# Disaster Recovery Plan

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: 2/6/2008

## *Table of Contents*

### Table of Contents

# *Plan Overview*
# *Disaster Recovery Plan*

2/6/2008

**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*

2/6/2008

***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<br>- TWICES System ( Client record system)<br>- 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

2/6/2008

**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**<br>Technical Support | *Work Phone* | 706-312-3500 |
| **Dell**<br>Customer Support | *Work Phone* | 1800-981-3355 |
| **AT&T**<br>Customer Service | *Work Phone* | 1800-332-4387 |
| **Reliant Energy**<br>Yesenia Zamarron | *Work Phone* | 713-497-3082 |
| **Excel Meridian - Technical Support**<br>Technical Support | *Work Phone* | 1800-995-1014 |

# *Application Details*

2/6/2008

**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

# *Alternate Site in Plan Details*
# *Disaster Recovery Plan*

2/6/2008

**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*
2/6/2008

**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

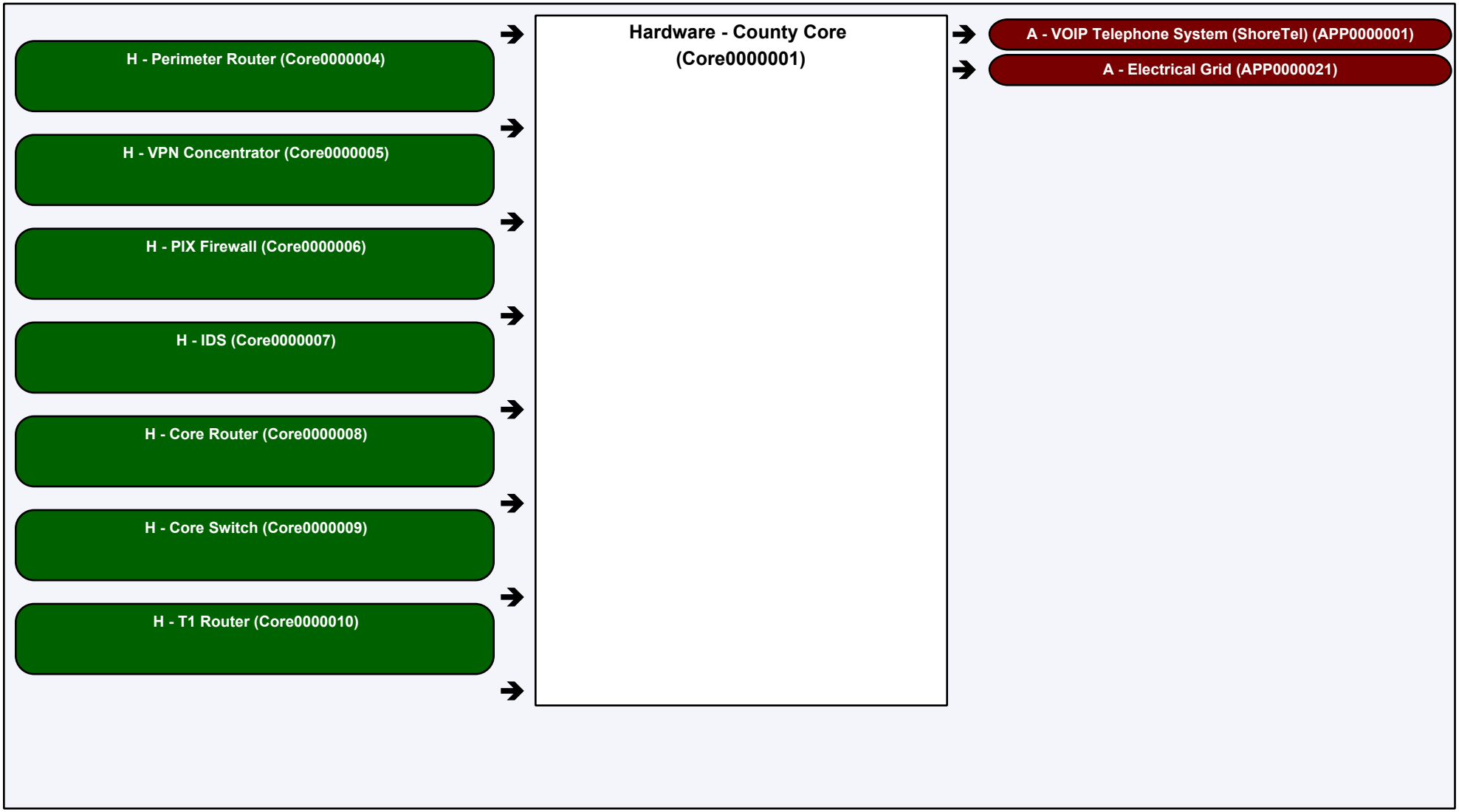
**Team Leader**
Health - Team Leader
Eduardo Olivarez, Health Department

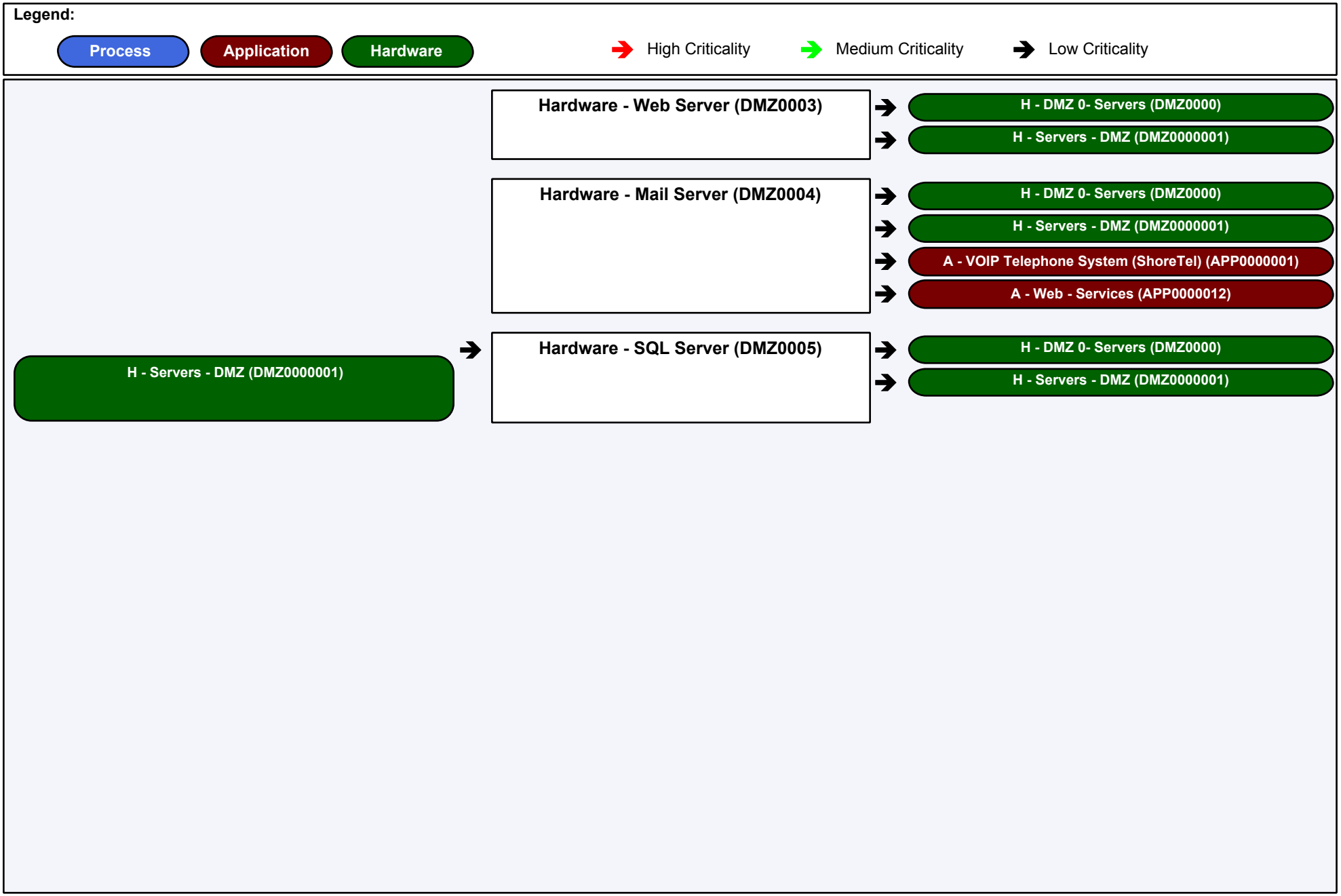
**Team Leader Alt**
Health - Team Leader Alternate
Rigo Hinojosa, Health Department

