
Encryption Req's	0
Third Party Req's	0

Backup Detail

Backup Available	Yes
Application Backup	Nightly - Data Center
Backup Type	Raw Data
Media	Disk Drive
Backup Frequency	Daily Full
Schedule	Yes

Enterprise Recovery Information

External Vendor	Lava Concepts (VND0000005)
Internal Vendor	Charles Graham (EMP0000013)
RPO (Hours)	12.00
RTO (Hours)	24.00

VOIP Telephone System (ShoreTel)

Application Profile

Application ID	APP0000001
Application Name	VOIP Telephone System (ShoreTel)
Description	Converged voice and data network county wide.
Business Function	County wide Telecom System
Application Type	Enterprise
Application Owner	Cruz Quintana (EMP0000009)
Vendor Org	Total Technologies (VND0000002)
BIA Last Updated	4/28/2007 12:00:00PM

Application Characteristics

Operating System	N/A
Program Languages	N/a
Location	Hidalgo County Courthouse (LOC0000001)
Internet Accessible	Yes

Application Configuration

Storage Req's	80 Gigs
Seats/Units	5
License Req's	Main, remotes, sites, phones, auxillary software
Protocol Req's	TCP/IP, UDP
Network Req's	10/100 Prioritized
Port Req's	random
IP Address/Range	10.2.1.2 - 10.2.1.25
Data Sensitivity	Internal Use Only
Known Bottlenecks	Core & WAN
Batch Processing	N/A

Backup Detail

Backup Available	Yes
Application Backup	Weekly
Backup Source Code	N/A
Backup Type	Raw Data
Media	Disk Drive
Backup Frequency	Weekly Full
Automated Backups	Yes
Backup Password	Yes

Enterprise Recovery Information

External Vendor	Total Technologies (VND0000002)
Internal Vendor	Cruz Quintana (EMP0000009)
RPO (Hours)	0.10
Priority Sequence	1

Web - Services

Application Profile

Application ID	APP0000012
Application Name	Web - Services
Description	County Websites & Judicial Search
Business Function	County Wide
Application Type	Departmental
Application Owner	Carlos Garcia (EMP0000007)
Vendor Org	Dell (VND0000009)

Application Characteristics

Operating System	Microsoft Windows 2000 Server
Location	Hidalgo County Administration Bldg. (LOC0000004)
Internet Accessible	Yes
Can Co-Exist	Yes

Application Configuration

Protocol Req's	TCP/IP
Port Req's	80, 443
IP Address/Range	68.88.107.133
Data Sensitivity	Highly Sensitive-Customer
Min. Client Req's	Microsoft Internet Explorer

Backup Detail

Backup Available	Yes
Backup Type	Raw Data
Media	Disk Drive

Enterprise Recovery Information

Report Description:
This report lists all the characteristics of every Location record organized by its geography.

Country: United States
State/Province: Texas
City: Edinburg

Site Name: Administration Bldg Annex (KMart)

Location ID	LOC0000006
Address 1	2802 S. Closner Blvd.
Normal Function	Office Area
Work Area Recovery	✓
Data Center	✓
Ops Center	✓

Core Component/Plan Specific Information

General Plan Segment

Site Name: Hidalgo County Administration Bldg

Location ID	LOC0000004
Address 1	100 E. Cano 2nd Floor
Normal Function	Office Area
Site Control	Public Access
Data Center	✓

Core Component/Plan Specific Information

General Plan Segment

Site Name: Hidalgo County Courthouse

Location ID	LOC0000001
Address 1	Hidalgo County Courthouse 1st Floor
Address 2	100 N. Closner Blvd.
Main Phone Number	956-292-7010
Room Or Area ID	IT Department
Normal Function	Network Ops Center
Site Control	Public Access
Number of Personnel	16
Site Contact	EXEC000001, Ramirez ,Renan
Work Area Recovery	✓
Command Control Center	✓
Data Center	✓
Non Data Storage	✓
Ops Center	✓
Digital Media Storage	✓
Additional Details	Main Network Ops

Core Component/Plan Specific Information

General Plan Segment

Alternate Site in Plan Details
Disaster Recovery Plan
6/5/2007

Country: United States
State/Province: Texas
City: Mission

Site Name: Commissioner PCT 3

Location ID	LOC0000005
Address 1	724 North Breyfogle Road
Main Phone Number	956-585-4509
Normal Function	Network Ops Center
Site Control	Public Access
Work Area Recovery	✓
Command Control Center	✓
Additional Details	Alternative Location #1

Core Component/Plan Specific Information

General Plan Segment

City: Weslaco

Site Name: Commissioner PCT 1

Location ID	LOC0000003
Address 1	1902 Joe Stephens Ave.
Main Phone Number	956-968-8733
Normal Function	Network Ops Center
Work Area Recovery	✓
Command Control Center	✓
Additional Details	Alternative Site #2

Core Component/Plan Specific Information

General Plan Segment

Report Description:
This report shows how people are organized to execute their plan (e.g.Teams. Positions on Teams, and who's assigned to fill each position, including employees, vendor and customer representatives.)

General Recovery

Network LAN/WAN Support Team

Coordinate the activities required to restore and recover the server systems, utility, application software and data at the Alternate Facility.

Team Leader
Network LAN/WAN Support Team - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
Network LAN/WAN Support Team - Team Leader Alternate
Mike Robledo, Info System Admin

Team Member
Network LAN/WAN Support Team - Team Member
Carlos Garcia, Technician V
Juan Deleon, Technician IV
Cruz Quintana, Telecomm Manager

DataNAS Recovery Team

Central Data File servers for the users of the county

Team Leader
DataNAS - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
DataNAS - Team Leader Alternate
Mike Robledo, Info System Admin

Team Member
DataNAS - Team Member
Stan Ramos, Technician III
Carlos Garcia, Technician V

Criminal Justice Recovery Team

Criminal Justice System (AbleTerm)

Team Lead
Criminal Justice Recovery - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
Criminal Justice Recovery - Team Leader Alternate
Mike Robledo, Info System Admin

Team Member
Criminal Justice Recovery - Team Member
Vivian Barrera, Technician II

Sage Financial

County wide financial system application

Sage Financial

County wide financial system application

Team Leader
Sage Financial - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
Sage Financial - Team Leader Alternate
Charles Graham, Application Developer II

VOIP Telephone System (ShoreTel)

County wide telephone system, this system is designed in a modular architecture

Team Leader
Shoretel Recovery - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
Shoretel Recovery - Team Leader Alternate
Stan Ramos, Technician III

Team Member
Shoretel Recovery - Team Member
Juan Deleon, Technician IV
Charles Graham, Application Developer II

TAAP

Time Attendance Application Program

Team Leader
TAAP - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
TAAP - Team Leader Alternate
Mike Robledo, Info System Admin

Team Member
TAAP - Team Member
Oralia Regino, Application Developer II
Charles Graham, Application Developer II

BAP

Budget Application Program

Team Leader
BAP - Team Leader
Renan Ramirez, Chief Information Officer

Team Leader - Alt
BAP - Team Leader Alternate
Mike Robledo, Info System Admin

BAP

Budget Application Program

Team Member

BAP - Team Member

Oralia Regino, Application Developer II

Charles Graham, Application Developer II

IMail - Services

County wide email services

Team Leader

Email - Team Leader

Renan Ramirez, Chief Information Officer

Team Leader - Alt

Email - Team Leader Alternate

Carlos Garcia, Technician V

Web Services

County wide web servers and applications

Team Leader

Web Services - Team Leader

Renan Ramirez, Chief Information Officer

Team Leader - Alt

Web Services - Team Leader Alternate

Carlos Garcia, Technician V

Internet, PRIs and Special Circuits

Communication lines for Network LAN/WAN

Team Leader

Internet, PRI - Team Leader

Renan Ramirez, Chief Information Officer

Team Leader - Alt

Internet, PRI - Team Leader Alternate

Carlos Garcia, Technician V

Team Member

Internet, PRI - Team Member

Juan Deleon, Technician IV

Cruz Quintana, Telecomm Manager

Electrical Grid

Power Failure

Team Leader

Electrical Grid - Team Leader

Renan Ramirez, Chief Information Officer

Team Leader - Alt

Electrical Grid - Team Leader Alternate

Daniel Flores, Building and Grounds

Electrical Grid

Power Failure

Team Member
Electrical Grid - Team Member
Carlos Garcia, Technician V

Urban County Finance Program

Finance system

Team Leader - Alt
Urban County - Facility Coordinator
Jaime Ortega, Urban County

Team Leader
Urban County - Recovery Manager
Diana Serna, Urban County

Team Member
Urban County - Network Coordinator
Maribel Lopez, Urban County

Team Administrator
Urban County - Administrative Coordinator
Nydia Vega, Urban County

Automated Tax Collection System

Tax Collection System

Team Leader
Tax - Team Leader
Armando Barrera, Tax Office

Team Leader - Alt
Tax - Team Leader Alternate
Fernando Cantu, Tax Office

Health Dept. Systems

Health Dept. Client/Medical Records System

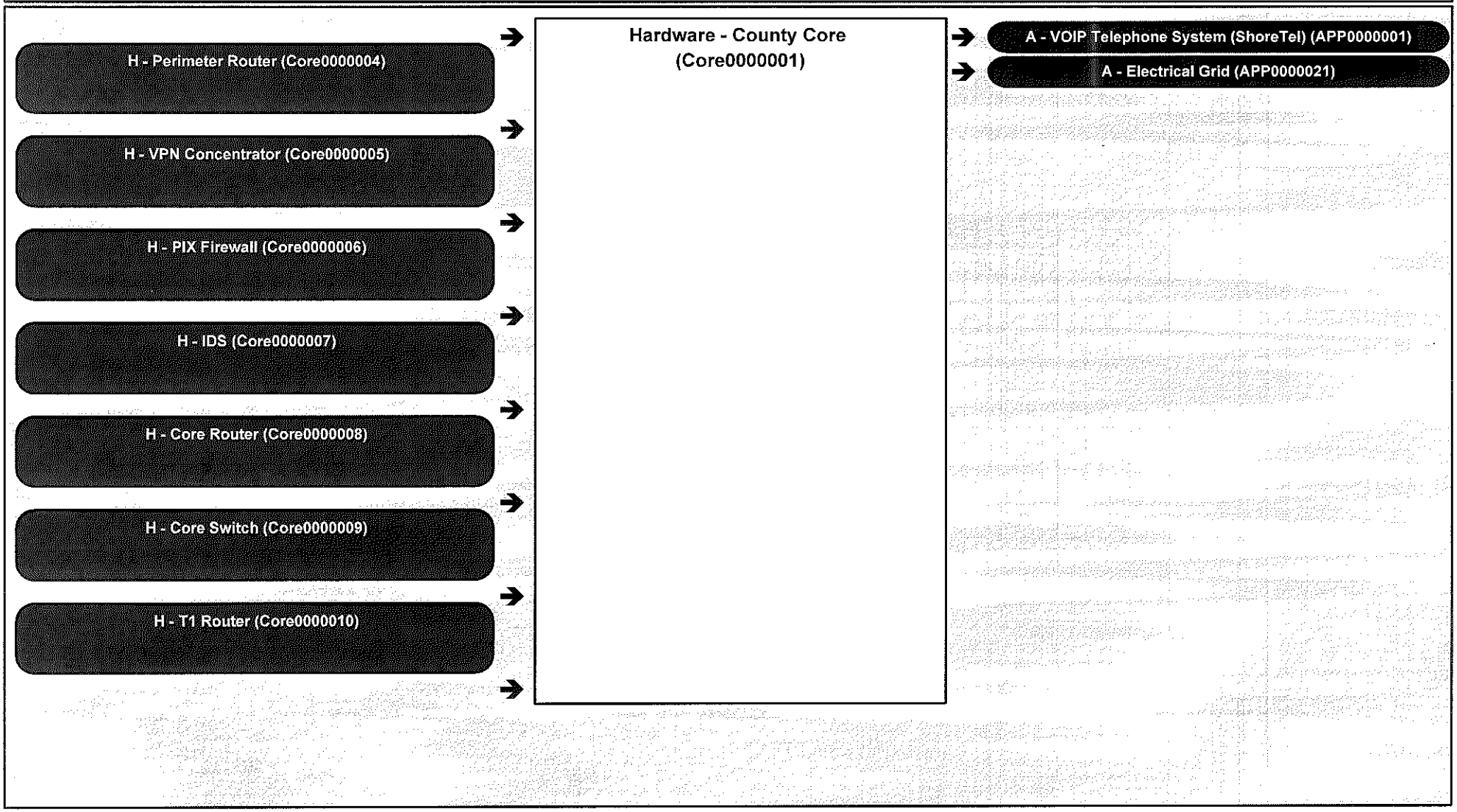
Team Leader
Health - Team Leader
Eduardo Olivarez, Health Department

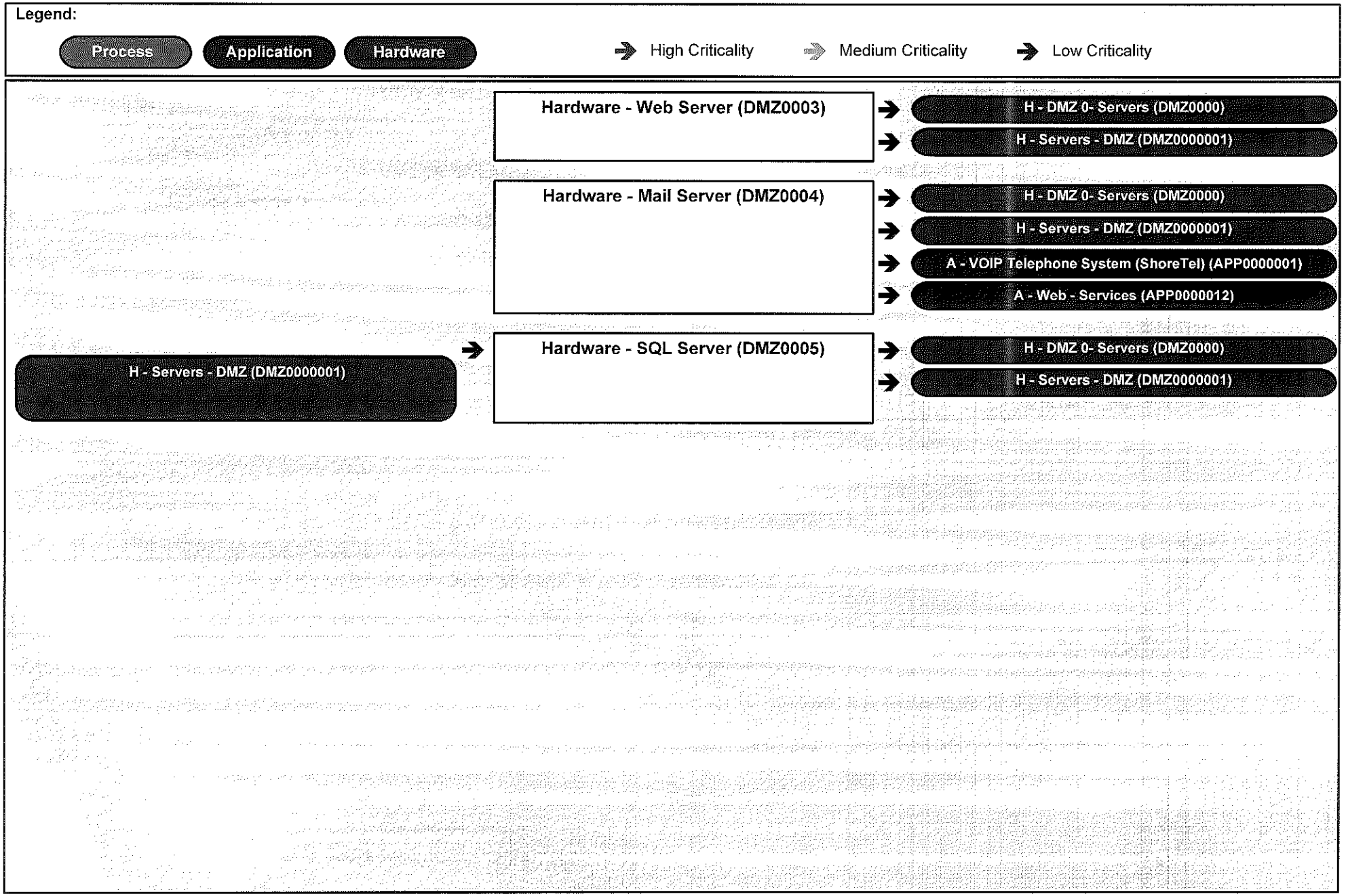
Team Leader Alt
Health - Team Leader Alternate
Rigo Hinojosa, Health Department

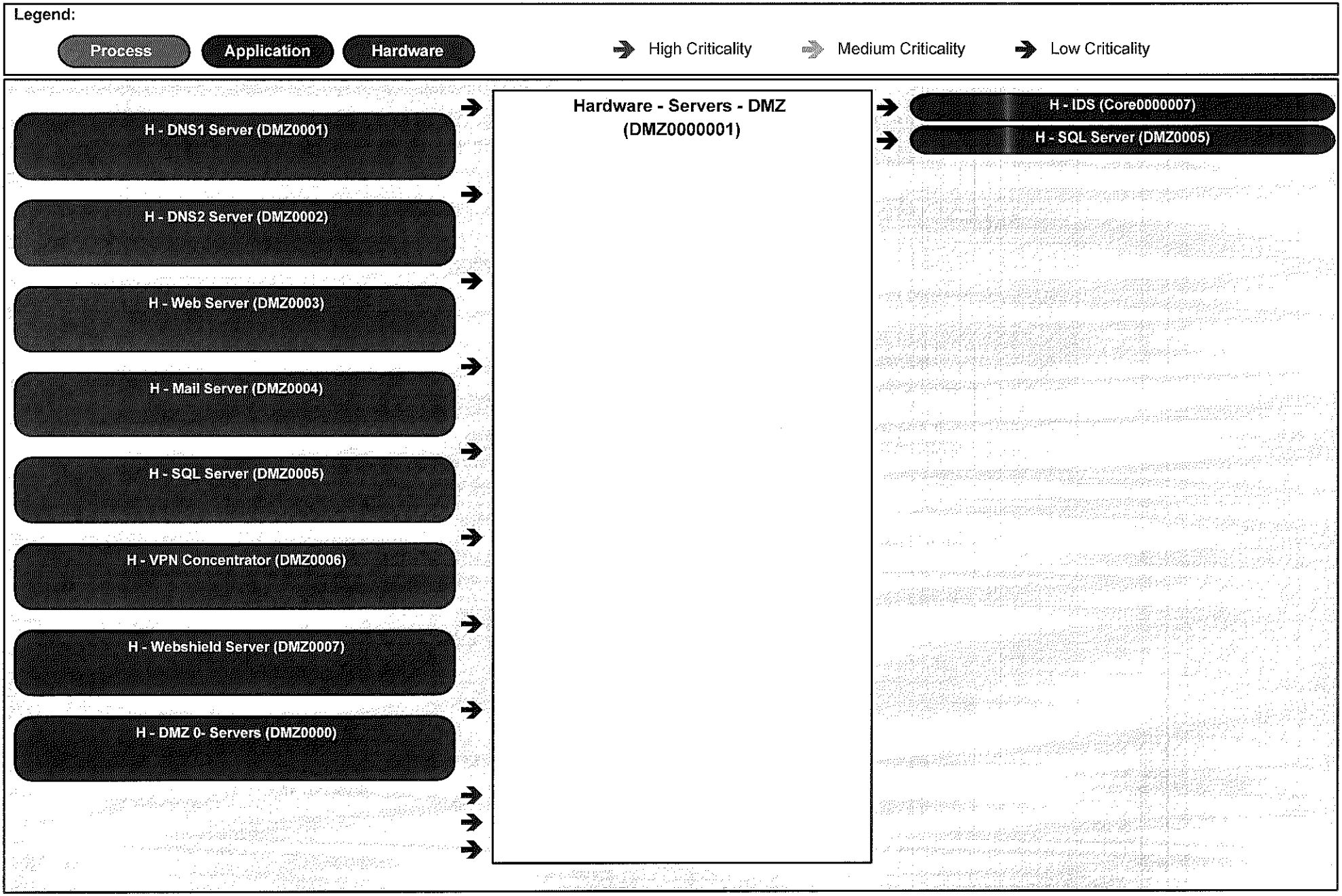
Report Description:
This report graphically depicts core components with up and downstream interdependencies.