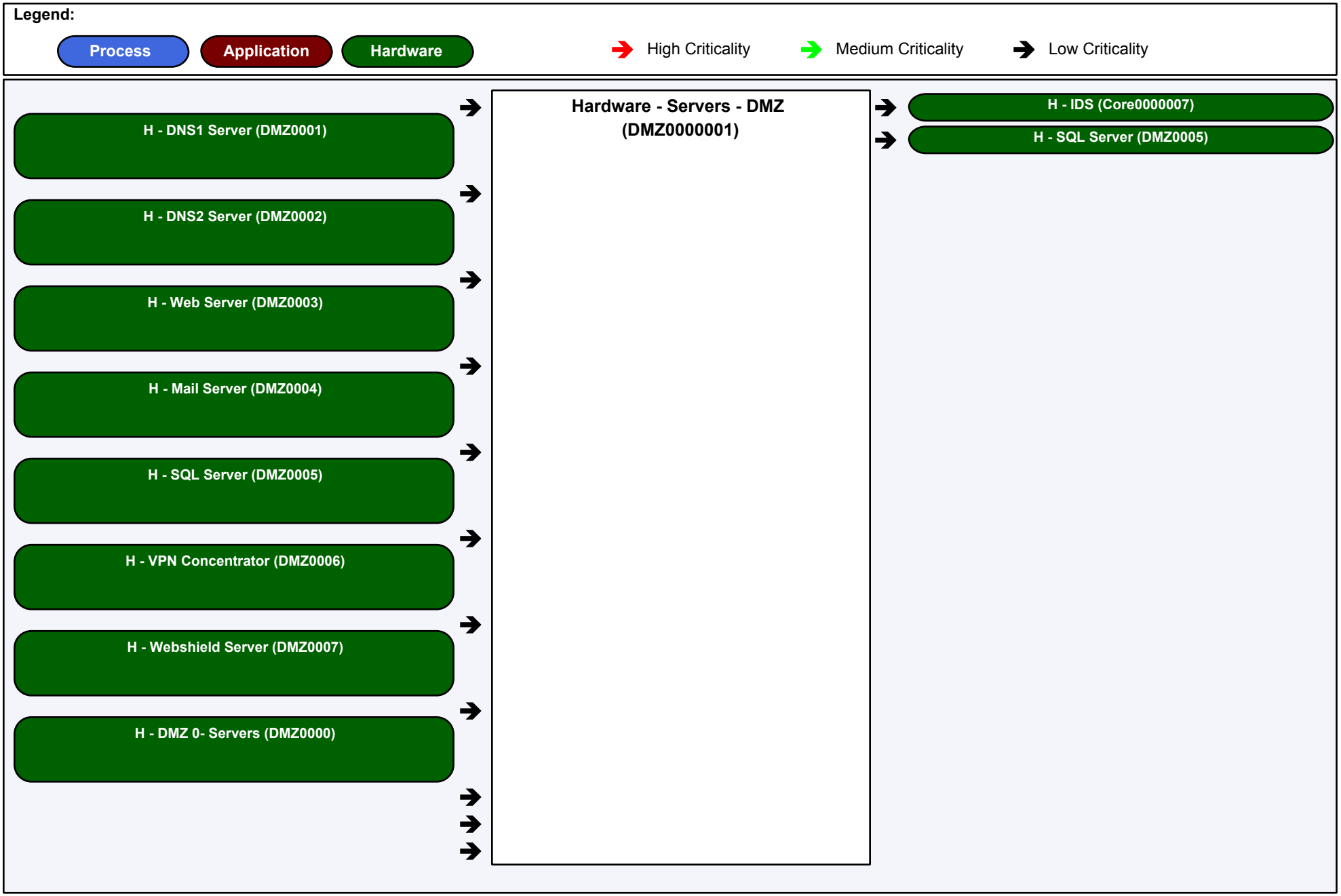
**Report Description:**
This report graphically depicts core components with up and downstream interdependencies.

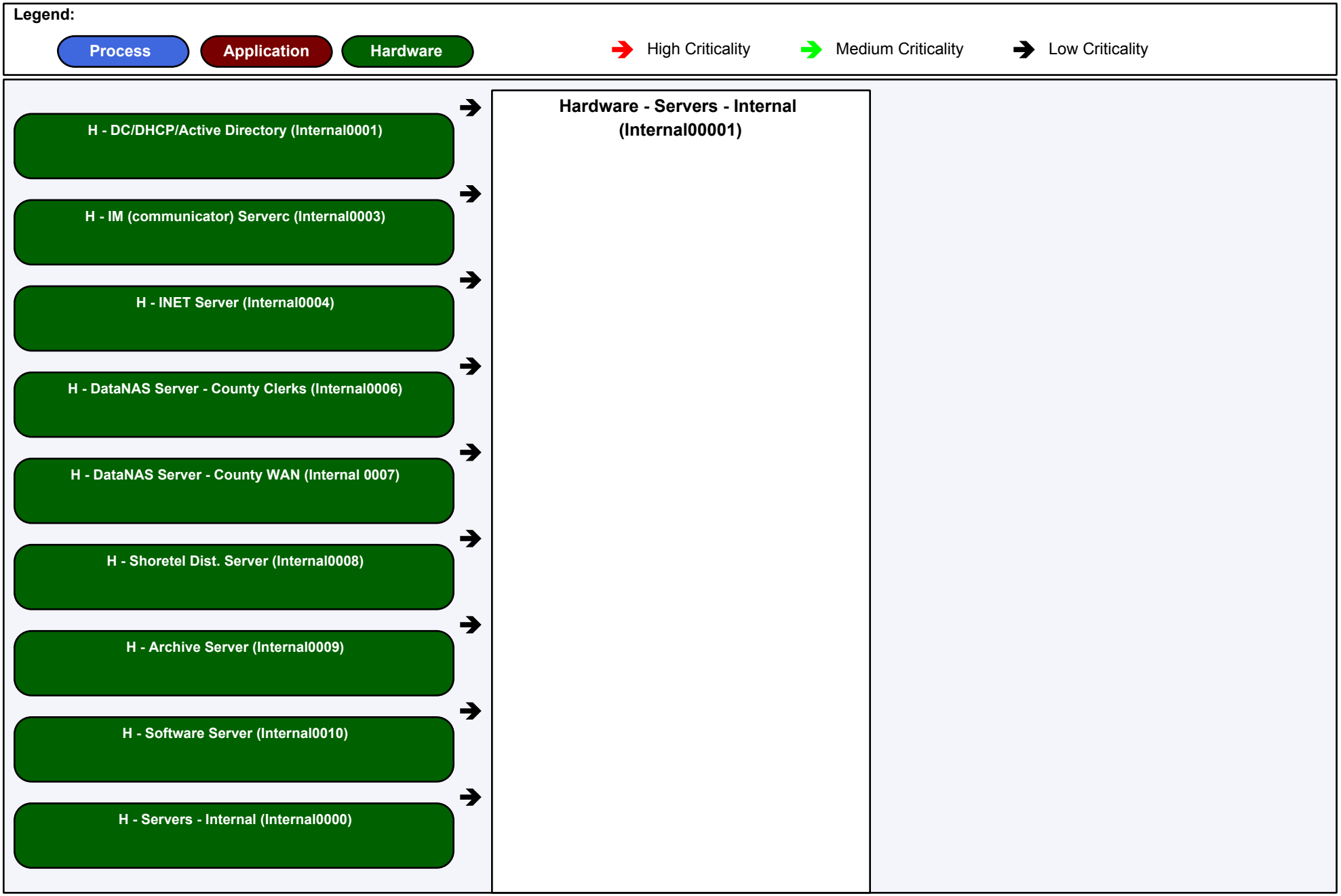
**Legend:**

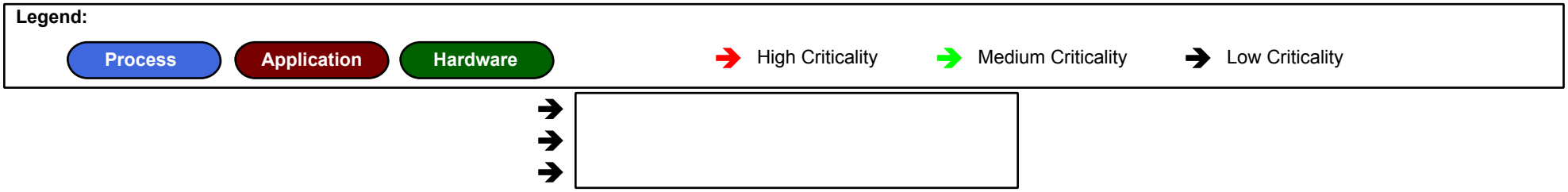
Process | Application | Hardware | High Criticality | Medium Criticality | Low Criticality

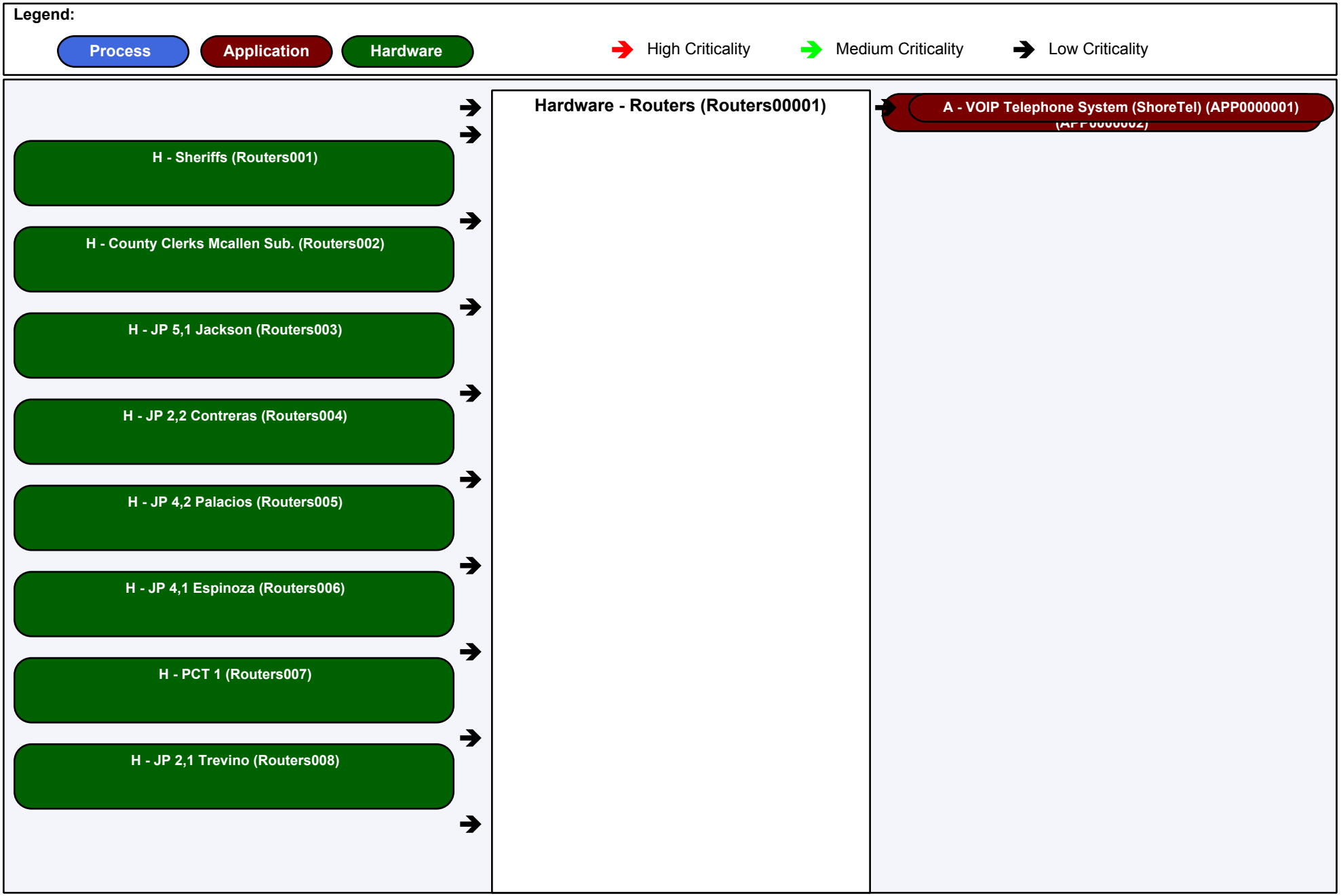


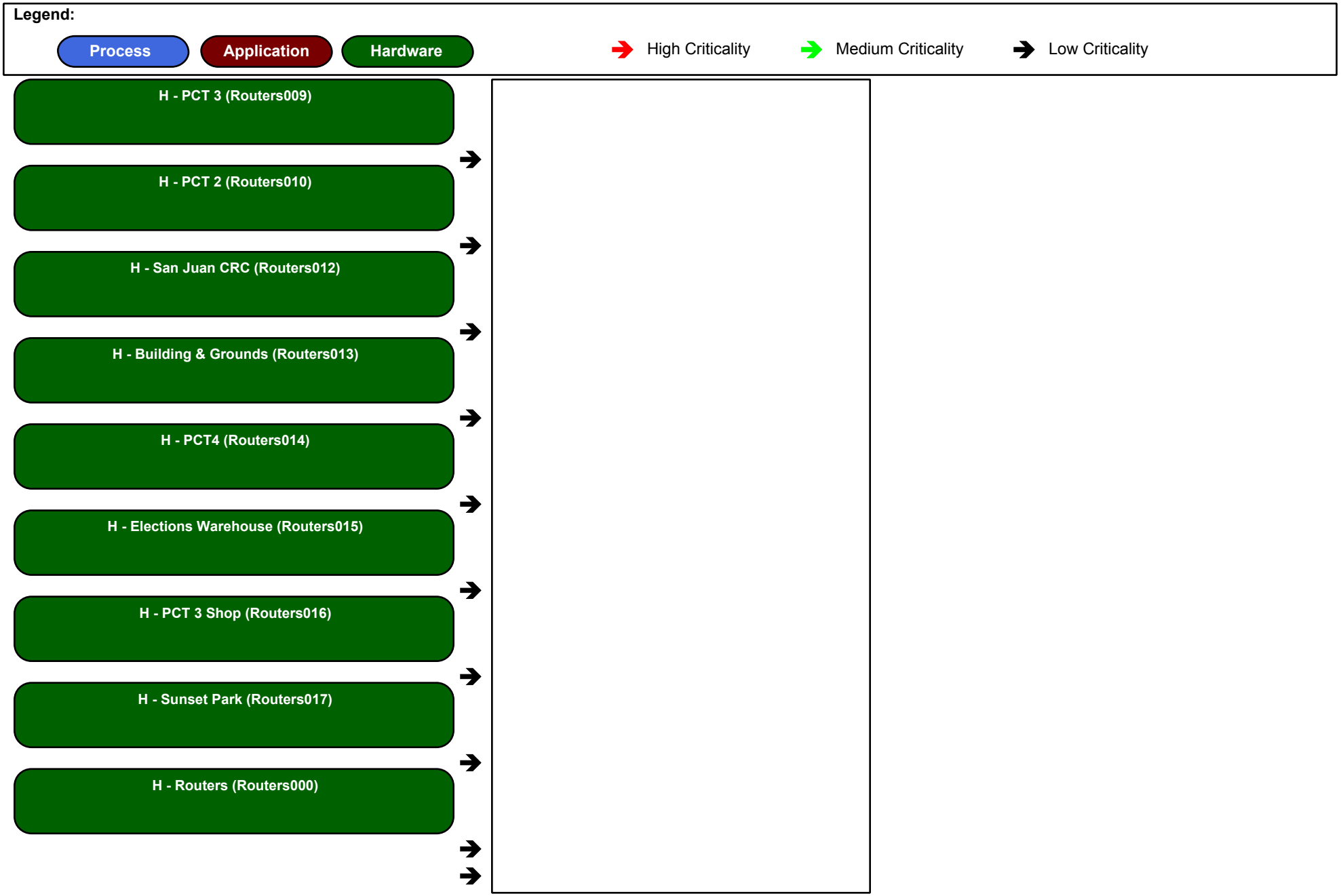

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
Hardware - Web Server (DMZ0003)
H - DMZ 0- Servers (DMZ0000)
H - Servers - DMZ (DMZ0000001)
Hardware - Mail Server (DMZ0004)
H - DMZ 0- Servers (DMZ0000)
H - Servers - DMZ (DMZ0000001)
A - VOIP Telephone System (ShoreTel)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