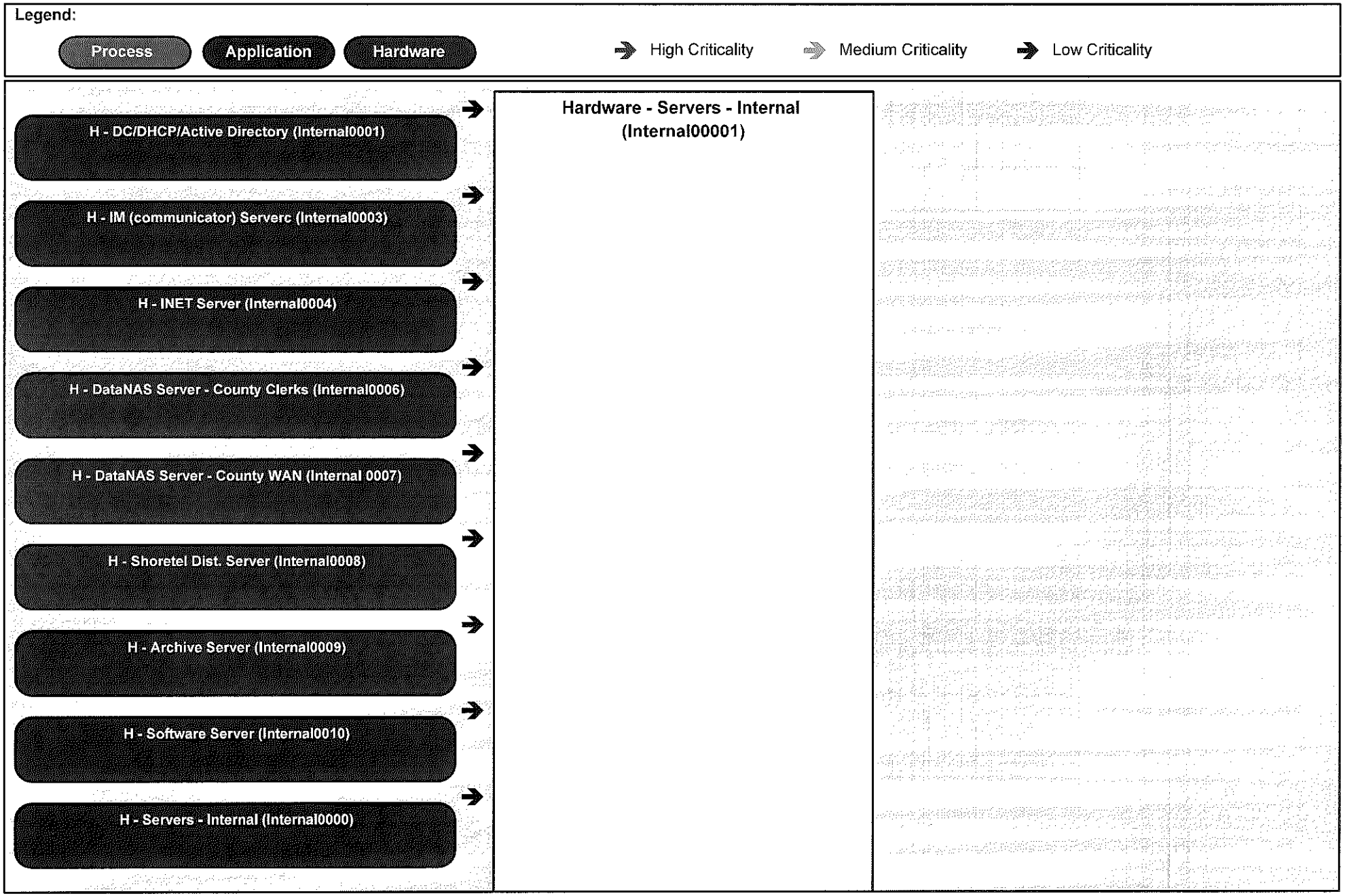
Legend:

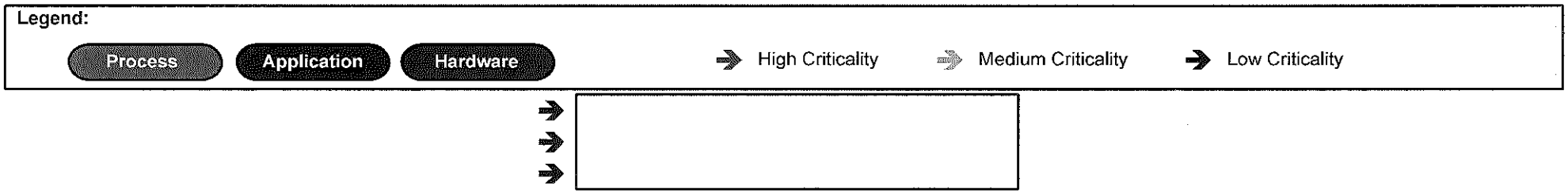
Process | Application | Hardware | High Criticality | Medium Criticality | Low Criticality

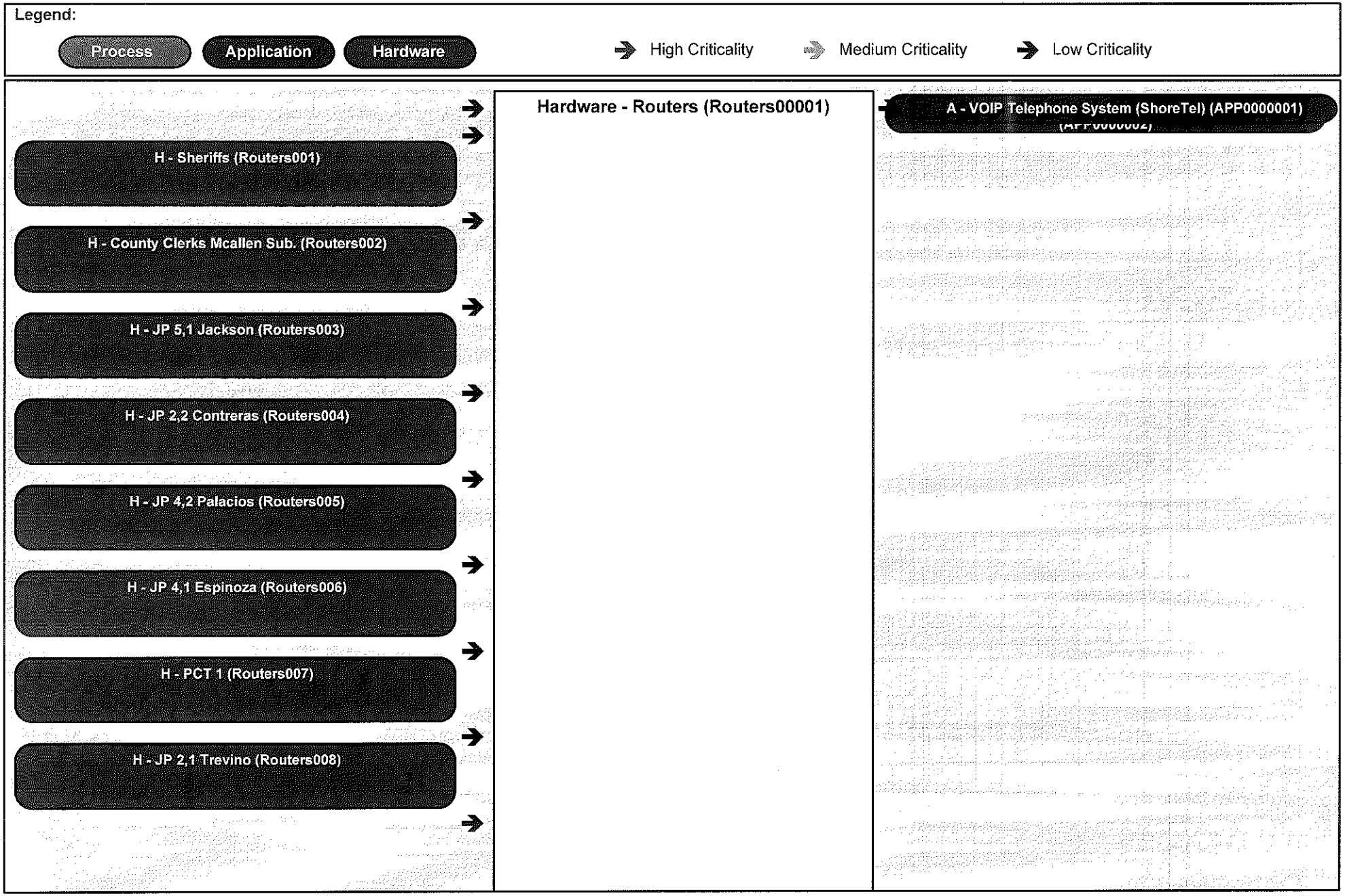


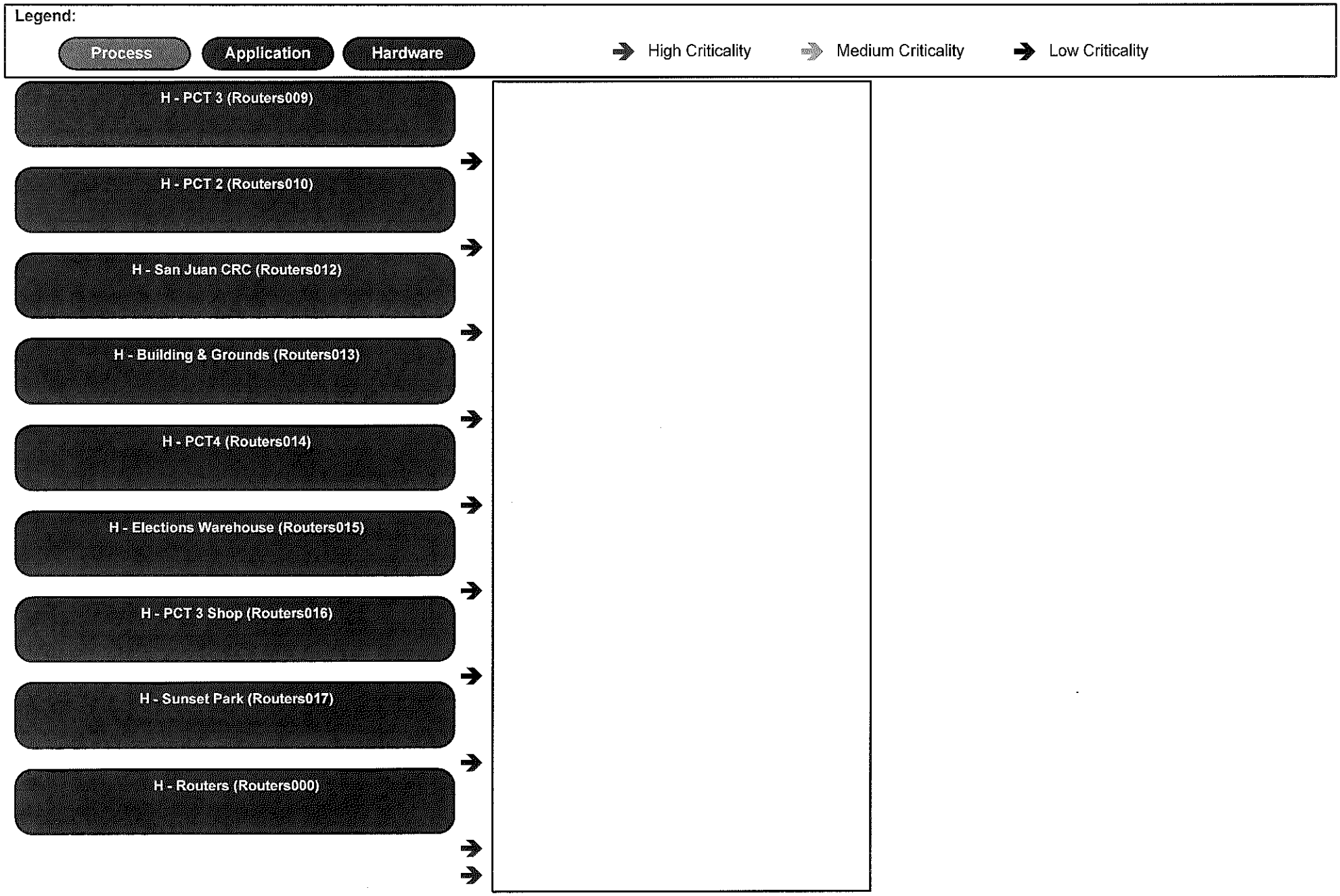

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
Hardware - Web Server (DMZ0003)
H - DMZ 0- Servers (DMZ0000)
H - Servers - DMZ (DMZ0000001)
Hardware - Mail Server (DMZ0004)
H - DMZ 0- Servers (DMZ0000)
H - Servers - DMZ (DMZ0000001)
A - VOIP Telephone System (ShoreTel) (APP0000001)
A - Web - Services (APP0000012)
H - Servers - DMZ (DMZ0000001)
Hardware - SQL Server (DMZ0005)
H - DMZ 0- Servers (DMZ0000)
H - Servers - DMZ (DMZ0000001)

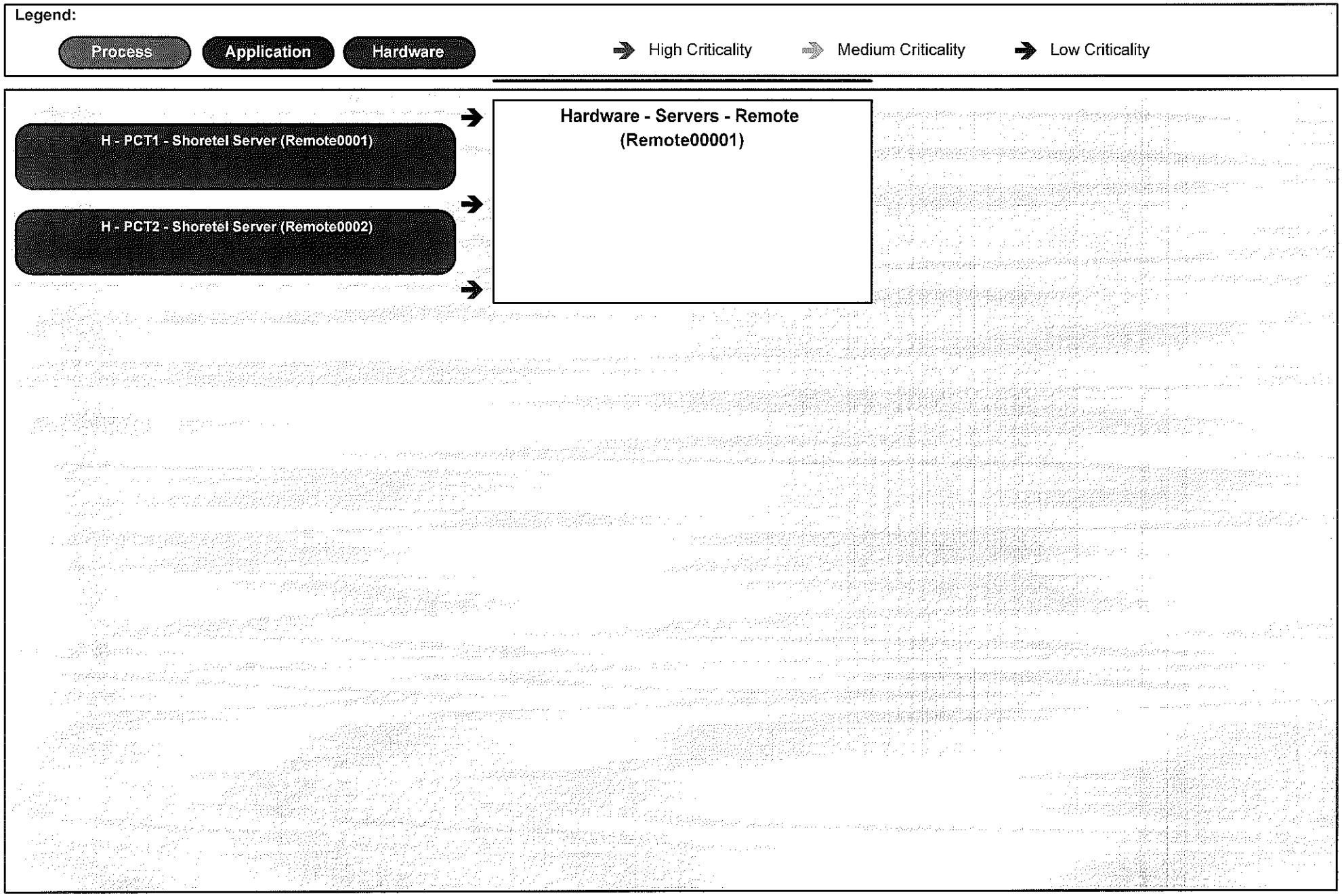

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - DNS1 Server (DMZ0001)
H - DNS2 Server (DMZ0002)
H - Web Server (DMZ0003)
H - Mail Server (DMZ0004)
H - SQL Server (DMZ0005)
H - VPN Concentrator (DMZ0006)
H - Webshield Server (DMZ0007)
H - DMZ 0- Servers (DMZ0000)
Hardware - Servers - DMZ
(DMZ0000001)
H - IDS (Core0000007)
H - SQL Server (DMZ0005)