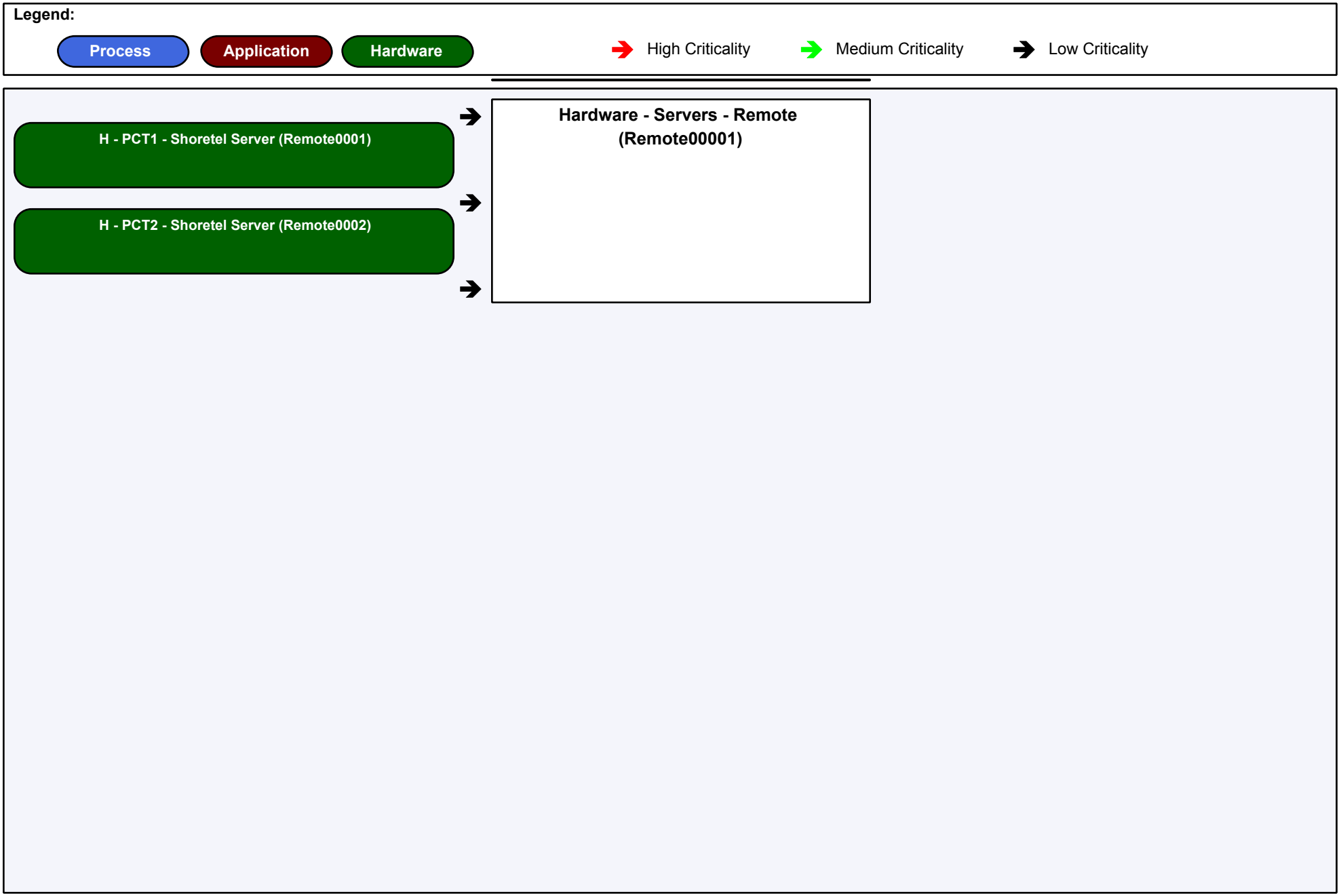

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - DNS1 Server (DMZ0001)
H - DNS2 Server (DMZ0002)
H - Web Server (DMZ0003)
H - Mail Server (DMZ0004)
H - SQL Server (DMZ0005)
H - VPN Concentrator (DMZ0006)
H - Webshield Server (DMZ0007)
H - DMZ 0- Servers (DMZ0000)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

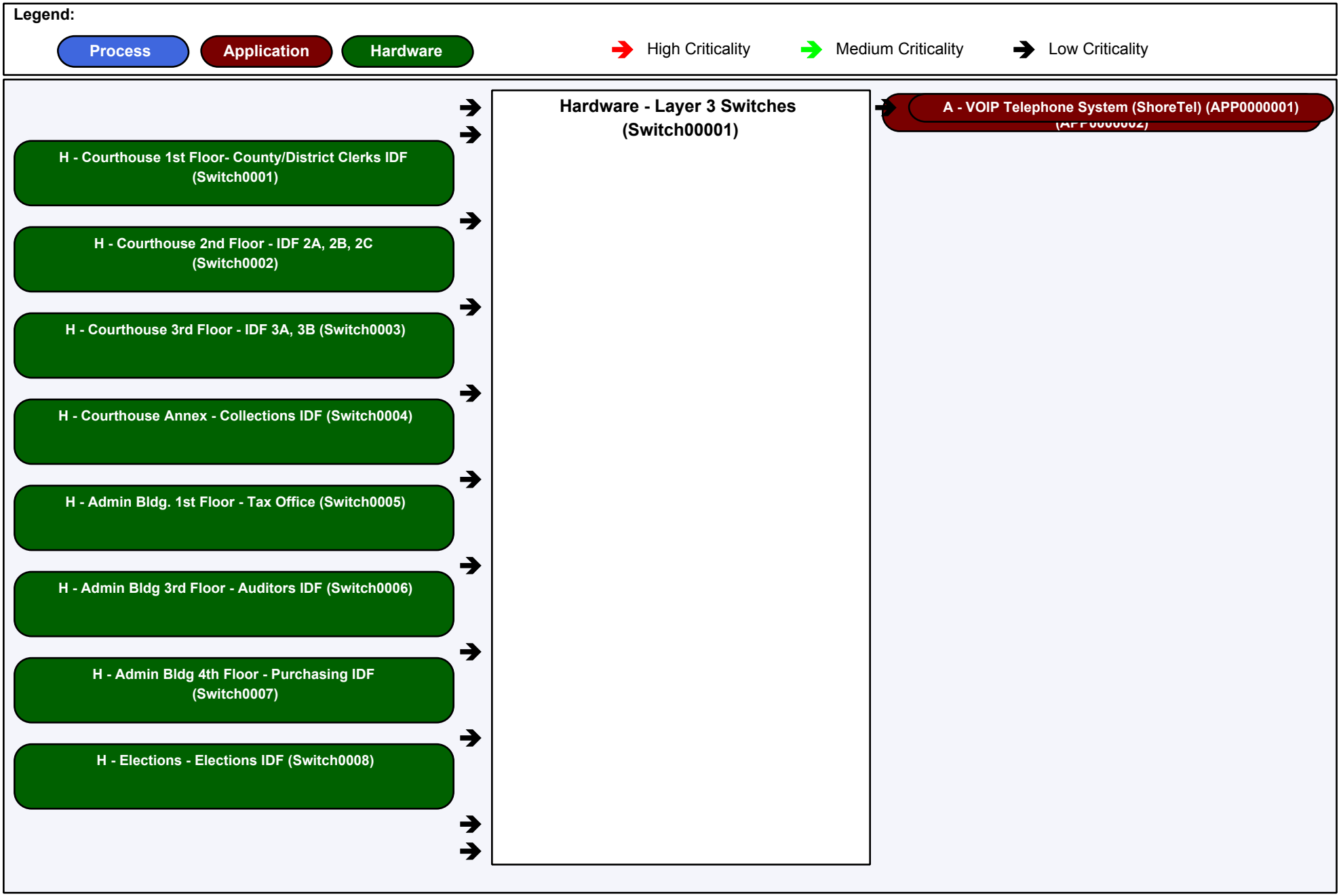

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - DC/DHCP/Active Directory (Internal0001)
H - IM (communicator) Serverc (Internal0003)
H - INET Server (Internal0004)
H - DataNAS Server - County Clerks (Internal0006)
H - DataNAS Server - County WAN (Internal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

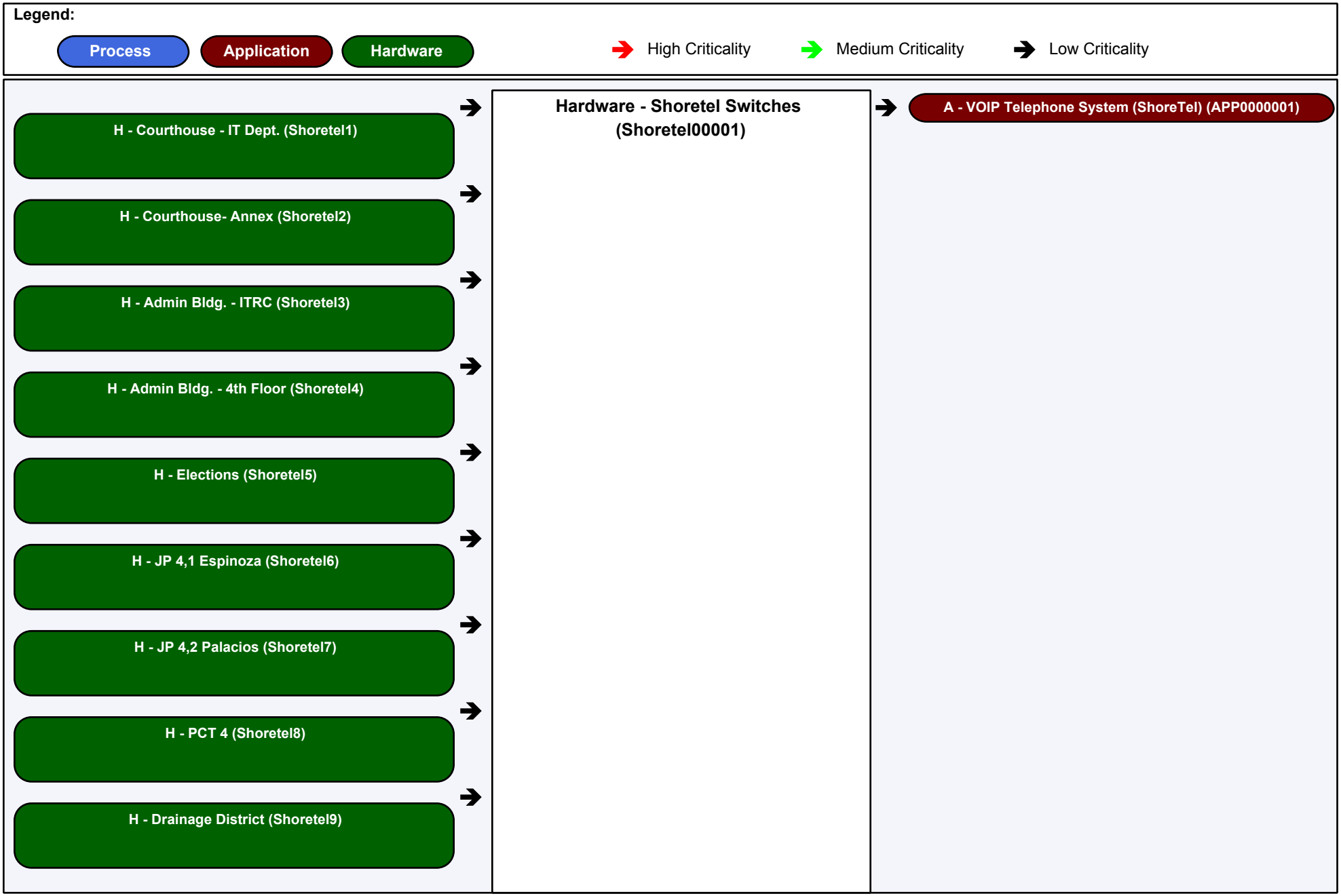

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality

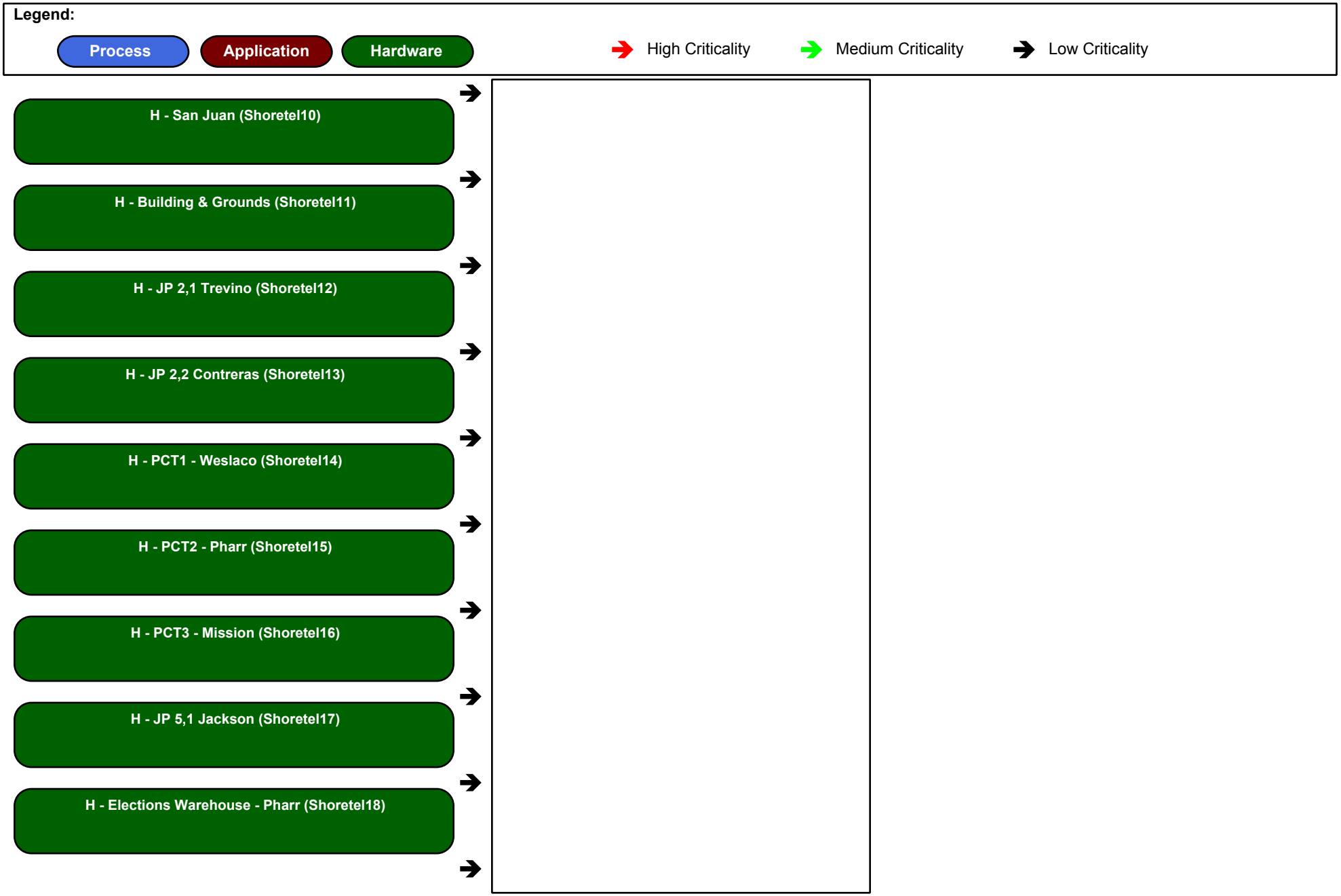

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sheriffs (Routers001)
H - County Clerks Mcallen Sub. (Routers002)
H - JP 5,1 Jackson (Routers003)
H - JP 2,2 Contreras (Routers004)
H - JP 4,2 Palacios (Routers005)
H - JP 4,1 Espinoza (Routers006)
H - PCT 1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

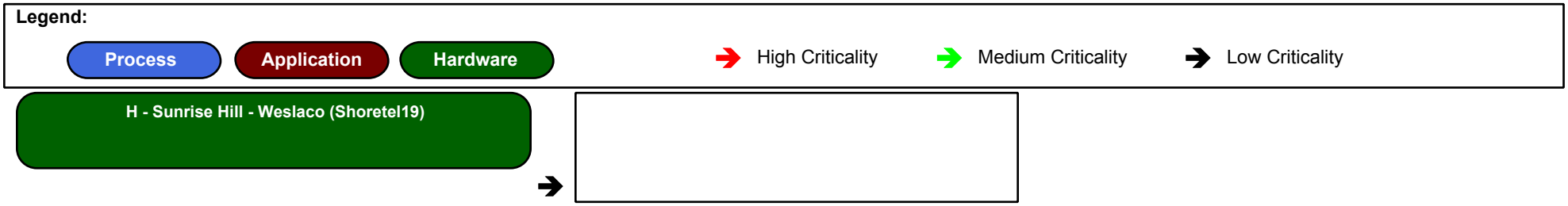

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT 3 (Routers009)
H - PCT 2 (Routers010)
H - San Juan CRC (Routers012)
H - Building & Grounds (Routers013)
H - PCT4 (Routers014)
H - Elections Warehouse (Routers015)
H - PCT 3 Shop (Routers016)
H - Sunset Park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

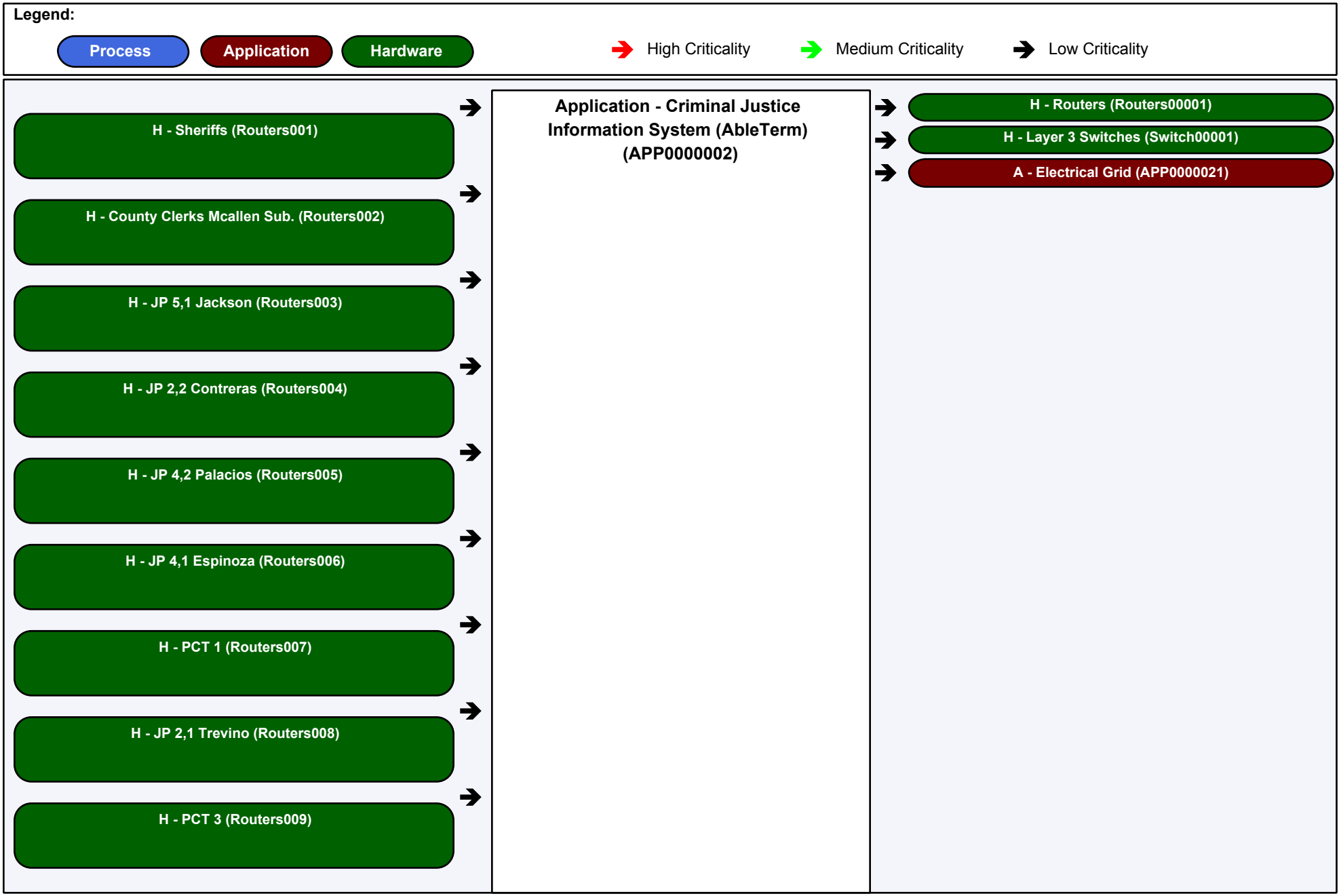

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT1 - Shoretel Server (Remote0001)
H - PCT2 - Shoretel Server (Remote0002)
Hardware - Servers - Remote
(Remote00001)