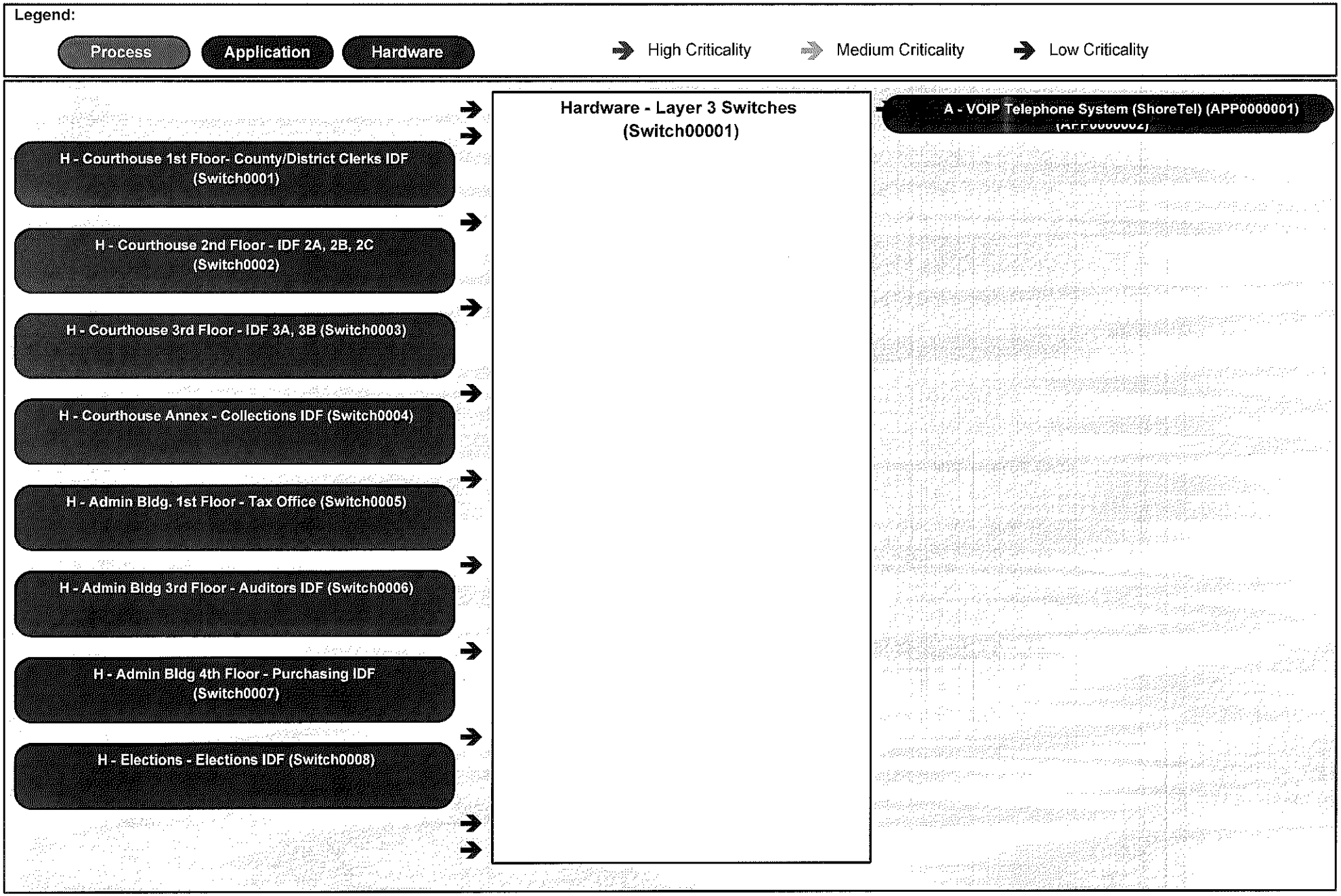

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - DC/DHCP/Active Directory (Internal0001)
H - IM (communicator) Serverc (Internal0003)
H - INET Server (Internal0004)
H - DataNAS Server - County Clerks (Internal0006)
H - DataNAS Server - County WAN (Internal 0007)
H - Shoretel Dist. Server (Internal0008)
H - Archive Server (Internal0009)
H - Software Server (Internal0010)
H - Servers - Internal (Internal0000)
Hardware - Servers - Internal (Internal00001)

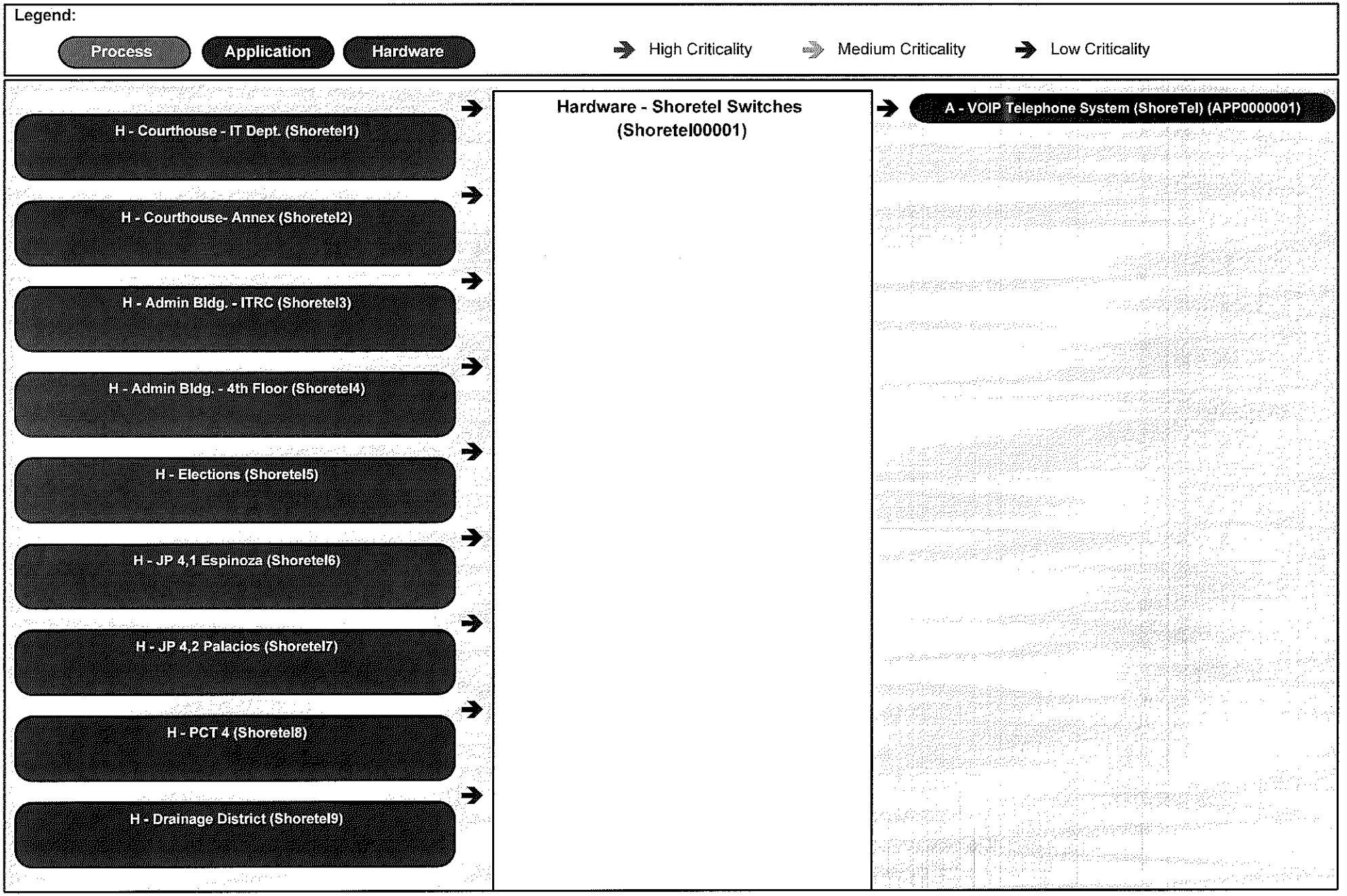

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality

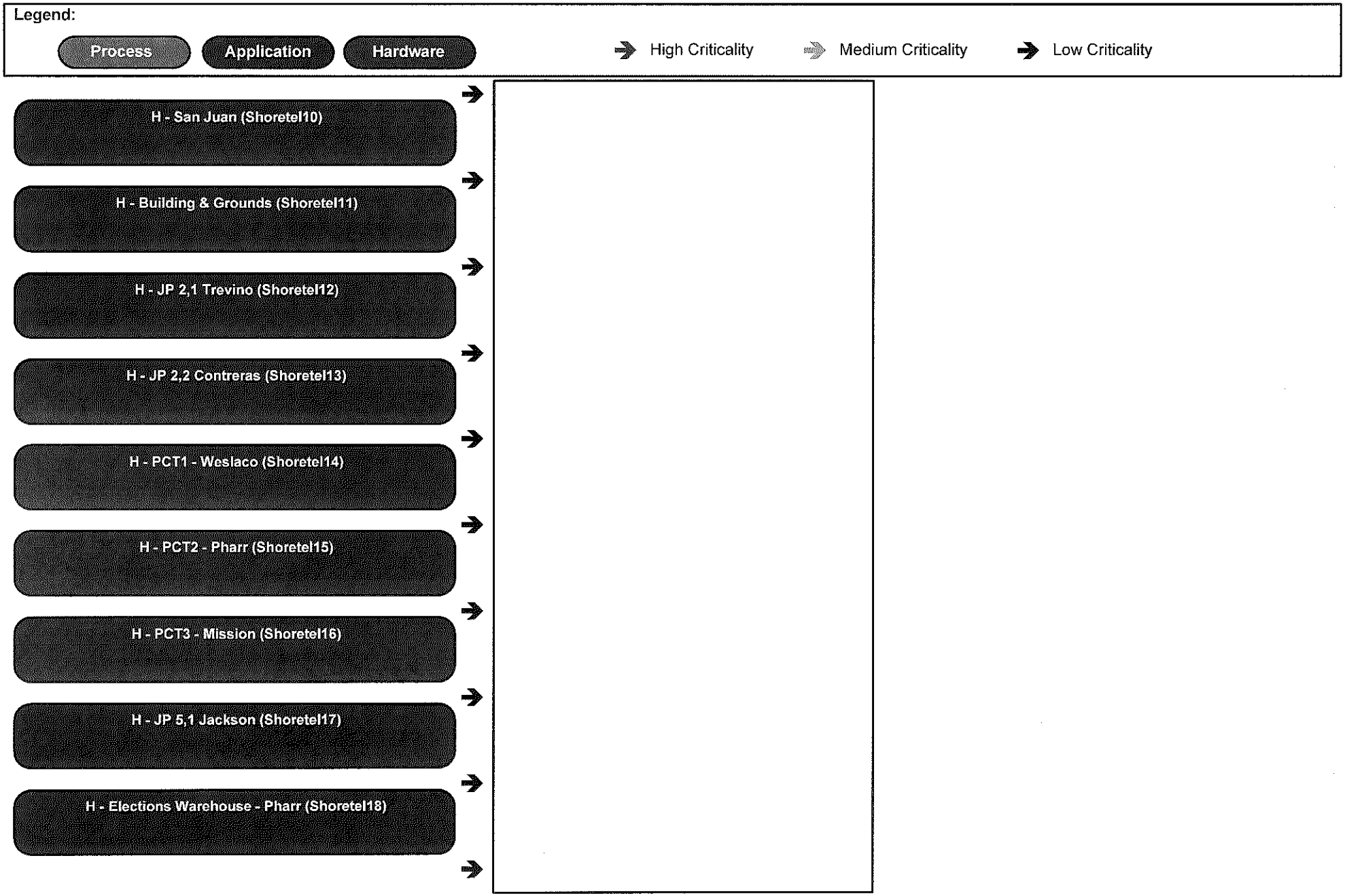

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sheriffs (Routers001)
H - County Clerks Mcallen Sub. (Routers002)
H - JP 5,1 Jackson (Routers003)
H - JP 2,2 Contreras (Routers004)
H - JP 4,2 Palacios (Routers005)
H - JP 4,1 Espinoza (Routers006)
H - PCT 1 (Routers007)
H - JP 2,1 Trevino (Routers008)
Hardware - Routers (Routers00001)
A - VOIP Telephone System (ShoreTel) (APP0000001)

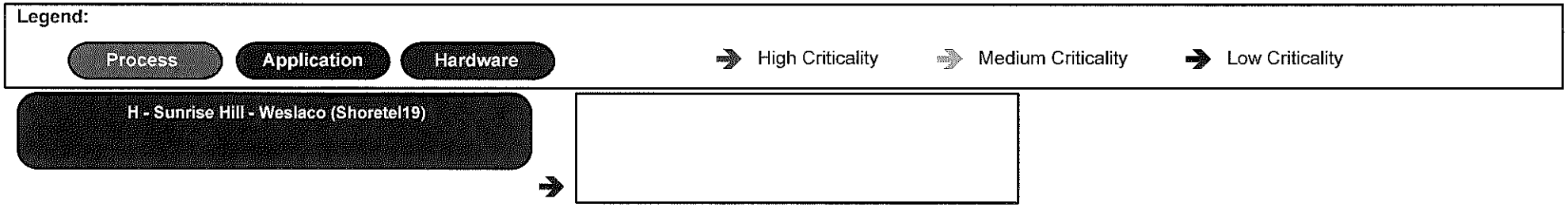

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT 3 (Routers009)
H - PCT 2 (Routers010)
H - San Juan CRC (Routers012)
H - Building & Grounds (Routers013)
H - PCT4 (Routers014)
H - Elections Warehouse (Routers015)
H - PCT 3 Shop (Routers016)
H - Sunset Park (Routers017)
H - Routers (Routers000)

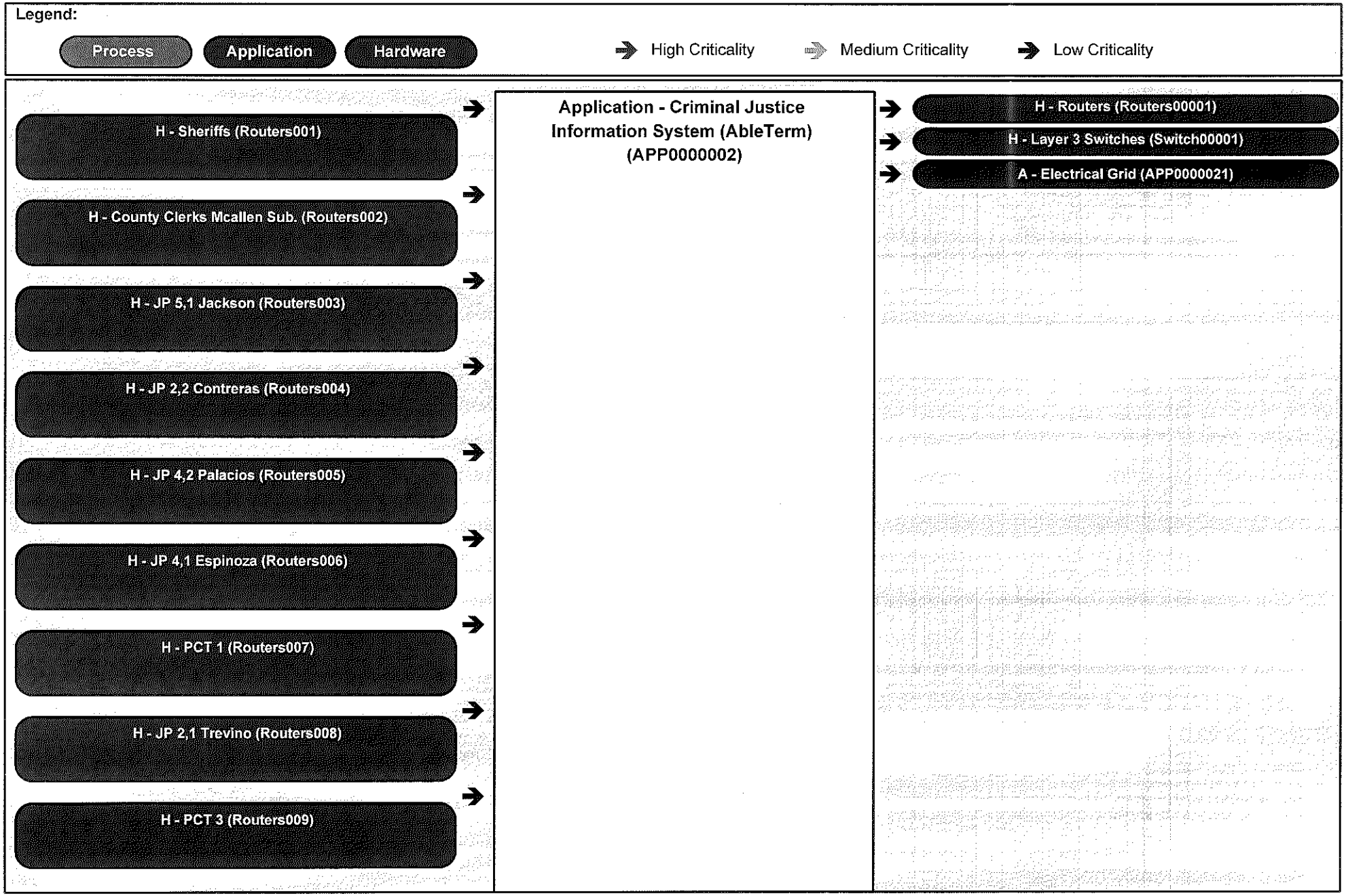

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT1 - Shoretel Server (Remote0001)
H - PCT2 - Shoretel Server (Remote0002)
Hardware - Servers - Remote
(Remote00001)