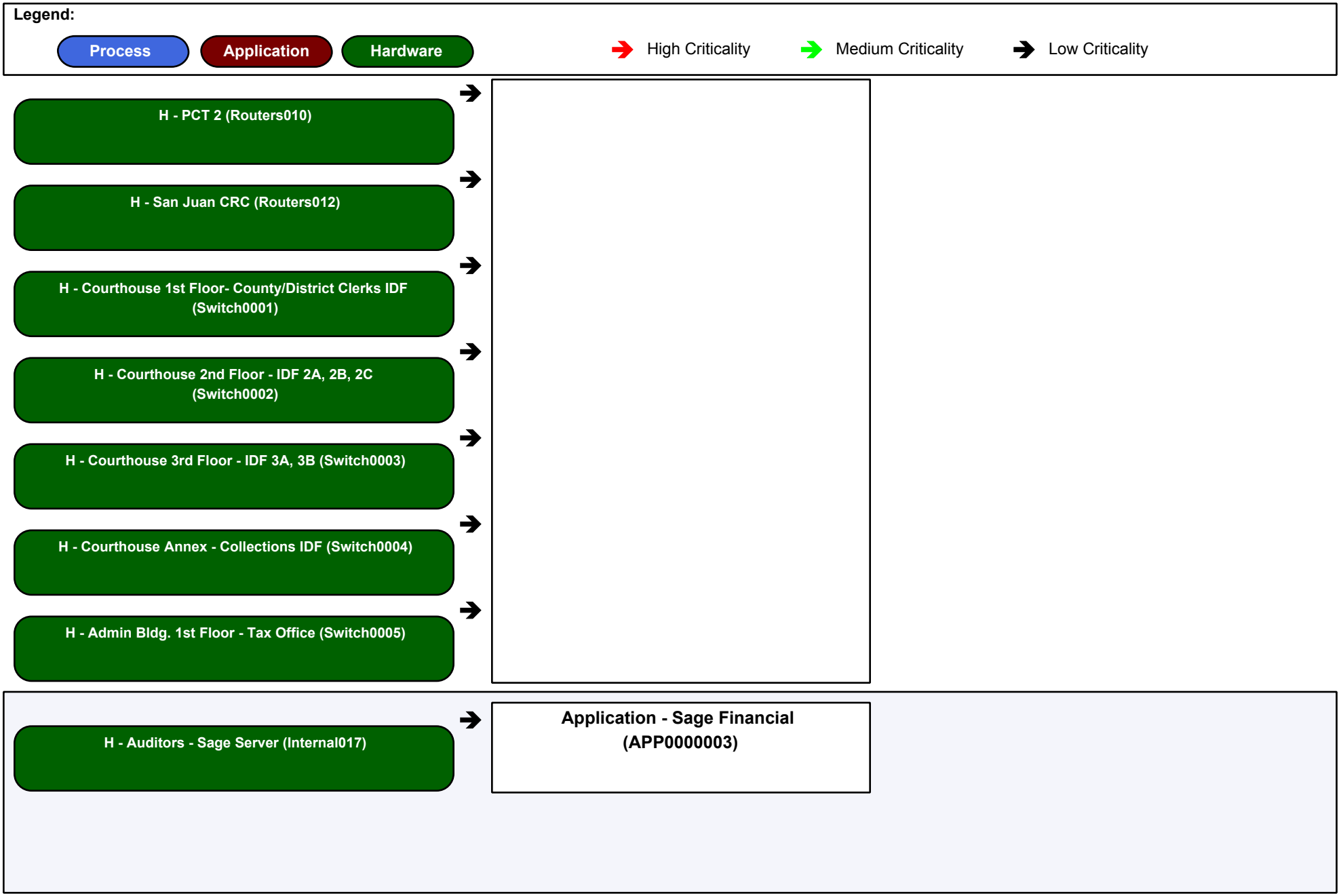

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Courthouse 1st Floor- County/District Clerks IDF (Switch0001)
H - Courthouse 2nd Floor - IDF 2A, 2B, 2C (Switch0002)
H - Courthouse 3rd Floor - IDF 3A, 3B (Switch0003)
H - Courthouse Annex - Collections IDF (Switch0004)
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)

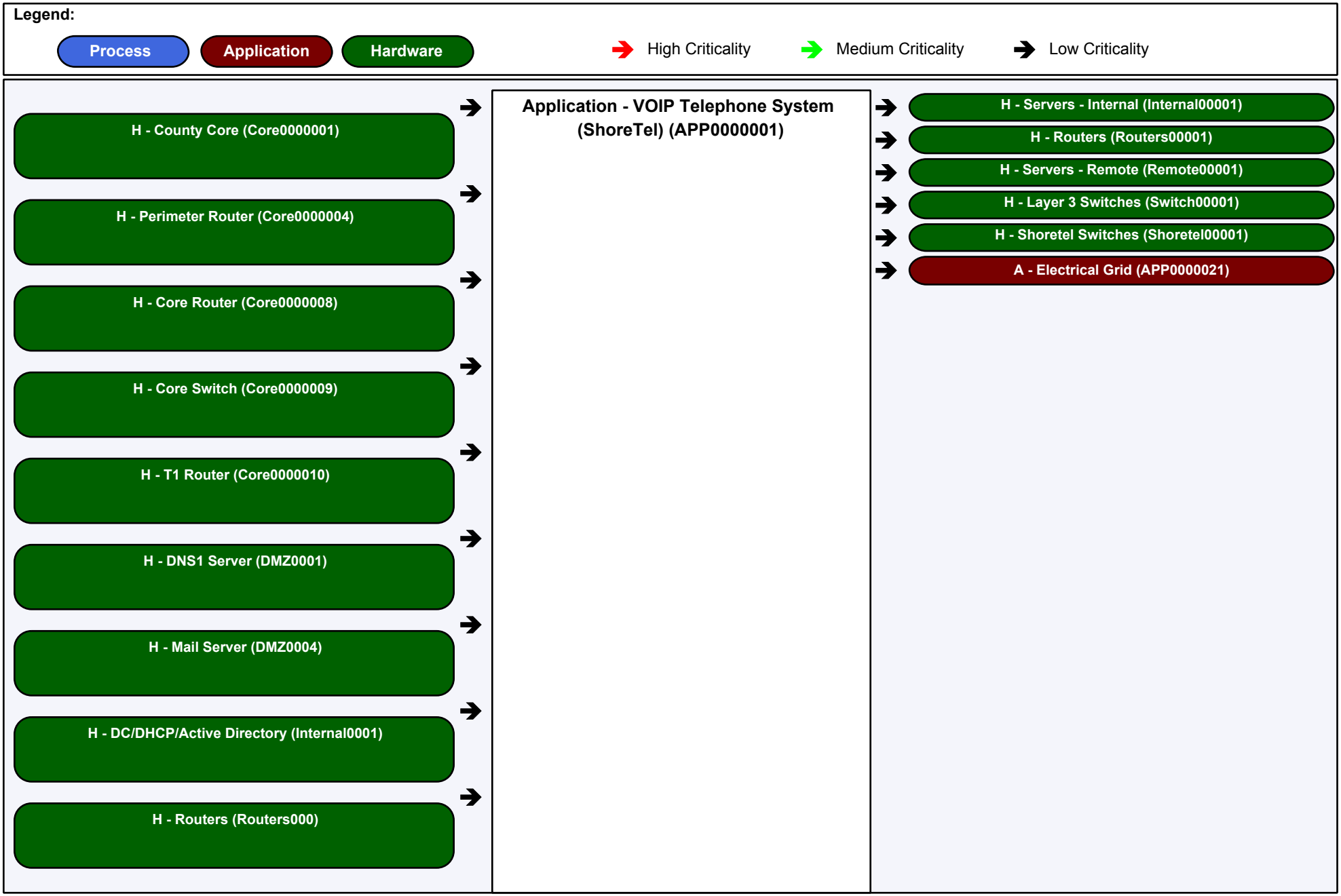

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Courthouse - IT Dept. (Shoretel1)
H - Courthouse- Annex (Shoretel2)
H - Admin Bldg. - ITRC (Shoretel3)
H - Admin Bldg. - 4th Floor (Shoretel4)
H - Elections (Shoretel5)
H - JP 4,1 Espinoza (Shoretel6)
H - JP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