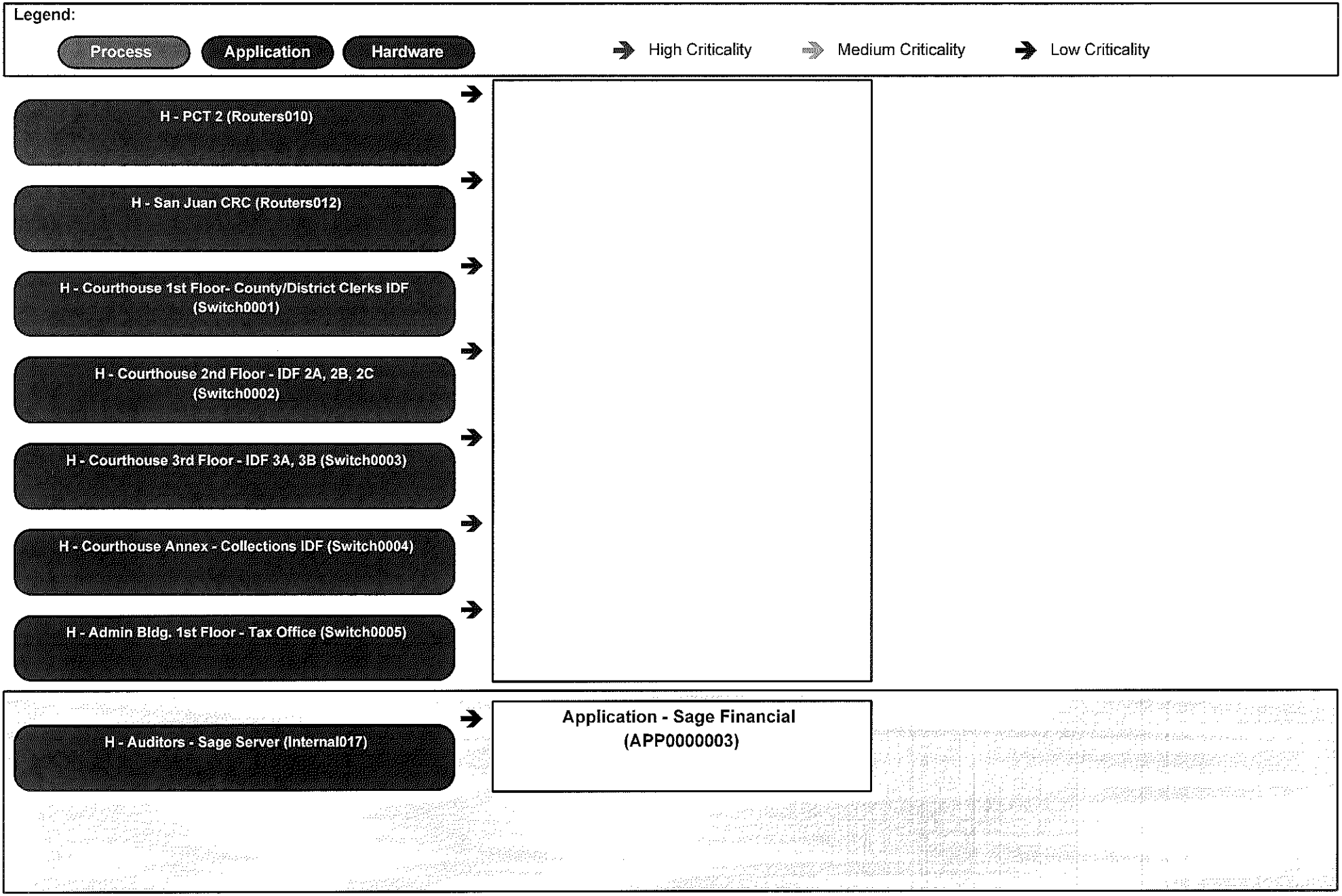

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Courthouse 1st Floor- County/District Clerks IDF (Switch0001)
H - Courthouse 2nd Floor - IDF 2A, 2B, 2C (Switch0002)
H - Courthouse 3rd Floor - IDF 3A, 3B (Switch0003)
H - Courthouse Annex - Collections IDF (Switch0004)
H - Admin Bldg. 1st Floor - Tax Office (Switch0005)
H - Admin Bldg 3rd Floor - Auditors IDF (Switch0006)
H - Admin Bldg 4th Floor - Purchasing IDF (Switch0007)
H - Elections - Elections IDF (Switch0008)
Hardware - Layer 3 Switches (Switch00001)
A - VOIP Telephone System (ShoreTel) (APP0000001)

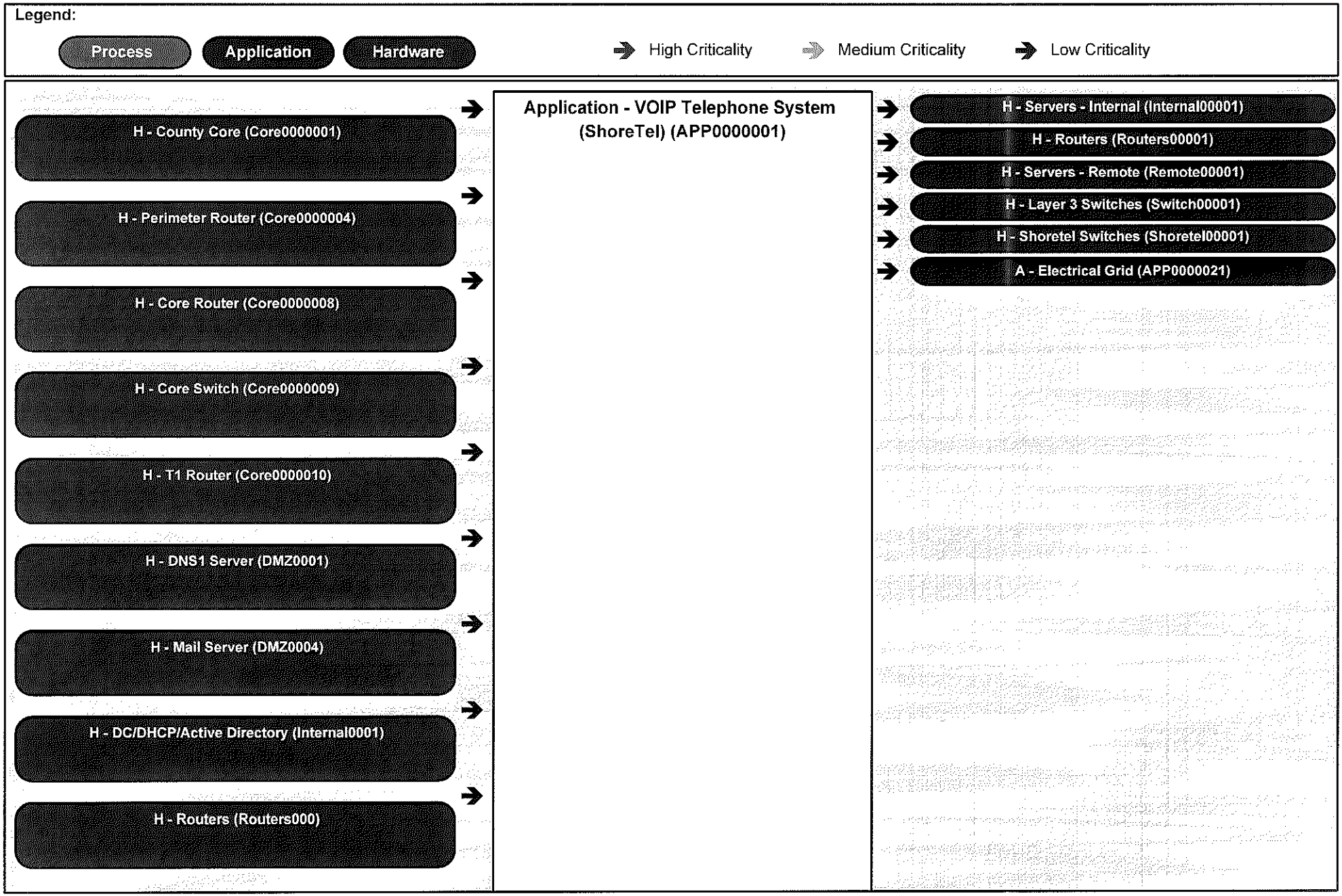

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Courthouse - IT Dept. (Shoretel1)
H - Courthouse- Annex (Shoretel2)
H - Admin Bldg. - ITRC (Shoretel3)
H - Admin Bldg. - 4th Floor (Shoretel4)
H - Elections (Shoretel5)
H - JP 4,1 Espinoza (Shoretel6)
H - JP 4,2 Palacios (Shoretel7)
H - PCT 4 (Shoretel8)
H - Drainage District (Shoretel9)
Hardware - Shoretel Switches (Shoretel00001)
A - VOIP Telephone System (ShoreTel) (APP0000001)

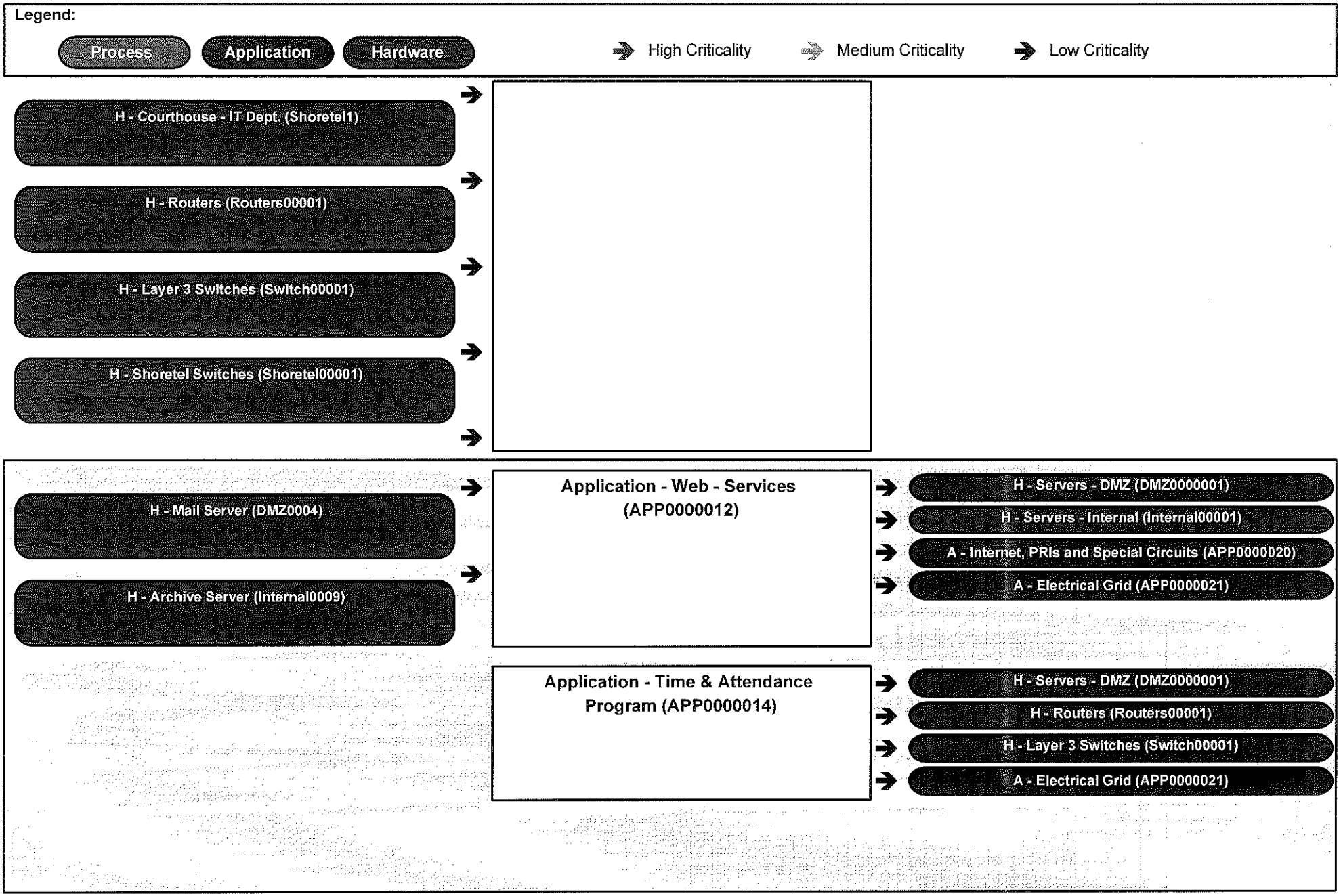

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - San Juan (Shoretel10)
H - Building & Grounds (Shoretel11)
H - JP 2,1 Trevino (Shoretel12)
H - JP 2,2 Contreras (Shoretel13)
H - PCT1 - Weslaco (Shoretel14)
H - PCT2 - Pharr (Shoretel15)
H - PCT3 - Mission (Shoretel16)
H - JP 5,1 Jackson (Shoretel17)
H - Elections Warehouse - Pharr (Shoretel18)

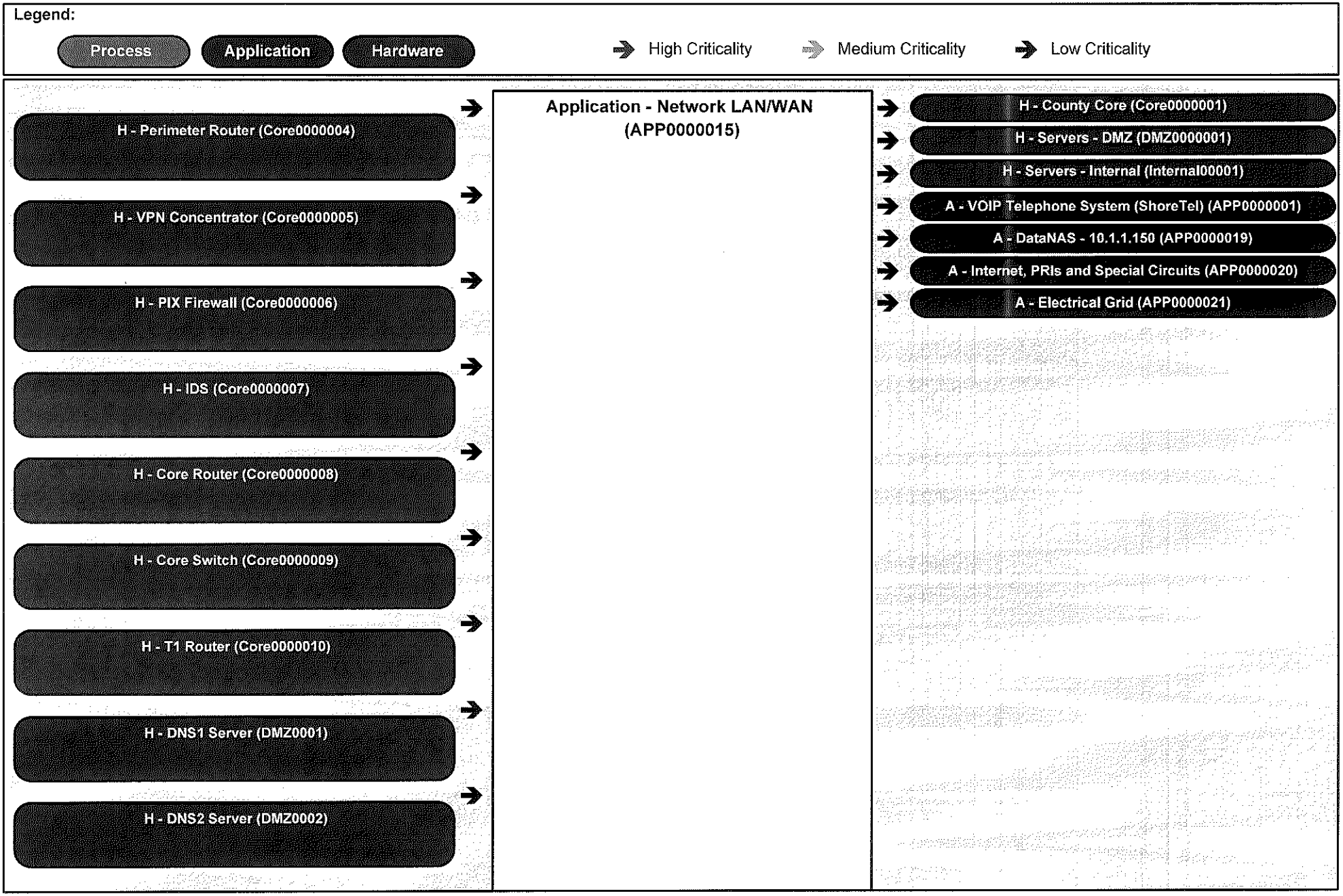

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sunrise Hill - Weslaco (Shoretel19)

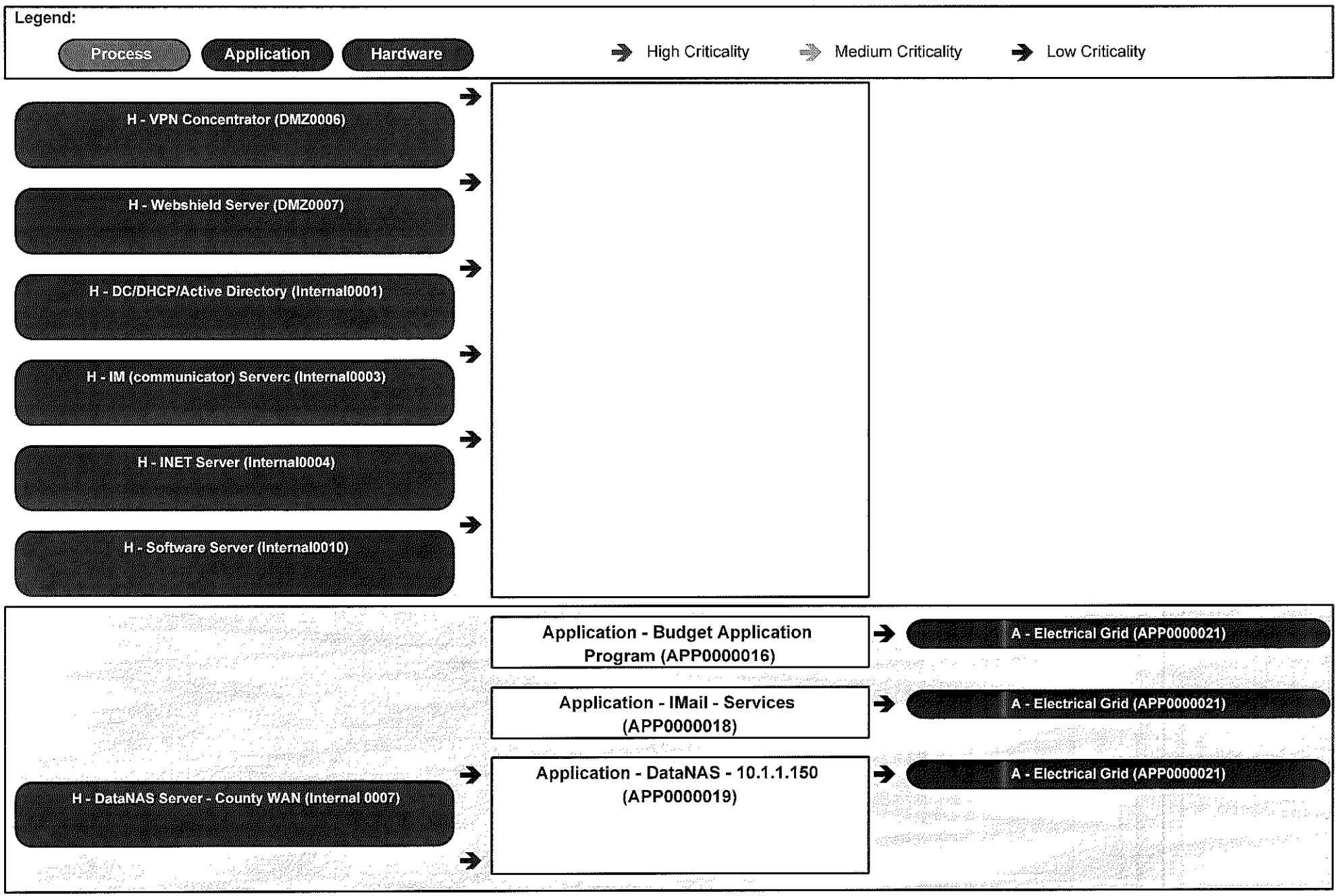

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sheriffs (Routers001)
H - County Clerks Mcallen Sub. (Routers002)
H - JP 5,1 Jackson (Routers003)
H - JP 2,2 Contreras (Routers004)
H - JP 4,2 Palacios (Routers005)
H - JP 4,1 Espinoza (Routers006)
H - PCT 1 (Routers007)
H - JP 2,1 Trevino (Routers008)
H - PCT 3 (Routers009)
Application - Criminal Justice Information System (AbleTerm) (APP0000002)
H - Routers (Routers00001)
H - Layer 3 Switches (Switch00001)
A - Electrical Grid (APP0000021)

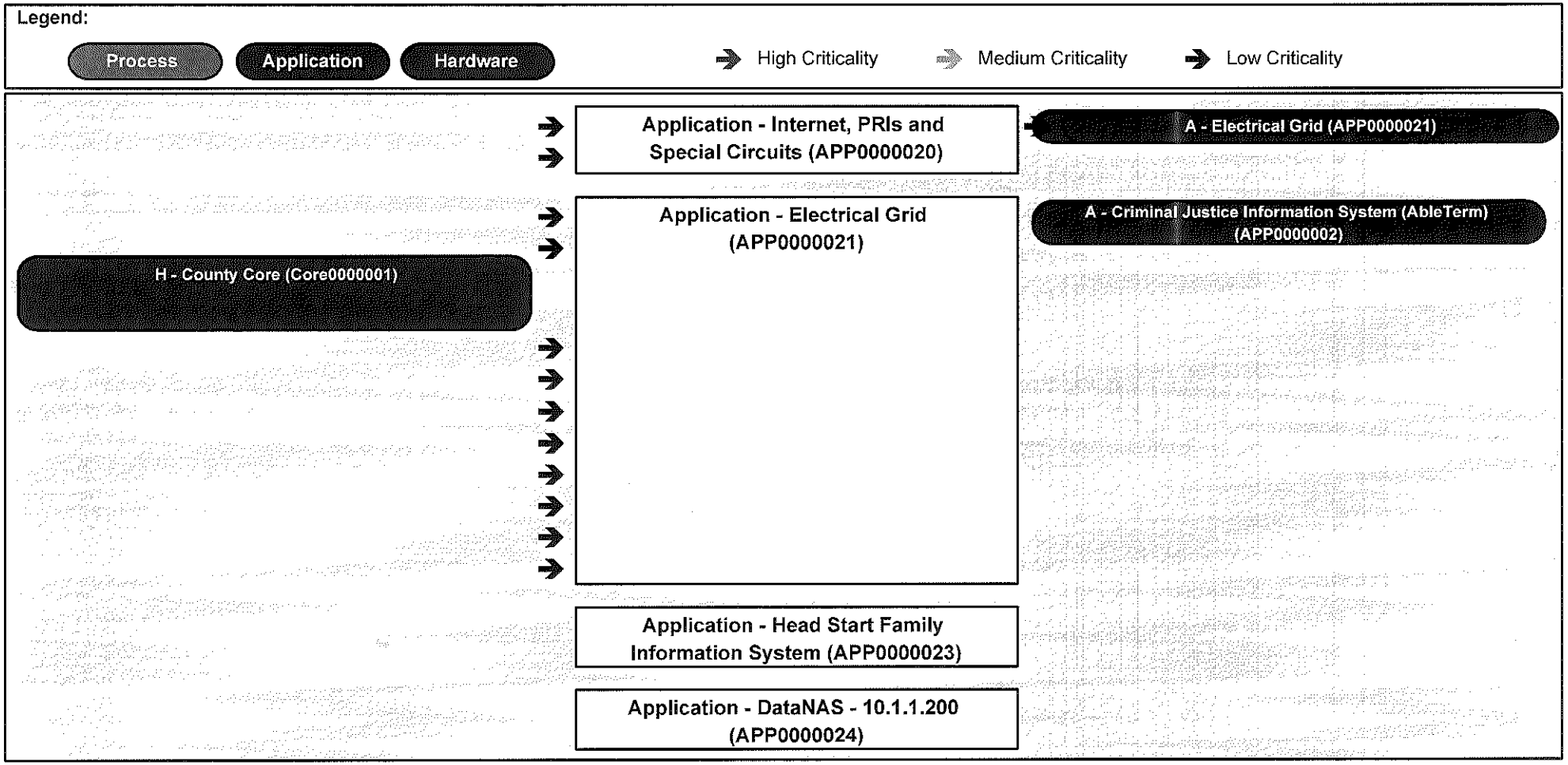

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT 2 (Routers010)
H - San Juan CRC (Routers012)
H - Courthouse 1st Floor- County/District Clerks IDF (Switch0001)
H - Courthouse 2nd Floor - IDF 2A, 2B, 2C (Switch0002)
H - Courthouse 3rd Floor - IDF 3A, 3B (Switch0003)
H - Courthouse Annex - Collections IDF (Switch0004)
H - Admin Bldg. 1st Floor - Tax Office (Switch0005)
H - Auditors - Sage Server (Internal017)
Application - Sage Financial (APP0000003)


Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - County Core (Core0000001)
H - Perimeter Router (Core0000004)
H - Core Router (Core0000008)
H - Core Switch (Core0000009)
H - T1 Router (Core0000010)
H - DNS1 Server (DMZ0001)
H - Mail Server (DMZ0004)
H - DC/DHCP/Active Directory (Internal0001)
H - Routers (Routers000)
Application - VOIP Telephone System (ShoreTel) (APP0000001)
H - Servers - Internal (Internal00001)
H - Routers (Routers00001)
H - Servers - Remote (Remote00001)
H - Layer 3 Switches (Switch00001)
H - Shoretel Switches (Shoretel00001)
A - Electrical Grid (APP0000021)


Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Courthouse - IT Dept. (Shoretel1)
H - Routers (Routers00001)
H - Layer 3 Switches (Switch00001)
H - Shoretel Switches (Shoretel00001)
H - Mail Server (DMZ0004)
H - Archive Server (Internal0009)
Application - Web - Services (APP0000012)
H - Servers - DMZ (DMZ0000001)
H - Servers - Internal (Internal00001)
A - Internet, PRIs and Special Circuits (APP0000020)
A - Electrical Grid (APP0000021)
Application - Time & Attendance Program (APP0000014)
H - Servers - DMZ (DMZ0000001)
H - Routers (Routers00001)
H - Layer 3 Switches (Switch00001)
A - Electrical Grid (APP0000021)


Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Perimeter Router (Core0000004)
H - VPN Concentrator (Core0000005)
H - PIX Firewall (Core0000006)
H - IDS (Core0000007)
H - Core Router (Core0000008)
H - Core Switch (Core0000009)
H - T1 Router (Core0000010)
H - DNS1 Server (DMZ0001)
H - DNS2 Server (DMZ0002)
Application - Network LAN/WAN (APP0000015)
H - County Core (Core0000001)
H - Servers - DMZ (DMZ0000001)
H - Servers - Internal (Internal00001)
A - VOIP Telephone System (ShoreTel) (APP0000001)
A - DataNAS - 10.1.1.150 (APP0000019)
A - Internet, PRIs and Special Circuits (APP0000020)
A - Electrical Grid (APP0000021)


Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - VPN Concentrator (DMZ0006)
H - Webshield Server (DMZ0007)
H - DC/DHCP/Active Directory (Internal0001)
H - IM (communicator) Serverc (Internal0003)
H - INET Server (Internal0004)
H - Software Server (Internal0010)
Application - Budget Application Program (APP0000016)
Application - IMail - Services (APP0000018)
Application - DataNAS - 10.1.1.150 (APP0000019)
H - DataNAS Server - County WAN (Internal 0007)
A - Electrical Grid (APP0000021)
A - Electrical Grid (APP0000021)
A - Electrical Grid (APP0000021)


Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
Application - Internet, PRIs and Special Circuits (APP0000020)
A - Electrical Grid (APP0000021)
Application - Electrical Grid (APP0000021)
A - Criminal Justice Information System (AbleTerm) (APP0000002)
H - County Core (Core0000001)
Application - Head Start Family Information System (APP0000023)
Application - DataNAS - 10.1.1.200 (APP0000024)

COUNTY OF HIDALGO, TEXAS

COUNTY AUDITOR'S OFFICE

DISASTER RECOVERY PLAN

EFFECTIVE: MARCH 1, 2007

RAYMUNDO EUFRACIO, C.P.A.
COUNTY AUDITOR

HIDALGO COUNTY AUDITOR'S OFFICE
DISASTER RECOVERY PLAN
EFFECTIVE: MARCH 1, 2007

Note: Terms defined in APPENDIX A: GLOSSARY are in **boldface type** the first time they appear in this document.

INTRODUCTION

This document contains the **disaster recovery plan** for the Hidalgo County Auditor's Office. It serves as a guide for the recovery of the Hidalgo County Auditor's Office (Auditor's Office) **mission-critical systems** in the event that a **disaster** destroys all or part of the components that comprise the mission-critical systems.

DESCRIPTION

The disaster recovery plan is composed of several sections that outline the resources and procedures to be used in the event that a disaster occurs at the Auditor's Office located at 100 E. Cano Street, Administration Building, 3rd Floor, Edinburg, Texas. There is also a section that documents the personnel that will be needed for the disaster recovery process.

PART 1: GENERAL INFORMATION ABOUT THE PLAN

Section 1.01: Objectives and Overview
Section 1.02: Mission-Critical Systems

PART 2: DISASTER RECOVERY PLANNING

Section 2.01: Disaster Preparation
Section 2.02: Recovery Facility
Section 2.03: Backup Procedures

PART 3: INITIATION OF EMERGENCY PROCEDURES

Section 3.01: Disaster Notification List
Section 3.02: Disaster Recovery Teams
Section 3.03: Damage Assessment
Section 3.04: Implementing the Disaster Recovery Plan

PART 4: MAINTAINING THE PLAN

Section 4.01: Maintaining the Plan

PART 5: INVENTORY OF SYSTEMS

Section 5.01: Servers-Hardware & Software

APPENDIX A: DEFINITIONS

APPENDIX B: INVENTORY OF SERVERS

PART 1: GENERAL INFORMATION ABOUT THE PLAN

Section 1.01: Objectives and Overview

The purpose of the disaster recovery plan is to provide an effective and documented method for responding to a disaster that may adversely affect the operability of the Auditor's Office mission-critical systems.

The objectives of the disaster recovery plan are:

- to describe the mission-critical systems (**hardware** and **software**) that will need to be restored,
- to describe the steps to be taken to restore the mission-critical systems,
- to describe the duties of each individual needed for the recovery process, and
- to list their contact information.

Section 1.02: Mission-Critical Systems

The Auditor's Office maintains the following seven **servers** which comprise the mission-critical systems of the Auditor's Office:

1. The SAGE server contains the SAGE financial software. SAGE, *Software for Administrators in Government and Education*, is a full functioning, graphical financial software, deployed in an Oracle ™ database. SAGE includes the following modules and their related data: Financial Accounting System (FAS), Budget Preparation System (BPS), Human Resources System (HRS), Check Reconciliation System (CRS), and Fixed Inventory System (FIS).

2. The TSWeb (Terminal Service Website) server is used to allow County Departments that are not on the **wide area network** (**WAN**) to connect to the SAGE server from a remote location by logging on to the Internet. The TSWeb server is also used to backup the SAGE server.

3. The Autostore server contains **Veritas Backup Software**, Audit Command Language (ACL) software and Autostore scanning software. The Veritas Backup Software controls the Quantum Ultrium LTO-2 Backup external drive, which is used to backup the File server.

4. The File server is used for central storage and management of the Auditor's Office data files so that other computers on the same network can access the files. The file server allows users to share information over a network without having to physically transfer files by floppy or some other external device.

5. The DHCP (Dynamic Host Configuration Protocol) server is used to assign **IP addresses** to devices (e.g., **workstations** and phones) on the Auditor's Office network.

6. The NAV (Norton Antivirus) server is used to keep the Auditor's Office servers and client computers virus free by downloading virus definition updates.

7. The Legacy server contains the Legacy financial software that was used prior to SAGE. It contains historical financial data from 1992-2001.

PART 2: DISASTER RECOVERY PLANNING

Section 2.01: Disaster Preparation

The first step in preparing for a disaster is to develop a disaster recovery plan. This document contains the disaster recovery plan for the Auditor's Office. This plan is a component of the countywide disaster recovery plan for Hidalgo County. Its effectiveness depends on the disaster recovery plans from the other offices or departments of the County.

Section 2.02: Recovery Facility

If the Auditor's Office is destroyed in a disaster, repair or rebuilding of the facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site. Alternate sites may be either cold or hot sites. A cold site is a disaster recovery facility that provides only the physical space for recovery operations while the organization using the space provides its own hardware and software systems. A hot site is a fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster or for disaster recovery.

The Auditor's Office disaster recovery plan calls for a cold site in the event of a disaster. The Hidalgo County Department of Health and Human Services, located at 1304 S. 25th Ave., Edinburg, Texas, has agreed to allow the Auditor's Office to use their facilities as a cold site during the disaster recovery process. The location has adequate space to house the hardware, with some office space available for operating and technical personnel.

Section 2.03: Backup Procedures

The Auditor's Office mission-critical systems are comprised of seven servers described in Section 1.02. The following describes the **backup** procedures for these servers.

The PC Specialist backs up the SAGE server and File server on a daily basis. The backup tapes are physically transported to and stored in a lockbox at First National Bank located at 100 W. Cano, Edinburg, Texas by the System Support Specialist. The close proximity of this off-site location to the Auditor's Office allows for quick retrieval of the backup tapes in a disaster situation. The close proximity, however, may also increase the risk that the off-site location is also affected by the same disaster.

The Auditor's Office is working on a contingency plan that will place a backup server at the Hidalgo County Department of Health and Human Services. Information Design, Inc. (IDI), the SAGE software vendor, will write a script that will transfer the data from the on-site server to the backup server though the Hidalgo County **VPN**.

The SAGE server is backed up to a **DLT** tape daily at 11:55 PM using Veritas Backup Software. The backup tape contains the **DMP** files (created at 10:00 PM) and the **QTHOME** folder. The System Support Specialist transports the backup tape to the lockbox the following morning. There are approximately 20 DLT tapes that are used in rotation. When the most recent backup tape is transported to the lockbox, the oldest backup tape in storage is retrieved and placed in rotation. The backup tape for the end of the month is not retrieved but left in the lockbox. In addition to the backup tape, a complete **disk image** of the SAGE server is stored onto a **DVD** every month. The System Support Specialist transports the DVD to the lockbox once completed.

The file server is backed up to an **LTO-2 Ultrium** tape daily at 8:00 PM using VERITAS Backup Software. Only the data files are backed up to the tape. Data files are stored using **Snap Appliance**. The System Support Specialist transports the backup tape to the lockbox the following morning. There are 12 LTO-2 Ultrium tapes used in rotation: 4 daily, 4 weekly, and 4 monthly. Monday through Thursday's backup tapes are rotated daily. Friday's backup tape is rotated weekly. The end of month backup tape is rotated every 4 months. In addition to the backup tape, a complete disk image of the device is stored onto a DVD every month. The System Support Specialist transports the DVD to the lockbox once completed.

The Legacy server contains historical financial data from 1992-2001. This server is used solely to view the County's historical financial information. Since the server contains no new data, a daily backup tape is not necessary. A complete backup of the server on 4 **DDS1** tapes is stored in the lockbox.

The remaining servers do not contain data that requires daily backup. However, since they store configuration information, a disk image of each server is stored onto a DVD every quarter except for the Autostore server which is done every month. The System Support Specialist transports the DVD to the lockbox once completed.

A set of the following original software is also kept in the lockbox at First National Bank: Windows 2000, PCAnywhere, Veritas Backup Software, ACL, Autostore Scanning Software, Windos NT 4.0, Symantec Antivirus Corporate Edition 8.1.

PART 3: INITIATION OF EMERGENCY PROCEDURES

Section 3.01: Disaster Notification List

The disaster notification list contains the names and numbers of the individuals to be notified in the event that a disaster destroys all or part of the components that comprise the Auditor's Office mission-critical systems. The PC Specialist is responsible for contacting the following individuals immediately, or as soon as possible after a disaster has been confirmed.

	Name	Title	Home Phone	Cell/Work Phone
Auditor's Office	Raymundo Eufracio	County Auditor	(956) 424-7717	(956) 205-8374
Auditor's Office	Linda Fong	1st Asst County Auditor	(956) 287-9176	(956) 457-7632
Auditor's Office	Abel S. Martinez	PC Specialist	(956) 781-0857	(956) 789-1134
Auditor's Office	Alex Mortera	System Support	(956) 867-3939	(956) 867-3939
IT Department	Renan Ramirez	Chief Information Officer	(956) 380-3979	(956) 457-0792
IT Department	Cruz Quintana	Phone Support	(956) 784-2064	(956) 207-9941
IT Department	Juan De Leon	Network Support	(956) 874-5255	(956) 207-9204
Health & Human Services	Rigoberto Hinojosa	Information Officer	(956) 781-2044	(956) 207-6789
Information Design, Inc.	John Green	Programmer		(303) 792-2990 x2002
Information Design, Inc	Corey Oates	Technical Support		(303) 792-2990 x2013

Section 3.02: Disaster Recovery Teams

The disaster recovery plan provides for the following two teams that will be assigned with specific aspects of the recovery process:

1. Damage Assessment Team will evaluate the extent of the damage caused to the computer systems by the disaster and determine what steps need to be taken to recover the systems. The Team will be lead by the County Auditor and will include the following people: PC Specialist, System Support Specialist, Chief Information Officer, Phone Support, and Network Support.

2. Computer Systems Recovery Team will be responsible for the recovery of the computer systems. The Team will consist of the PC Specialist, System Support Specialist, Network Support, Programmer and Technical Support.

Section 3.03: Damage Assessment

In the event of a disaster, it is critical that a damage assessment be performed to evaluate the extent of the damage to the site and the equipment it houses.

The Damage Assessment Team will perform a preliminary damage assessment intended to establish the extent of damage to critical hardware and the facility that houses it. The primary goal is to determine where the recovery should take place (current facility or cold site) and what hardware must be ordered immediately.

Section 3.04: Implementing the Disaster Recovery Plan

The following are the procedures for recovery of the Auditor's Office mission-critical systems:

1. When a disaster occurs, the Damage Assessment Team will inspect the critical hardware and the facility that houses it to determine the extent of the damage and the resources that will be required to recover the mission critical systems.
    a. The PC Specialist and the System Support Specialist will assess and report on the condition of critical hardware. The report should identify hardware that can be repaired separately from hardware that must be replaced.
    b. Phone Support will assess and report on the condition of communication lines.
    c. Network Support will assess and report on the status of the network.

    The results of the damage assessment will be reported to the County Auditor and should include recommendations for proceeding with the disaster recovery. Based on the damage assessment, the County Auditor will determine if the recovery process will be conducted in the current facility or at the cold site. The County Auditor will also determine which hardware will need to be ordered immediately.

2. Based on direction from the County Auditor, the PC Specialist will order replacement hardware with overnight delivery. Hardware deemed to be repairable will be repaired by the PC Specialist and System Support Specialist.