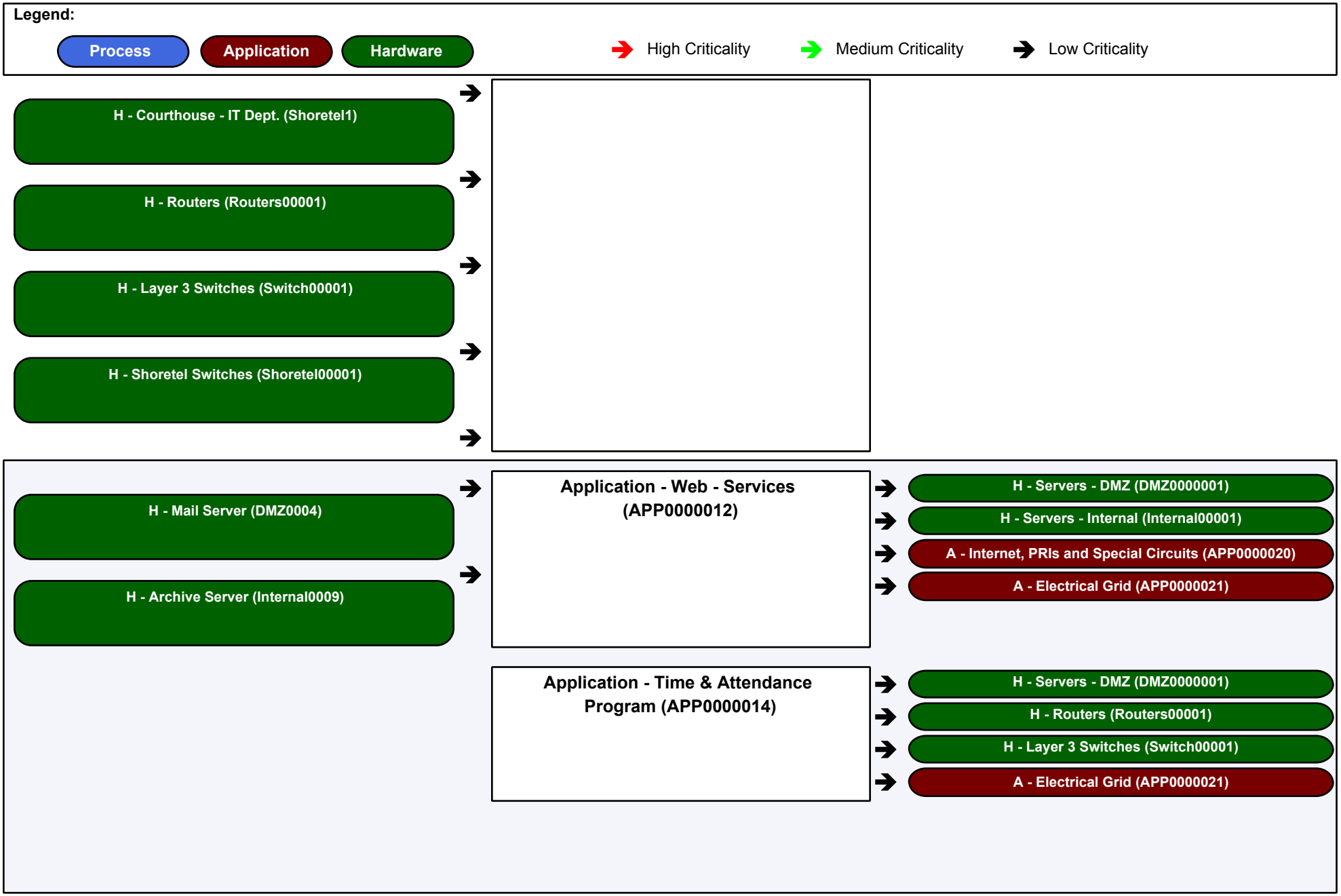

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - San Juan (Shoretel10)
H - Building & Grounds (Shoretel11)
H - JP 2,1 Trevino (Shoretel12)
H - JP 2,2 Contreras (Shoretel13)
H - PCT1 - Weslaco (Shoretel14)
H - PCT2 - Pharr (Shoretel15)
H - PCT3 - Mission (Shoretel16)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

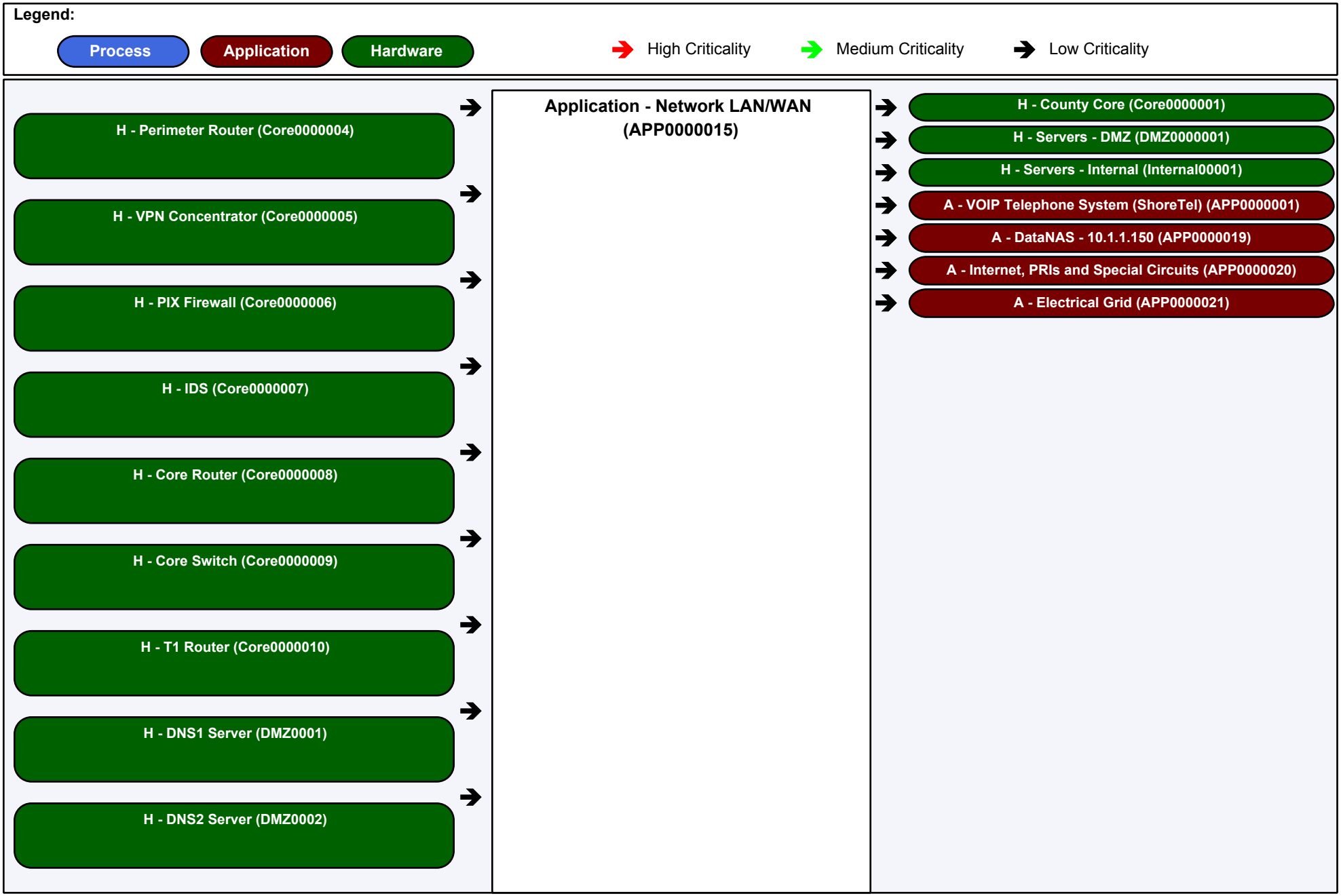

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sunrise Hill - Weslaco (Shoretel19)