3. If the recovery process will take place at the cold site, the PC Specialist and the System Support Specialist will transport all repairable equipment to the site. Otherwise, the PC Specialist and the System Support Specialist will clean and ready an area in the current facility to house the critical hardware.

4. The System Support Specialist will retrieve the backup tapes and the disk images from the lockbox.

5. The PC Specialist will recover the servers using the backup tapes and the disk images.

    a. The first server to be recovered will be the SAGE server. The PC Specialist will copy the disk image from the DVD to the server. The data from the previous day will then be restored to the server from the DLT backup tape. The System Support Specialist will call IDI to request a test of the SAGE financial software. The System Support Specialist will notify the First Assistant County Auditor when the SAGE server has been recovered. The First Assistant County Auditor will coordinate with the Accounting and Audit Divisions to determine if the financial data has been recovered successfully or whether the recovery process must be repeated.

    b. The second server to be recovered will be the TSWEB server. The PC Specialist will copy the disk image from the DVD to the server. The Chief Information Officer will be responsible for restoring Internet access to the outside departments in order for them to access the SAGE server.

    c. The third server to be recovered will be the Autostore server. The PC Specialist will copy the disk image from the DVD to the server.

    d. The fourth server to be recovered will be the File server. The PC Specialist will use the restore CD on the server. The data will then be restored to the server from the LTO-2 Ultrium tape.

    e. The fifth server to be recovered will be the DHCP server. The PC Specialist will copy the disk image from the DVD to the server.

    f. The sixth server to be recovered will be the NAV server. The PC Specialist will copy the disk image from the DVD to the server.

    g. The last server to be recovered will be the Legacy server. The data will be restored to the server from the backup tape.

PART 4: MAINTAINING THE PLAN

Section 4.01: Maintaining the Plan

To ensure that the plan will work when a disaster occurs, the plan must be maintained and updated. On a semi-annual basis, the PC Specialist will evaluate and update the plan with the approval of the First Assistant County Auditor. Updates to the plan will include changes in hardware, software, facilities, procedures, and personnel. In addition, the plan will be tested on an annual basis and any faults will be corrected.

PART 5: INVENTORY OF SYSTEMS

Section 5.01: Servers-Hardware & Software

APPENDIX B: INVENTORY OF SERVERS contains a complete list of all the servers that are used in the Auditor's Office. The list contains both hardware and software components for each server. The list will be routinely updated on a quarterly basis to keep up with the changes in hardware and software.

Approved by _____ Date 3/1/07

Raymundo Eufracio, C.P.A.
Hidalgo County Auditor

APPENDIX A: GLOSSARY

antivirus software
A computer program designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected files, cleaning infected files or systems, or informing the user that an infected program was detected.

application
A program or group of programs designed for end users. Applications software (also called *end-user programs*) includes database programs, word processors, and spreadsheets.

backup
The term *backup* usually refers to a disk or tape that contains a copy of data.

cold site
A disaster recovery facility that provides only the physical space for recovery operations while the organization using the space provides its own hardware and software systems.

DDS1
DDS or digital data storage tape is a magnetic tape used for backing up data with a native capacity of 2 GB.

disaster
An event that makes the continuation of normal functions impossible.

disaster recovery plan
A plan for business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data records and the physical space of an organization. The goal of a DRP is to resume normal computing capabilities in as little time as possible.

disk image
An exact copy of a computer's hard drive. Disk images are used to transfer a hard drive's contents during a hardware upgrade, to restore a hard drive's contents during disaster recovery or when a hard drive is erased, and to transfer the contents of a hard drive from one computer to another.

DLT
DLT or Digital Linear Tape is a form of magnetic tape and drive system used for computer data storage and archiving with a capacity of 40GB native and 80GB compressed.

DMP
A compressed form of the SAGE database used for restoring the database. It is made using a command included with Oracle database called exp (export).

hardware
Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips. In contrast, software is untouchable. Software exists as ideas, concepts, and symbols, but it has no substance.

hot site
A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster or for disaster recovery.

IP address
An identifier for a computer or device on a network.

local area network (LAN)
A computer network covering a small geographic area, like a home, office, or group of buildings. The defining characteristics of LANs, in contrast to WANs (wide area networks), include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

LTO-2 Ultrium
LTO or Linear Tape-Open is a magnetic tape data storage technology used for computer data storage and archiving with a capacity of 200GB native and 400GB compressed. LTO was developed as an "open" alternative to the proprietary Digital Linear Tape (DLT). The standard form-factor of LTO technology goes by the name "Ultrium".

mission-critical system
A system that is critical to the functioning of an organization and the accomplishment of its mission.

QTHOME
A folder that holds all SAGE software including any custom programs the users have.

server
A computer that delivers information and software to other computers linked by a network.

Snap Appliance
Snap Appliance ™ provides network attached storage (NAS) solutions. A large storage device used to access information quickly.

software
Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware.

Veritas Backup Software
Is software that provides continuous data protection of data on the servers by backing up data to a tape.

VPN
VPN or Virtual Private Network is the extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet.

wide area network (WAN)
A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or less formally, a network that uses routers and public communications links. The largest and most well known example of a WAN is the Internet. WANs are used to connect (LANs) and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations.

Workstation
Any computer connected to a local-area network.

APPENDIX B: INVENTORY OF SERVERS

Server	Hardware	Software
SAGE	Compaq Proliant ML 370R G3 (2) Intel Xeon 2.4 GHz processors 2 GB RAM (4) 36.4 GB SCSI hard drives CDROM 1.44 FDD	Windows 2000 Oracle 8i SAGE PCAnywhere
TSWEB	Compaq Proliant ML 370R G2 Intel Pentium III 1.2 GHz processor 1 GB RAM (3) 18.2 GB SCSI hard drives Quantum DLT1 tape drive CDROM 1.44 FDD	Windows 2000 Veritas Backup Software Terminal Services
Autostore	HP Proliant DL 140 Intel Xeon 2.4 GHz processor 1 GB RAM 80 GB hard drive Quantum Ultrium LTO 2 Backup external drive	Windows 2000 Veritas Backup Software ACL Software Autostore Scanning Software
File	Snap Appliance Snap Server 4100	
DHCP	Clone PC Intel P-III 450MHz 64 MB RAM 4 GB hard drive CDROM 1.44 FDD	Windows NT 4.0 DHCP Services
NAV	Dell PowerEdge 2650 Intel Xeon 2.4 GHz processor 512 MB RAM 80 GB hard drive CDROM 1.44 FDD	Windows 2000 Symantec Antivirus Corporate Edition 8.1
Legacy	HP3000 Computer System	HP MPE/iX software

Hidalgo County
Head Start Program

Disaster Recovery Plan

Last Update:
June 19, 2003

Hardware & Software description

Hidalgo County Head Start Program automated data is stored at the administration building in the Management Information System (MIS) department. All automated data is kept online on two file servers. Both servers are running Novell NetWare version 5.0. The main server stores and shares all user/department files, MIS software/data, Finance software/data, Personnel software/data, Risk Management software/data, Staff Development software/data, Transportation software/data, Procurement software/data, Education software/data, Family Literacy & Transition software/data, Mental Health software/data, Health software/data, Special Services & Nutrition software/data, Family Services software/data. All information on the server is backed up on a daily basis. An unattended full system backup is scheduled to run every evening at 11:59 p.m.

Hardware:

* The **primary server** is a Dell PowerEdge 4300 with 1 GB of memory and three 9GB drives with RIAD 5 configuration. The server holds 2 Intel Pro/1000 gigabit, fiber optic, server adapters, 1 Intel Pro 100+Ethernet adapter, 2 Hewlett Packard 100VG Ethernet adapters. This unit shares all user/department files.
* The **secondary server** is a digital Prioris HX 5133 with 512 MB of memory and two 2GB drives and two 4GB drives with RAID 0 configuration. The server holds one 3Com 10/100 Ethernet adapter, and one 10 Mbps Ethernet adapter. This unit is primarily used as a print server and contains Office Suite software that is run off the network.
* An internal DLT4000 tape backup is installed on the primary server. This unit can store up to 40 GB (compressed) of information on one DLT tape.
* An **A**merican **P**ower **C**onversion (APC) Smart-UPS (Uninterruptible Power Supply) 2200, and 1400 battery backup units supply 5 – 15 minutes of backup power to the file servers in case of an electrical power outage.
* A Hewlett Packard ProCurve Switch 4000M that contains seven 8 port, 10/100 Mbps modules and two 1 port 1000 Mbps modules. The transmitting/receiving of data between the workstations and server are handled through this unit.
* Three Hewlett Packard AdvanceStack 100VG, 15 port, 10/100 Mbps, hubs. The transmitting/receiving of data between the workstations and server and the hub and server are handled through this unit.
* Two Digital MultiStack 90T-16, 16 port, 10 Mbps, repeaters. The transmitting/receiving of data between the workstations/printers and server are handled through this unit.
* One Intel Express 8100 router is connected to the HP 4000M switch at 100 Mbps over the Local Area Network (LAN). This unit will allow any workstation which has been properly setup for access to the Internet via an ISDN line.

Software:

* Novell NetWare version 5.0 is the networking operating system installed on the servers. The storage space is separated into 5 separate volumes on the server (SYS:, Vol1:, Vol2:, Vol3:, Vol4:) and 5 separate volumes on the secondary server (SYS:, Vol1:, Vol2:, Vol3:, Vol4:). The primary server's network name is HCHSP0 and the secondary is HCHSP1.
* Veritas Backup Exec version 8.0 (Enterprise Edition) is the software used to backup the data on the servers. This software version can handle a multiple server environment.
* MIP NonProfit Series is the fund accounting software used by Hidalgo County Head Start Program. This program handles financial data, current and historical, to include general ledger, payroll, accounts payable, encumbrances, purchase orders, and fixed assets. This software is stored on VOL3: of the primary server along with most of the data pertaining to the finance department.
* Head Start Family Information System (HSFIS) is a data collection system used to track all family and child information, current and historical, to include family demographics (Family Services), child development (Education), child health (Mental Health/Special Services & Nutrition), family (Family Services), transition (Family Literacy & Transition), volunteer and inkind (Finance), staff (Personnel/Staff Development), community resources (All Departments), center, program and setup information. This software is stored on VOL4: of the primary server along with most of the data pertaining to the MIS department.
* Microsoft Office 2000 Professional (Access, Excel, Outlook, PowerPoint, Publisher, Word), Corel WordPerfect Office 2000 (WordPerfect, QuatroPro, Presentations), and Lotus 123 are the software titles that are run off the LAN. These programs are contained in the secondary server. This server handles all print queue information submitted by users on VOL1:. Lotus 123 is stored on VOL2:, Microsoft Office 2000 Professional is stored on VOL3:, and Corel WordPerfect Office 2000 is stored on VOL4: of the secondary server.
* Original copies of the software listed will be cataloged and kept in the same fireproof cabinets as the backup tapes(Planned for October 2001). Backup copies of the software will be created on CD-Rom and kept at the off-site location along with copies of their license numbers.(Planned upon receiving fireproof cabinets for off-site location.)

Backup Description:

The information that is stored by the backup software and hardware described previously is kept on DLT4000 compatible tapes. The daily backups are scheduled to run automatically and unattended at 11:59 p.m. every workday. The tapes used can store up to 70GB (compressed) of data. Each tape is labeled with the day of the week of when that backup was run and then overwritten on the same day of the following week. This gives the agency 5 days of data recovery. A monthly backup is also run on the first workday of every month. This is a new procedure that began on September 2001. The daily backup tapes are rotated every workday morning. The tapes are locked and stored in a fireproof cabinet with the drawer marked "Backup Tapes", in the MIS department. A two drawer fireproof cabinet was order on September 2001. This cabinet will be placed in the Edinburg IV center where the "Monday" and "Friday" tapes will be rotated, locked and stored off-site. The keys to the cabinet are kept by the MIS assistant (Blanca Mayorga) which are issued to an MIS clerk to initiate the daily backup procedure. A backup procedure log has been established on September of 2001. This log is updated each time a backup tape is loaded/unloaded from the server. The log is kept in the same drawer with the backup tapes. The MIS assistant will be responsible to check the log once a week for proper documentation.

Off-Site Location Description:

The off-site location chosen was Edinburg IV. This location was selected for the following reasons:

1. Location: The Edinburg IV center is located near the administration office for easier accessibility.
2. Ownership: This center is owned by Hidalgo County Head Start Program. This allows us to have access to the information at any given time.
3. Security: This center has s security alarm system.
4. Space Availability: This newly built center has the available space needed for the storage cabinet.

Disaster Recovery:

Currently, hardware used to recover information from backup tapes is only available at the administration building. This hardware that was previously listed must be in operational condition to recover any data. In the event that the equipment needed is non-operational the agency must replace those items before any restoration of data is done. Once the equipment for recovery is available backup tapes from either the administration or off-site location, depending on availability, may be used. The information restored will be recovered by priority. Priority "1" is the highest to priority "10" the lowest.

The following table illustrates priority sequences by department and hardware and software requirements. These are minimal automation requirements needed to keep the department operational. Optimal requirements that match or surpass the current implemented.

Priority	Department	Minimum Hardware Requirements	Software
1	Finance, Procurement	Server requirements: Single Intel 200 MHz processor, 128 MB RAM, 3 GB HD, Fast Ethernet compatible hardware, Novell 5.0, Windows Server 2000 operating system Workstation Requirements: Single Intel 200 MHz processor, 128 MB RAM, 600 MB HD, SVGA Monitor, Laser printer, Fast Ethernet compatible hardware, MS Windows 98 or higher	MIP software data from tape backup system MIP workstation files
2	MIS	Server requirements: Single Intel 1 GHz processor (currently running On a 600 MHz server), 256 MB RAM, *73 GB, 10,000 RPM, SCSI HD, Novell. Windows 2000 Server operating systems Workstation Requirements: Single Intel 800 MHz processor (currently running on 133-1000 MHz workstations), 128 MB RAM, *4 GB HD, SVGA Monitor, Laser Printer, MS Windows 95/98/NT/2000/ME *The average minimum hard drive space requirements for HSFIS family data storage is 10 MB per 100 families per year.	HSFIS software, data from tape backup system HSFIS Workstation files
2	Personnel	Single Intel 200 MHz processor, 64 MB RAM, 2 GB HD, SVGA Monitor, Laser Printer, MS Windows 98/2000	Microsoft Access, Word, and WordPerfect
3	All other departments if needed	Single Intel 200 MHz processor, 64 MB RAM, 2 GB HD, SVGA Monitor, Laser/Inkjet Printer, MS Windows 98/2000	Microsoft Word, Excel, Access, and WordPerfect

The following is a list of current files stored on tape:

MIS Department:

Head Start Family Information System (HSFIS) program. All family and child information, current and historical, to include family demographics (Family Services),child development (Education), child health MentalHealth/Health/Special Services & Nutrition), family development transition (Family Literacy & Transition), volunteer and inkind (Finance), staff (Personnel/Staff Development), and community resources (All Departments) information.
All system data, current and historical, to include agency, center program sessions, and setup information.

Any individual files created by the MIS department and stored on a volume of the file server.

Finance Department:

MIP NonProfit Series program (fund accounting program)
All financial data, current and historical, to includegenral ledger, payroll, accounts payable, encumbrance, purchase orders, and fixed assets.

Any individual files created by the personnel department and stores on a volume of the file server.

Personnel Department:

Staff information kept on a Microsoft Access database. Staff data tracked on the HSFIS program.

Any individual files created by the risk management department and stores on a volume of the file server.

Risk Management:

Employee COBRA information.

Any individual files created by the risk management department and stored on a volume of the file server.

Staff Development:

Staff development information tracked through the HSFIS program.

Any individual files created by the staff development department and stored on a volume of the file server.

Transportation & Maintenance:

Any individual files created by the transportation and maintenance department and stored on a volume of the file server.

List of current files stored on tape – continued:

Procurement Department:
MIP NonProfit Series program (fund accounting program)
All MIP data, current and historical, pertaining to the procurement department.

Any individual files created by the procurement department and stored on a volume of the file server.

Education Department:
Education information tracked through the HSFIS program.

Any individual files created by the education department and stored on a volume of the file server.

Family Literacy & Transition:
Family Literacy & Transition information tracked through the HSFIS program.

Any individual files created by the family literacy & transition department and stored on a volume of the file server.

Health Department:
Health information tracked through the HSFIS program.

Any individual files created by the mental health department and stored on a volume of the file server.

Mental Health Department:
Mental Health information tracked through the HSFIS program.

Any individual files created by the mental health department and stored on a volume of the file server.

Special Services & Nutrition:
Special Services & Nutrition information tracked through the HSFIS program.

Any individual files created by the special services & nutrition department and stored on a volume of the file server.

Family Services:
Family Services information tracked through the HSFIS program.

Any individual files created by the family services department and stored on a volume of the file server.

The following table illustrates a sample of the tape backup log kept in use:

Hidalgo County Head Start Program File Server Tape Backup Log				
Tape Label	Dt Loaded	Dt Unloaded	Status	Comments
Monday	01/08/2001	01/09/2001	Normal	
Tuesday	01/09/2001	01/11/2001	Normal	
Wednesday			Aborted	Agency closed, tape contains Information from 01/03/2001
Thursday	01/11/2001	01/12/2001	Normal	
Friday	01/12/2001	01/15/2001	Normal	
Monthly	02/01/2001	02/02/2001	Normal	

The following table illustrates tape backup rotation:

Wk	Tape Label	Day/Time of Backup	Tape Contents	Tape Location
1	Monday	Monday at 11:59 p.m.	Full System Backup	Bring "Monday" tape from Edinburg center drop off "Friday" tape at off-site location.
1	Tuesday	Tuesday at 11:59 p.m.	Full System Backup	MIS Department/Rotate "Monday" tape with "Tuesday" tape.
1	Wednesday	Wednesday at 11:59 p.m.	Full System Backup	MIS Department/Rotate "Tuesday" tape with "Wednesday" tape.
1	Thursday	Thursday at 11:59 p.m.	Full System Backup	MIS Department/Rotate "Wednesday" tape with "Thursday" tape.
1	Friday	Friday at 11:59 p.m.	Full System Backup	Bring "Friday" tape from Edinburg center drop off "Monday" tape at off-site location.
2		Monday at 11:59 p.m.	Full System Backup/Overwrite Monday data of Week 1	Bring "Monday" tape from Edinburg center drop off "Friday" tape at off-site location.
2		Tuesday at 11:59 p.m.	Full System Backup/Overwrite Tuesday data of Week 1	MIS Department/Rotate "Monday" tape with "Tuesday" tape.
2		Wednesday at 11:59 p.m.	Full System Backup/Overwrite Wednesday data of Week 1	MIS Department/Rotate "Tuesday" tape with "Wednesday" tape.
2		Thursday at 11:59 p.m.	Full System Backup/Overwrite Thursday day data of Week 1	MIS Department/Rotate "Wednesday" tape with "Thursday" tape.
2		Friday at 11:59 p.m.	Full System Backup/Overwrite Friday data of Week 1	Bring "Friday" tape from Edinburg center drop off "Monday" tape at off-site location
2				

Urban County Program

Disaster Recovery Plan

Diana R. Serna, UCP Director

Urban County Program
Disaster Recovery Plan
Table of Contents

URBAN COUNTY PROGRAM DISASTER RECOVERY PLAN

Introduction

This document is the disaster recovery plan for the Urban County Program. The information presented in this plan guides Urban County management and technical staff in the recovery of computing information and facility operations in the event that a disaster destroys all or part of the facility.