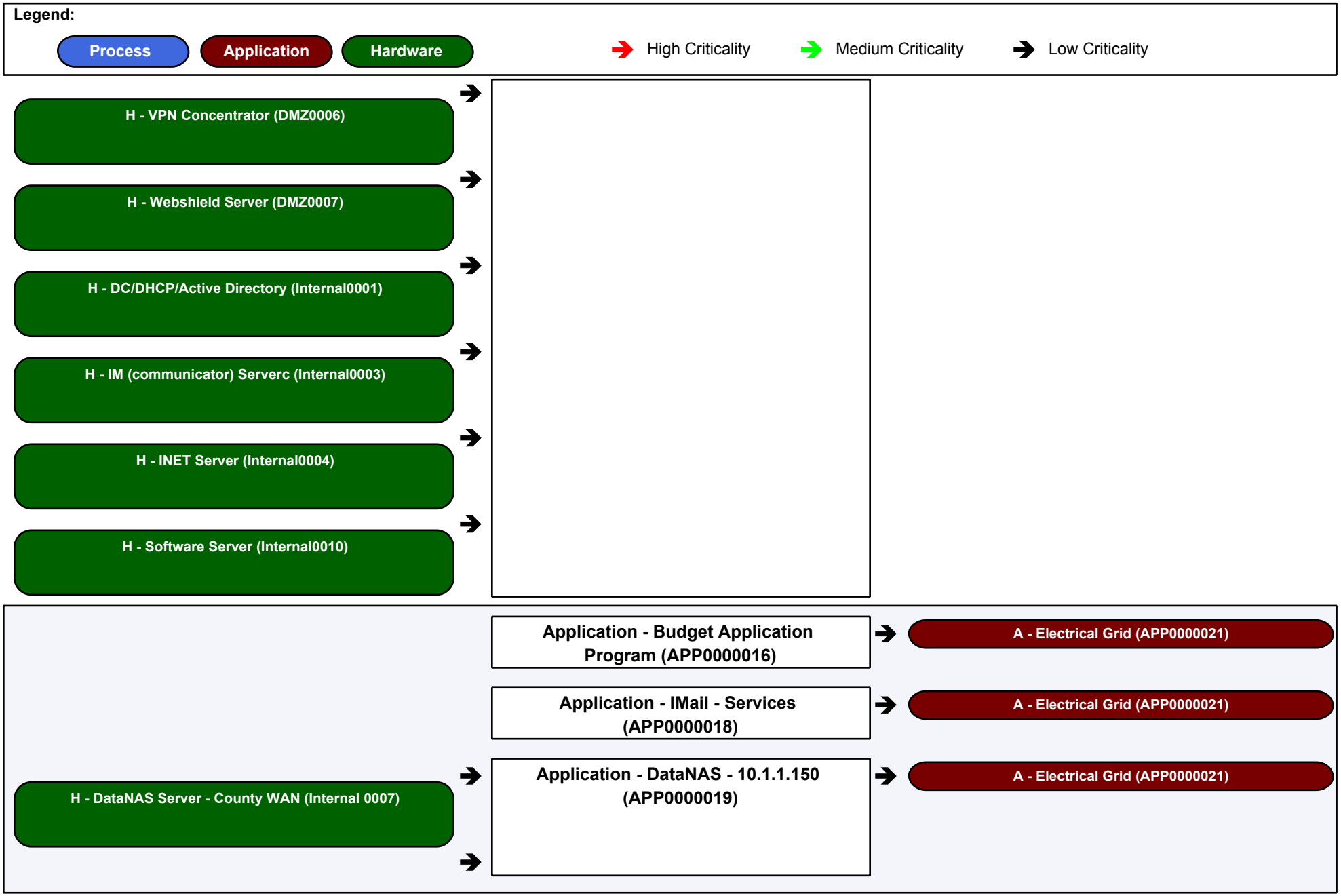

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - Sheriffs (Routers001)
H - County Clerks Mcallen Sub. (Routers002)
H - JP 5,1 Jackson (Routers003)
H - JP 2,2 Contreras (Routers004)
H - JP 4,2 Palacios (Routers005)
H - JP 4,1 Espinoza (Routers006)
H - PCT 1 (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)

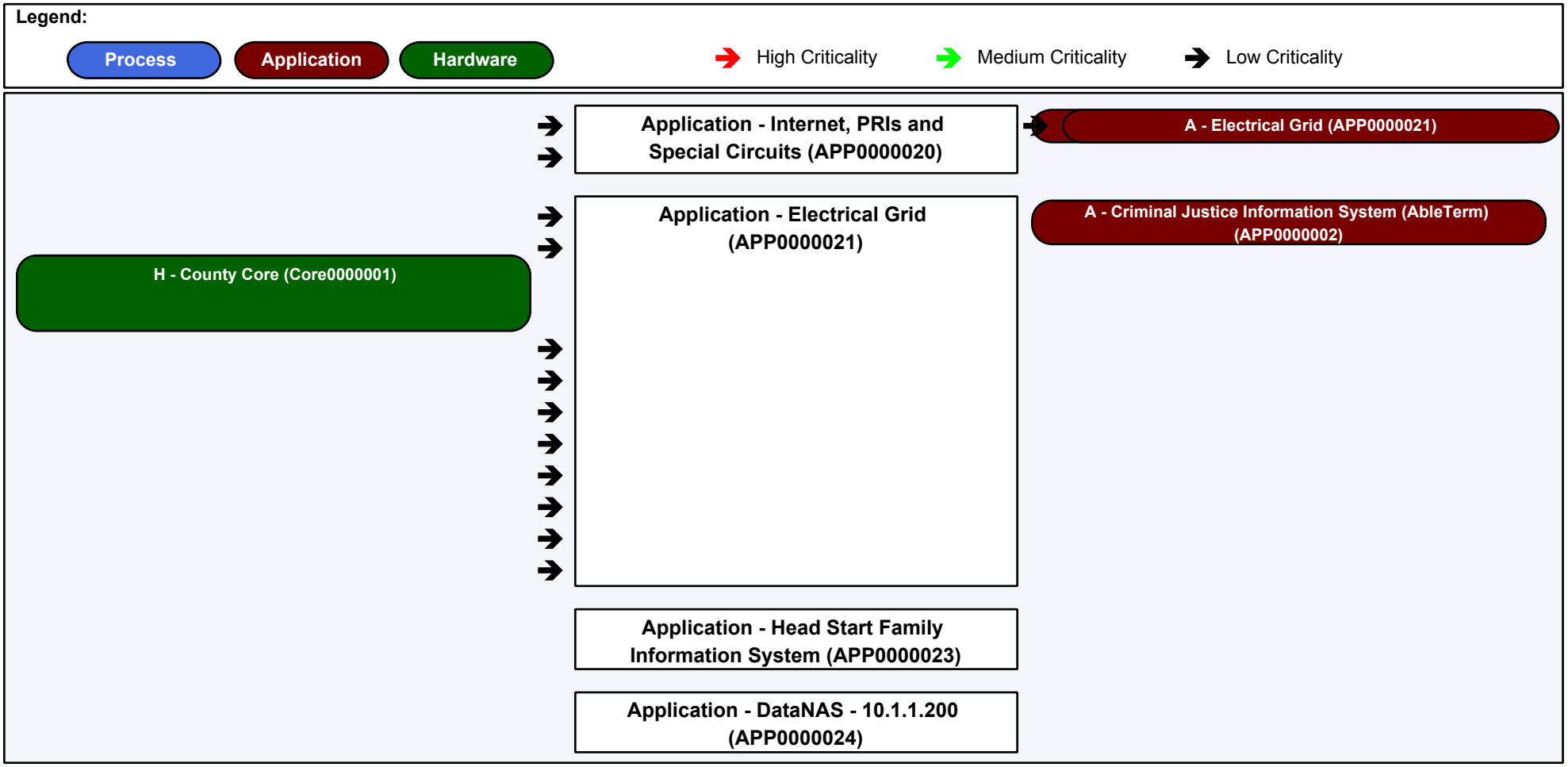

Legend:
Process
Application
Hardware
High Criticality
Medium Criticality
Low Criticality
H - PCT 2 (Routers010)
H - San Juan CRC (Routers012)
H - Courthouse 1st Floor- County/District Clerks IDF (Switch0001)
H - Courthouse 2nd Floor - IDF 2A, 2B, 2C (Switch0002)
H - Courthouse 3rd Floor - IDF 3A, 3B (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)
A - Electrical Grid (APP0000021)
A - Electrical Grid (APP0000021)
A - Electrical Grid (APP0000021)
H - DataNAS Server - County WAN (Internal 0007)


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

# 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

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

## 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<br>(2) Intel Xeon 2.4 GHz processors<br>2 GB RAM<br>(4) 36.4 GB SCSI hard drives<br>CDROM<br>1.44 FDD | Windows 2000<br>Oracle 8i<br>SAGE<br>PCAnywhere |
| **TSWEB** | Compaq Proliant ML 370R G2<br>Intel Pentium III 1.2 GHz processor<br>1 GB RAM<br>(3) 18.2 GB SCSI hard drives<br>Quantum DLT1 tape drive<br>CDROM<br>1.44 FDD | Windows 2000<br>Veritas Backup Software<br>Terminal Services |
| **Autostore** | HP Proliant DL 140<br>Intel Xeon 2.4 GHz processor<br>1 GB RAM<br>80 GB hard drive<br>Quantum Ultrium LTO 2 Backup external drive | Windows 2000<br>Veritas Backup Software<br>ACL Software<br>Autostore Scanning Software |
| **File** | Snap Appliance<br>Snap Server 4100 | |
| **DHCP** | Clone PC<br>Intel P-III 450MHz<br>64 MB RAM<br>4 GB hard drive<br>CDROM<br>1.44 FDD | Windows NT 4.0<br>DHCP Services |
| **NAV** | Dell PowerEdge 2650<br>Intel Xeon 2.4 GHz processor<br>512 MB RAM<br>80 GB hard drive<br>CDROM<br>1.44 FDD | Windows 2000<br>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:<br>Single Intel 200 MHz processor, 128 MB RAM, 3 GB HD, Fast Ethernet compatible hardware, Novell 5.0, Windows Server 2000 operating system<br><br>Workstation Requirements:<br>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<br><br>MIP workstation files |
| 2 | MIS | Server requirements:<br>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<br><br>Workstation Requirements:<br>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<br><br>*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<br><br>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**<br>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.

Anna P Jenne
**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.