Description

The Recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Urban County Program office at 1916 Tesoro Blvd., Pharr, Texas 78577. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

This plan will be available in the Urban County Library and additionally it will be distributed to each Urban County Manager. This plan will be updated on a regular basis as changes to the computing and facility operations are made. An extra copy will be kept in the Precinct #1 location.

Objectives and Overview

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. Urban County certainly is no exception to this trend. Today, each division of Urban County has computers with information vital to its operation. These machines are linked together by a network that provides communications with HUD servers. Vital functions of Urban County depend on the availability of this network of computers.

Consider for a moment the impact of a disaster that prevents the use of the system to process Payroll, Accounts Payable, IDIS connection, or any other vital application. It is hard to estimate the effects a disaster event might cause Urban County. One Hurricane could easily cause enough damage to disrupt these and other vital functions of Urban County. Without adequate planning and preparation to deal with such an event, Urban County's computer systems could be unavailable for many weeks, perhaps months.

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples Urban County's computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

All disaster recovery plans assume a certain amount of risk, the primary one being how much data is lost in the event of a disaster. Disaster recovery planning is much like the insurance business in many ways. There are compromises between the amount of time, effort, and money spent in the planning and preparation for a disaster and the amount of data loss you can sustain and still remain operational following a disaster. Time enters the equation, too. Many organizations simply cannot function without the computers they need to stay in business. So their recovery efforts may focus on quick recovery, or even zero down time, by duplicating and maintaining their computer systems in separate facilities.

The techniques for backup and recovery used in this plan do NOT guarantee zero data loss. The Program is willing to assume the risk of some data loss and do without computing for a period of time in a disaster situation. To put it in a more fiscal sense, the Program is saving funds in up-front disaster preparation costs, and then relying upon business interruption and recovery insurance to help restore computer operations after a disaster.

Data recovery efforts in this plan are targeted at getting the finance system up and running with the last available off-site backup tapes. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the period of the disaster forward.

This plan does not attempt to cover either of these two important aspects of data recovery. Instead, individual users and divisions will need to develop their own disaster recovery plans to cope with the unavailability of the computer systems during the restoration phase of this plan and to cope with potential data loss and synchronization problems.

Primary Objectives of the Plan

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to Urban County within 14 days of initiation of the plan.

2. Set criteria for making the decision to recover at Cold Site (Precinct #1) or repair the affected site.

3. Describe an organizational structure for carrying out the plan.

4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.

5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

Overview of the Plan

This plan uses a step-by-step approach to recovery from a disaster that destroys or heavily damages the computing resources of the Finance Division and Administrative Building at 1916 Tesoro Blvd in Pharr, Texas.

Personnel

Immediately following the disaster, a planned sequence of events will begin. Key personnel are notified and a staff recovery team will begin to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

In a disaster it must be remembered that some STAFF might not be available. The recovery personnel working to restore the computing systems will likely be working at great personal sacrifice, especially in the early hours and days following a disaster. The Program must be able to ensure that the recovery workers are provided with resources to meet their physical and emotional needs. This plan calls for the appointment of a person in the Administrative Support Team (DIRECTOR) whose job will be to secure these resources so they can concentrate on the task at hand.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, all magnetic storage media (hard drives, backup tapes/diskettes) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

A survey of the disaster scene will need to be conducted by appropriate personnel in order to estimate the amount of time required to put the facility back into working order. A decision is then made whether to use the Cold Site (Precinct #1), where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this plan.

Purchase of New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The Program will rely upon emergency procurement procedures documented in this plan and approved by the Director to quickly place orders for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been kept up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups

Data recovery will rely on the use of backups stored in a location off-site from the Program's Building. Backups can take the form of disk tapes, CDROMs, and other storage media. Early data recovery efforts focus on restoring the operating system of the Finance Division. Next, each of the Program's divisions will be restored with proper backup tapes, if applicable. Individual application owners may need to be involved at this point, so department staff will be required to ensure that data is restored properly.

A backup of the Finance Computer System is performed weekly. The backup is stored at the Precinct 1 location. In the event of a disaster at the Urban County location, the latest backup will be restored using the Precinct #1 computer containing the Finance System software. Backups will also occur prior to a forecasted natural disaster (i.e. hurricane).

Restore Application Data

It is at this point that the disaster recovery plans for users and department staff must merge with the completion of the Finance Division. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running applications database to the point of the disaster. They must also take all new data collected since that point and input it into the application database. When this process is complete, the Program's can begin normal operation. Some applications may be available only to a limited few key employees.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Cold Site (Precinct #1), physical restoration of the Program's Building will have begun. When the building is ready for occupancy, the systems assembled at the Cold Site are to be moved back to their permanent location. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the Cold Site.

Disaster Risks and Prevention

Fire

The threat of fire at the Building, especially in the storage area, is very real and poses the highest risk factor of all the causes of disaster mentioned here. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. Not to be forgotten are the attached office spaces, which could hold hidden dangers.

Preventive Measures

The Building is equipped with smoke detectors placed in the finance vault and others scattered widely throughout the building. Hand-held fire extinguishers are required in visible locations throughout the building. Staff is trained in the use of the fire extinguishers. Detailed instructions for dealing with fire are present and escape exit signs are placed throughout the building.

Flood

The building is located on high ground. There also is adequate drainage surrounding the building. However, a storm dropping large amounts of rain in the Pharr area can create a threat for flooding. Floodwaters penetrating the Finance area, especially submerging the floor, can cause a lot of damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. Of course, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel within the Finance area.

Preventive Measures

All Finance computer equipment, data storage boxes, and network surge protectors have been elevated from the floor by at least three feet. In addition, the Finance staff has been trained on shutting down the main electrical switch to the building located in the Finance vault. Periodic inspections of the under flooring of the finance area must be conducted to detect water seepage, especially any time there is a heavy downpour.

Computer Crime

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. However, internet viruses or unauthorized installations can affect data systems.

Preventive Measures

The Finance server will have security software installed to protect against unauthorized entry. All computers will be protected by passwords, especially those containing highly sensitive data. All users should be required to change their passwords on a regular basis. All systems should require a log and security administrators should review any errors on these logs on a regular basis. All systems should be backed up on a periodic basis. Those backups should be stored in an area separate from the original data. Standards will be established on the number of backup cycles to retain and the length of their retention.

Disaster Recovery Team

The Disaster Recovery Team is responsible for the coordination of the entire recovery plan. The Recovery Manager has the final authority on decisions that must be made during the recovery. The Recovery Manager is responsible for appointing the other members of the Team. The team is composed of the following individuals:

Recovery Manager

This individual is the problem solver who is accustomed to dealing with pressure situations. The individual must also have authority to delegate responsibilities, as there will be many problems arising that may not have been anticipated in advance. The individual must also have signature authority to expend funds as a part of the disaster recovery process.

Facility Coordinators

These individuals need to be highly skilled in a number of areas. They must have a strong background in the setup and interfacing of the Urban County Program. They will be responsible for assessing the damage to each division and reporting to the Manager.

Network Coordinator

This individual needs to be skilled in the area of the network design and maintenance. The individual should be trained in the diagnosing and correcting network outages and in connecting and debugging new additions to an existing network. The individual will assess the amount of damage to the computing system and report to the Manager.

Administrative Coordinator

This individual needs to be skilled in communicating with staff. The individual will be responsible for making contact with all other staff (See attachment #2) not involved in the immediate recovery process. The individual should also be able to deal with employees and their families during these times.

Current Recovery Management Team Roster

Position	Primary	Alternate
Recovery Manager	Diana R Serna	Miguel Mesa
Facility Coordinators	Jaime Ortega, Tony Barco	Pete De La Cruz
Network Coordinator	Maribel Lopez	Jaime Ortega
Administrative Coordinator	Nydia Vega	Irma Garza

Activating the Disaster Recovery Plan

The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Recovery Manager should designate where the Recovery Control Center is to be established. If a location in the Urban County Building is not suitable, Precinct 1 has been designated as the off-site location of the center.

The Recovery Manager sets the Plan into motion. Early steps to take are as follows.

1. The Recovery Manager should obtain an up-to-date copy of the Disaster Recovery Plan. Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team.

2. The Recovery Manager is to appoint new members to the Recovery Team, if previously designated members will not be available.

3. The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.

4. Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.

5. Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.

6. The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet or communicate each day for the first week of the recovery process.

7. The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective teams and call meetings to set in motion their part of the recovery.

8. Mobile communications will be important during the early phrases of the recovery process. This need can be satisfied through the use of cellular telephones. A list of each member's cellular telephone numbers will be provided.

Disaster Recovery – Finance Computer System

In order to facilitate recovery from a disaster, which destroys all or part of the Urban County Finance Computer System, certain preparations have been made in advance. This plan describes what has been done to lay the way for a quick and orderly restoration of the Division and the system it operates.

The following topics are presented in the plan:

- Recovery Facility
- Equipment Replacement
- Backups
- Media Storage Boxes

Recovery Facility

The Urban County Program has a number of options for alternate sites, each having a varying degree of up-front costs.

Hot Site

This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for very large organizations. A separate computer facility, possibly even located in a different city, can be built, complete with computers and other facilities ready to cut in on a moment's notice in the event the primary facility goes offline.

Disaster Recovery Company

A number of companies provide disaster recovery services on a subscription basis. For an annual fee you have the right to a variety of computer and other recovery services on extremely short notice in the event of a disaster. These services may reside at a centralized hot site or sites that the company operates, but it is necessary for you to pack up your backup tapes and physically relocate personnel to restore operations at the company's site. Some companies offer mobile services, which move the equipment to

your site in specially prepared vans. These vans usually contain all of the necessary computer and networking gear already installed, with motor generators for power, ready to go into service almost immediately.

Cold Site

A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the Finance Computer System while the primary site is being repaired.

The Urban County Program has chosen to use the cold site approach for **this** disaster recovery plan. The necessary arrangements are in place for the Finance Division to utilize space in the Precinct #1 Building as its Cold Site. The location has been outfitted with a computer system, which contains a copy of Fundware software and all other software applications used by the Finance Division. The location is currently used to house the weekly backups and has access to the internet in order to connect to HUD servers.

Equipment Replacement

This plan contains a complete inventory of hardware requirements of the Finance network system and the software that must be restored after a disaster (See attachment #1). The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current system configuration. Where possible, agreements have been made with vendors (RTI Sales & Service) to supply replacements and technical assistance in an event of emergency. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The Recovery Management Team will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

Backups

New hardware can be purchased. New buildings can be built. New employees can be hired. But the data that was stored on the damaged equipment cannot be bought at any price. It must be restored from a copy that was not affected by the disaster. There are a number of options available to us to help ensure that such a copy of your data survives a disaster at the primary facility.

The Urban County Program has chosen to use the off-site tape backup restoration approach. This option calls for the transportation of backup tapes made at the primary computer facility to an off-site location. Choice of the location is important. You want to ensure survivability of the backups in a disaster, but you also need quick availability of

the backups. The Finance Division makes a backup tape every Friday. The backup is then stored in a media box in Precinct #1. The backup will also be installed on the off-site computer on weekly/monthly basis.

This option has some drawbacks. First, there is period of exposure from the time that a backup is made, to the time it can be physically removed off-site. A disaster striking at the wrong time may result in the loss of all data changes that have occurred from the time of the last off-site backup. There is also the time, expense, and energy of having to transport the tapes. And there is also the risk that tapes can be physical damaged or lost while transporting them.

The Urban County Program has opted to taking periodic backups of its Finance System and restoring those backups at the Precinct #1 location. Existing tapes from Precinct #1 are relocated to the Urban County Program and stored in Media boxes. They are retained until the next set up backups are made and restored, and then released to scratch status. Then the cycle starts all over again.

The actual backup and cycling procedures may vary somewhat depending on the workweek and amount of tapes available.

Media Boxes

To ensure that an up-to-date copy of this plan is available when disaster occurs, procedures have been established to store a copy of the plan with other important recovery information at the Cold Site backup tape storage area. Two Media boxes have been purchased to hold these materials. The contents of both boxes are identical. One resides at the Precinct #1 location, the other in the Finance vault in the Urban County Building.

When changes to the contents of the boxes are necessary, the box at the Urban County Building is first updated, then it is take over to Precinct 1 and swapped with the box stored there. That box is returned to Urban County and updated and replaced in the Finance Vault. This ensures that at least one copy of the plan is available at the recovery site.

Contents of Media Boxes

1. Weekly Backup Tape
2. Copy of Disaster Plan
3. Copies of Software
4. List of Financial Bank Accounts
5. List of Contacts

The Finance Manager will update each media box on a monthly basis to ensure current information.

Anne R Jeans
Approving Official

4-19-05
Date

ATTACHMENT #1

Intuit FundWare

IMPORTANT NOTICE: *PLEASE READ*

April 7, 2004

Dear Valued Client:

Intuit will end support of FundWare 5.x versions on July 1, 2006.

Many of you have developed a strong loyalty to our character-based versions of FundWare. We appreciate your support! In fact, some of you have told me personally that even though you've purchased 7.x, you haven't installed it, and others plan to stay on 5.8 until the very last day. Well, that day is coming, and we're giving you plenty of notice.

The good news is that extensive surveys have found a **substantial increase in satisfaction** for clients using newer versions of FundWare. So, we are excited for you to make this transition so you too can enjoy the many benefits of the newer product line.

After listening carefully to your comments, we have taken some creative steps to make your transition as smooth as possible:

- **We have allowed more than two years for you to make this transition.** Many of you have told us that you want extra time to work through your budget cycles. The support department will still help you during this interim period, and you will continue to receive W2 and 1099 updates for this year and next.

- **We have created additional options for clients that struggle with hardware upgrade costs.** We've teamed with a vendor that can provide re-furbished options when cost-effectiveness is paramount.

- **We can refer you to a leasing provider** if you prefer to spread upgrade costs, including software, hardware and services, over a longer period. Leasing provides very affordable monthly payments instead of a large one-time up-front payment.

- **We are also offering 0% financing** now through July 31, 2004. Since this is for a limited time, call today.

- **Intuit FundWare version 7.30, releasing soon, will be our best yet.** Many long-standing client issues are addressed in this latest version. Also, this is the first version of FundWare that incorporates some of Intuit's famous best practices to make our software easier to use. Attend a webcast seminar to see for yourself! (www.intuitfundware.com/clients)

- **We encourage you to move quickly.** Take advantage of the new 7.30 benefits sooner rather than later! To avoid a disruptive rush at the end of the transition period, call your client sales representative or your Authorized FundWare reseller today. We stand ready to help you make the transition as quickly, smoothly and as cost efficiently as possible.

Please contact your Authorized FundWare reseller or your Intuit client sales representative (800-551-4458) to get started on a specific transition plan for your organization.

Thanks for being our client! Many of you have worked with us for many years — we look forward to many more.

Sincerely,

Michael Potts
Vice President, Intuit Public Sector Solutions

Intuit FundWare

Hardware Requirements

Fundware Professional Edition 1-8 user environments

January 30, 2004

Revised April 12, 2004

Table of Contents:

Supported Platforms

The Server Operating Systems supported for use with 7.30 Intuit Fundware products are Windows 2003 and Windows 2000.

The Server Operating System supported for use with 7.20 Intuit Fundware products is Windows 2000 ONLY.

Intuit Public Sector Solutions does not support the use of packaged operating systems such as Windows Small Business Server, BackOffice Server, or Project server on the application server.

Intuit Public sector Solutions does not support the application server being used as any type of domain controller. The domain controller must be a separate server within the network environment.

The current Workstation Operating Systems supported for use with Intuit Fundware products are Windows 2000 Professional and Windows XP Professional.

Any workstation operating systems supported as Terminal Server Clients may be used. (Win 95, Win 98, Win NT, etc.)
Microsoft requires additional Licensing for Terminal Services use with these workstation platforms. Microsoft now requires that all workstation platforms are licensed for Terminal Services use if you are using Windows 2003.

Standalone Environment

System Component	Minimum Requirements	Recommended Configuration
General	Windows 2000 Professional or Windows XP Professional	Windows 2000 Professional or Windows XP Professional
Processor (CPU)	Pentium III 600 MHz	Pentium IV 2.0+ GHz
Number of Processors	Single (1 processor)	Single (1 processor)
Memory (RAM)	256MB	512MB -1GB
Disk Requirements	One IDE drive with 20 GB capacity & speed of 7200 rpm	One IDE drive with 20 GB capacity & speed of 7200 rpm
Fault Tolerance	None	None
CD-ROM	Required	Required
Network Cabling	100 Base-T Category 5	100 Base-T Category 5
Network Interface Card	10Mbs/ 100Mbs	10Mbs/100Mbs
Back-up Device	Required *	Required *
Server Price Range	499.00-1000.00	699.00-1500.00

* The backup device can be internal or external Tape drives, a CD Read/Writable device or another device capable of creating backup media (Zip drive, Jazz Drive, etc.) separate from the host computer.
Copying files from the FundWare locations to other locations on the local computer is not acceptable.

2-3 Fundware Users

System Component	Minimum Requirements	Recommended Configuration
General	Dedicated Windows 2003*/2000 Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.	Dedicated Windows 2003*/2000 Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.
Processor (CPU)	Pentium III 800 MHz	Pentium IV 2.0+ GHz
Number of Processors	Single (1 processor)	Single (1 processor)
Memory (RAM)	512MB	756MB -1GB
Disk Requirements	Two IDE drives with min. 40 GB capacity 7200 rpm	Three SCSI drives with min. 18 GB capacity 10,000 rpm
Fault Tolerance	IDE RAID controller with 64 MB Cache configured with a Raid Level 1.	RAID controller with 128 MB Cache configured with a Raid Level 5.
CD-ROM	Required	Required
Network Cabling	100 Base-T Category 5	100 Base-T Category 5
Network Interface Card	10Mbs/ 100Mbs	10Mbs/100Mbs
Back-up Device	Required	Required
Server Price Range	1500.00-3500.00	2200.00-4200

*Version 7.30 is supported on Windows 2000 and 2003 Server operating system but 7.20 is only supported on Windows 2000 Server.

Workstation Hardware Requirements

System Component	Minimum Requirements	Recommended Configuration
General	Windows 2000 or XP Professional	Windows 2000 or XP Professional
Memory (RAM)	128 MB (Check specific Operating system requirements)	256 MB (Check specific Operating system requirements)
Disk Space	1000 MB	1000 MB
Monitor	17" SVGA. Monitors must have a resolution of at least 800 x 600	19" SVGA. Monitors must have a resolution of at least 800 x 600

3-5 Fundware Users

Server Component	Minimum Requirements	Recommended Configuration
General	Dedicated Windows 2003*/2000 Terminal Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.	Dedicated Windows 2003*/2000 Terminal Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.
Processor (CPU)	Pentium III 800 MHz	Pentium IV 2.0+ GHz
Number of Processors	Single (1 processor)	Single (1 processor)
Memory (RAM)	512MB	756MB -1GB
Disk Requirements	Two IDE drives with min. 40 GB capacity 7200 rpm	Three SCSI drives with min. 18 GB capacity 10,000 rpm
Fault Tolerance	IDE RAID controller with 64 MB Cache configured with a Raid Level 1.	RAID controller with 128 MB Cache configured with a Raid Level 5.
CD-ROM	Required	Required
Network Cabling	100 Base-T Category 5	100 Base-T Category 5
Network Interface Card	10Mbs /100Mbs	100 Mbs/1000Mbs
Back-up Device	Required	Required
Server Price Range	1,500.00-3,500.00	2,200.00-5,500.00

*Version 7.30 is supported on Windows 2000 and 2003 Server operating system but 7.20 is only supported on Windows 2000 Server.

Workstation Hardware Requirements

System Component	Minimum Requirements	Recommended Configuration
Processor (CPU)	Pentium II 400+ MHz	Pentium III 600+ MHz
Memory (RAM)	128 MB (Check specific Operating system requirements)	256 MB (Check specific Operating system requirements)
Disk Space	1000 MB	1000 MB
Monitor	17" SVGA. Monitors must have a resolution of at least 800 x 600	19" SVGA. Monitors must have a resolution of at least 800 x 600

5-8 Fundware Users

Server Component	Minimum Requirements	Recommended Configuration
General	Dedicated Windows 2003*/2000 Terminal Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.	Dedicated Windows 2003*/2000 Terminal Server for Intuit FundWare. NOTE: If more than 2 users Terminal Server is required.
Processor (CPU)	Pentium III 800 MHz	Pentium IV 2.0+ MHz
Number of Processors	Single (1 processor)	Single (1 processor)
Memory (RAM)	756MB - 1GB 1.5GB	1GB – 1.5 GB
Disk Requirements	Three SCSI drives with min. 18 GB capacity 10,000 rpm	Three or Four SCSI drives with min. 18 GB capacity 10,000+ rpm
Fault Tolerance	RAID controller with 128 MB Cache configured with a Raid Level 5	RAID controller with 128 MB Cache configured with a Raid Level 5 or RAID Level 10.
CD-ROM	Required	Required
Network Cabling	100 Base-T Category 3	100 Base-T Category 5
Network Interface Card	10Mbs /100Mbs	100 Mbs/1000Mbs
Back-up Device	Required	Required
Server Price Range	1,500.00-3,500.00	2,200.00-5,500.00

*Version 7.30 is supported on Windows 2000 and 2003 Server operating system but 7.20 is only supported on Windows 2000 Server.

Workstation Hardware Requirements

System Component	Minimum Requirements	Recommended Configuration
Processor (CPU)	Pentium II 400+ MHz	Pentium III 600+ MHz
Memory (RAM)	128 MB (Check specific Operating system requirements)	256 MB (Check specific Operating system requirements)
Disk Space	1000 MB	1000 MB
Monitor	17" SVGA. Monitors must have a resolution of at least 800 x 600	19" SVGA. Monitors must have a resolution of at least 800 x 600

ATTACHMENT #2

EMPLOYEE NAME	ADDRESS	PHONE
SERNA, DIANA R	220 LAS PALMAS DRIVE	(956) 514-1618
GARZA, IRMA	P.O. BOX 1733	(956) 381-0786
VEGA, NYDIA O.	1701 N 83RD STREET	(956) 383-4832
SANDOVAL, LINDA	BOX 1804	(956) 782-7726
DE LA CRUZ, PEDRO	301 JUANITA ST.	(956) 262-2448
GOMEZ, JOSE ESTEBAN	1209 IMA	(956) 383-7144
ORTEGA, JAIME	321 QUARTZ ST	(956) 381-1154
MORIN, NELLIE N	PO BOX 560	(956) 262-7873
BAZAN, HILDA G.	1008 SOUTH 20TH STREET	(956) 585-0669
GOMEZ, ELIZABETH	3336 MIDLAND CIRCLE	(956) 534-0594
MARTINEZ, FRANCISCO MARIO	P.O. BOX 6643	(956) 381-8025
GARZA III, LUCIANO S	1704 W. SIXTH STREET	(956) 968-5304
GARZA, OSCAR	1710 BASHAM ST.	(956) 581-1127
OZUNA, NINFA G	PO BOX 203	(956) 381-8535
GARCIA, GUADALUPE V	PO BOX 470	(956) 262-1433
BARCO, ANTONIO	P.O. BOX 2205	(956) 262-7904
LOPEZ, MAREVEL	P.O. BOX 449	(956) 380-0539
MENDOZA, MICHELLE L	922 VIA SOL	(956) 316-1618
CASIANO, HECTOR P	402 W SILVER	(956) 464-8162
MESA, MIGUEL E	308 WEST STUBBS	(956) 316-2403
BARRON, JOSE A	BOX 2311	(956) 781-3137
LUMBRERAS, JOSE LUIS	2819 E MESQUITE	(956) 929-4595
DE LA GARZA, STEVEN	P.O. BOX 976	(956) 262-7872
LEAL, MONICA	819 DENVER ST.	(956) 383-0508
LUNA, MONICA	5662 W SCHUNIOR	(956) 929-6413
GUERRA, MONICA	1414 N 4TH	(956) 655-1709

ATTACHMENT #3

Date: 07/11/05

From: Fernando Cantu Jr., Account Reports Specialists
To: Armando Barrera Jr., Hidalgo County Tax Assessor Collector

Subj: STANDARD OPERATION PROCEDURE FOR NATURAL DISASTER OR NATIONAL EMERGENCY.

The following documents are the Hidalgo County Tax Office SOP dealing with emergency and natural disaster.

The two major concerns to these instructions are to secure the data on the ATC system, and to protect the electronic property of the Tax Office. There are two check-off sheets and a set of instructions on how to fill out each.

SOP INSTRUCTION FOR NATURAL DISASTER

Note 1: These instructions should be carried out as time and safety of life is permitted. In case of immediate danger follow the SOP instructions for national or immediate emergency.
Note 2: All hard copies of delinquent tax rolls and complete bill listings are located inside vault near assessing department.

Step 1. Go to Appendix A of this manual. Make a copy of Appendix A.

Step 2. Fill out date, time, your name, nature of emergency and estimated time allowed for preparation.

Step 3. Create Collections Transfer Tape 8,15.

1. Entity	: all
2. Year	: all
3. Paid bills	: yes
4. P&I/Disc/Attfee	: yes
5. As of Date	: T
6. Conf Owner Info	: yes
7. EBCDIC tape	: no
8. File Type	: Flat
9. File Name	:/tsg/tax/fernando/HidalgoCollTape
10. Wait before making tape	: n/a
11. Print Totals	: yes
12. Printer for Totals	: TSG-HS

Burn Copy to DVD.
FTP copy to Columb Group, San Antonio

Step 4. Make backup. Insert blank tape at county courthouse MIS. Log into AIX ROOT prompt. Type the following at root prompt and hit return.

tar –cvf /dev/rmt0 ./usr/tsg/tax

Step 5. Securing tapes. If time and conditions allow it, remove all backup tapes from the tax office computer room and place them in the auditor's vault. If this is not feasible place them in the collections vault.

Step 6. Log out all users. Call all the different entities, banks, attorneys, and mortgage companies that log into the ATC system through modem that your intentions are to secure all computers and are requesting them to log out. Walk around the collections and assessing department and tell all users to log out. Place a message on the time clock saying, "THE TAX OFFICE COMPUTER SYSTEM WILL BE DOWN UNTIL FURTHER NOTICE."

Step 7. Secure system racks. There are two system racks located at the back of the computer room. Turn off all devices including HUBS, MODEMS, ROUTERS, MUXES, CONCENTRATORS, TRANSCEIVERS, POWER SURGE STRIPS, UPS, ETC. Secure Snap Server, place in appropriate container, and place in cashier vault. Secure all power trips and UPS to be at least one foot of the ground.

Step 8. Secure all electrical devices. Go around both collections and assessing and unplug all electrical devices from the electrical outlets in the wall and floor.

Step 9. Secure building. Place sandbags and board up windows if necessary. Turn off all lights and lock the building.

Step 10. Evacuate area. Make sure you have located the nearest shelter available to you or that you know of the designated routes in leaving the area in case of a direct hit from a Hurricane. Log out the Date and time of evacuation on check off sheet.

CHECK OFF LIST FOR NATURAL DISASTER EMERGENCY

DATE _____ TIME: _____

NAME: _____

EMERGENCY DISC: _____

ESTIMATED TIME BEFORE EVACUATION: _____

___ MAKE COLLECTIONS TAPE FOR INTERNET (18 HOURS)

___ MAKE TAR BACKUP (4 HOURS)

___ SECURE TAPES (20 MIN)

___ LOG OUT ALL USERS (20 MIN)

___ SECURE SYSTEM RACKS (30 MIN)

___ SECURE SNAP SERVER (5 MIN)

___ SECURE ALL ELECTRICAL DEVICES (1 HOUR)

___ SECURE BUILDING (10 MIN – 2 Hrs)

___ EVACUATE AREA DATE:_____ TIME:_____

APPENDIX A

CHECK OFF LIST FOR IMMEDIATE THREAT EMERGENCY

Time:_____

Emergency Description:_____

___ Secure System racks

___ Secure Backup tapes

___ Secure Snap Server

___ Secure building

___ evacuate Area

APPENDIX B

SOP INSTRUCTIONS FOR NATIONAL OR IMMEDIATE THREAT EMERGENCY

Note 1: These instructions are superseded by any policy or instructions set forth at the county judge level. Be aware of county contingency plan in evacuating building in case of bomb threat or fire emergencies.

These instructions should be carried out as time and safety of life is permitted. Depending on Duress of the impending emergency, do as many of the following steps as posible.

Step 1. Remove Appendix B from the end of this pamphlet. Fill out time and nature of emergency.

Step 2. Secure system racks. Go to the back of computer room. Power down all the devices including HUBS, MODEMS, ROUTERS, MUXES, CONCENTRATORS, TRANSCEIVERS, POWER SURGE STRIPS, UPS, ETC.

Step 3. Secure Snap Server, place in appropriate container, and place in cashier vault or walk out with it as time allows.

Step 4. Evacuate and secure building.

Step 5. In case of National emergency evacuate area through designated routes.

Hidalgo County Health Department

Disaster Recovery Plan

Part I. Introduction and Overview

INTRODUCTION

Crisis management is the enterprise s first response to an event that could change the way business operations are normally conducted. A well-managed approach to such an event will help significantly to ensure the employees, clients, partners, and the general public will continue to have confidence in the functionality of the Health Department.

This Disaster Recovery Plan focuses on the recoverability of the Hidalgo County Health Department's main computing facility at Hidalgo County Health Department Administration Building, 1304 S. 25th Ave., Edinburg, TX 78539.

Overview

Section 1.01 Statement of Purpose

This document describes the data center disaster recovery plan for the Hidalgo County Health Department. It details how the various organizational units intend to carry out their responsibilities in the event of a disaster. And it also describes the provisions and safeguards, which are undertaken in preparation for such a contingency.

The Plan is supported by Management and has the objective to provide for a cost effective and documented method for responding to a disaster that may disrupt the ongoing computer operations of Hidalgo County Health Department. As such, the Plan is primarily intended to serve as a predefined resource that would aid Management during and following a significant crisis that impairs and affects the computer hardware, software, networks, telecommunications, and the administrative information systems.

Definition: A disaster is "an occurrence inflicting widespread destruction and/or distress." For the purposes of this document this means that the facilities, computing resources, or major components thereof, are deemed unavailable for operations.

The following are the major purposes of this document:

(a) To plan for ongoing operations in the event of a disaster.
(b) To detail and describe the level of contingency preparations for management review.
(c) To prioritize and outline the recovery of pre-defined critical components, systems, and applications.
(d) To develop an organizational preparedness so that disruption and chaos are minimized if a disaster should occur.
(e) To anticipate vulnerabilities regarding the security and protection of the corporate data center facilities.

Section 1.02 Scope of the Plan

The scope of this plan is limited to the services and responsibilities of the Hidalgo County Health Department for Information Services and covers these major resources:

(a) computing facilities
(b) computer hardware and systems software
(c) enterprise network electronics, transport, and ISP access
(d) telecommunications equipment, software, and services
(e) databases, electronic media and files
(f) computer programs
(g) computer execution and operation's procedures
(h) documentation

The disaster recovery plan provides only for the continuation of certain essential technology services and administrative information processing activities during the period of time, which may be required for recovering from a disaster.

Section 1.03 Procedure for Assessing the Magnitude of a Crisis

The Disaster Assessment Team will confer about the presenting crisis in an effort to classify the magnitude of the crisis as defined within this plan. The Disaster Assessment Team will be comprised of the following members:

(a) The Chief Administrative Officer
(b) The Chief Financial Officer
(c) The Network Manager
(d) The System Support Specialist

Crisis Designations

The following are potential crisis classifications that the Crisis Assessment Team may designate:

Category 3 - A major disruption in service affecting a subset of users or systems deemed to be non-critical for alternate site recovery.

Category 2 - Major disruption to one or more sites.

Category 1 - A Total system(s) outage affecting all systems, and sites.

Section 1.04 Procedures for Communicating Internally

(a) **Telephone based communications** : Using telephone trees and distributed calling responsibilities, pertinent Health Department officials and staff will be notified once a disaster is declared.

(b) **Voice Mail** : Emergency announcements can be disseminated internally using overall existing voice mail announcement capabilities. This would entail delivering a recorded and stored message to all voice mail users who will receive the message upon their next use of the voice mail systems. The voice mail distribution capability falls under the auspices of Telecommunications Services and represents an efficient and economical means to deliver an official message rapidly to a broad internal audience.

(c) **Mail based communications** : If electronic mail facilities continue to be functional, list serve capabilities and available grouping characteristics can be used to target the message to one or more population segments within the enterprise.

If electronic mail capabilities are not adequately available for this requirement, third party Internet Service Provider (ISP) email facilities will be used to attempt contact with staff. It is recognized that not all individuals possess ISP accounts, but for those who do, this is a viable communication method.

Section 1.05 Built-in Plan review Procedures and Schedule

Reviewing the Plan: To assure the Plan's continued accuracy and viability, the Network Manager shall review the Disaster Recovery Plan periodically. Maintenance of the plan and overall coordination of plan activities (such as rehearsals and unit activities) will be performed by the Disaster Assessment Team

Part II. Plan Strategies

Section 2.01 Contingency Site

The Health Department will use one of the remote clinic sites as a contingency site. Equipment available at that site and any of the other clinics will be utilized as needed to restore the network functionality.

Section 2.02 Backup Environments Network Equipment

Any and all hardware and any of the viable clinic sites will be utilized to restore network functionality to the Hidalgo County Health Department.

Section 2.03 Applications Analysis

An analysis of critical application and key processing components has been performed to identify and prioritize recovery efforts. These applications are considered business critical and must be included in any recovery plan to sustain the operational/financial viability of the Health Department.

Hidalgo County Health Department

- TWICES System (client record system)

- SDI System (Medical Billing System)
- Human Resources System
- Access to Financial Accounting System
- Health Permitting System
- Nursing Certification System
- E-mail System

Section 2.04 Local and Off-site Media and Backup Storage

System backups are maintained on magnetic tape media for all critical systems for the purpose of operational and disaster recovery. Multiple versions of backups are maintained on a weekly basis (unless otherwise specified by application backup requirements). The most recent version of the backups are rotated through an offsite storage. This ensures that recovery of any system is at most a week old.

Section 2.05 - Telecommunication Services

Local Telephone Service : Southwestern Bell Telephone provides incoming and outgoing local telephone lines to the telephone system. In the event that the SBC serving wire center experiences a catastrophe, SBC has established plans which they will activate.

Long Distance Service : AT&T outgoing long distance service will be available as soon as SBC establishes outgoing dial tone.

Nortel Networks PBX System : The Phone Den is charged with the responsibility of fully restoring service to the PBX System when we have experienced a catastrophic event which has resulted in service outages or damaged equipment. The procedure calls for a complete system replacement within 24 hours.

Nortel Networks Voice Mail System: A NAM 6 voice mail system is installed at the Hidalgo County Health Department Administration Building. The Phone Den is charged with the responsibility of fully restoring service to the Voice Mail System when we have experienced a catastrophic event which has resulted in service outages or damaged equipment. The procedures calls for a complete system replacement within 24 hours.

Part III. Disaster Response Actions

The below actions can only be undertaken when a disaster classification of Category 1 exists: as defined in part I of this document. All communications shall explain and include reference to the defined nomenclature of the disaster classification.

Section 3.01 Implementation of the Plan

Once the classification of a disaster is made, and it is determined that disaster conditions exist, the disaster plan is to be implemented immediately. This step is undertaken formally once the management notifications under the Plan begin.

The end disaster conditions must also be communicated formally through such management notifications.

Section 3.02 Plan Execution

The detailed recovery plans will be implemented once the disaster has been declared.

Section 3.03 End of Disaster State

Formal notice of the end of a disaster state shall be given as per the management notifications in section B of this part. In addition, users shall be notified as per section C of this part. Depending on the characteristics and duration of the disaster, this notification may not entail a complete return to normal processing schedules. However, this notification shall signal the end of specific disaster operations.

Part IV Disaster Plan Testing

Tests of the disaster plan, or of one or more of its facets, will be conducted periodically and/or may be requested by management to insure that elements of the plan are feasible, compatible, and effective. An objective of this testing will be to minimize interference and interruption of the normal production operations. While most exercises are performed on a scheduled basis, an unannounced recovery may be conducted to validate preparedness for unanticipated outages.

Part V. Facilities Restoration

The objective of Facilities Restoration is to establish a viable/ongoing processing facility to which to return computing operations from the contingency site. This may require an extended period of time depending on the crisis event experienced and the extent to which the original data center facility is unacceptable for ongoing operations.

Office of the Attorney General – Child Support Division

Certificate of Destruction for Contractors and Vendors **ATTACHMENT H**

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

Contact Name	Title	Company Name and Address	Phone

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

Media Type				Media Title / Document Name			
	HARD COPY		ELECTRONIC				
Media Description (Paper, Microfilm, Computer Media, Tapes, etc.)							
Dates of Records							
Document / Record Tracking Number				OAG Item Number		Make / Model	Serial Number

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

Comments:

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

Description of OAG Data Retained and Retention Requirements:		
Proposed method of destruction for OAG approval:	Type of storage media?	
	Physical location?	
	Planned destruction date?	

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

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

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

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

Send the signed Certificate of Destruction to:

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

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

INSTRUCTIONS FOR CERTIFICATE OF DESTRUCTION

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

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

There are two primary types of media in common use:

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

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

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

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

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

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

6. Send the signed Certificate of Destruction to:

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

FAX to: 512-460-6070

or send as an email attachment to:

Willie.Harvey@cs.oag.state.tx.us

Final Distribution of Certificate	Original to:	Willie Harvey, Information Security Officer 512-460-6764
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. CSD Contract Manager