Cumberland Heights

Information Systems Disaster Recovery Plan

Table of Contents

Overview

Background – Cumberland Heights is a nationally recognized alcohol and drug treatment center located west of Nashville on the banks of the Cumberland River, offering both in-patient and out-patient services for individuals as well as programs for family members. Cumberland Heights' primary location for inpatient services is located on River Road in Nashville. Additional locations in Tennessee include Hermitage, Smyrna, and Jackson. Only the River Road has an local area network. All primary systems are located at the River Road facility. The scope of this plan is limited to systems hosted at the River Road facility. Cumberland Heights is committed to protecting the confidentiality, integrity, and availability of all of its systems, but has placed special emphasis on those systems that contain electronic protected health information or EPHI.

Planning Assumptions – Due to the nature of services that are provided at Cumberland Heights, a disaster sufficient to destroy or render the primary campus that houses information systems unusable, would require that inpatients be discharged and placed in the care of other providers. The logistics for responding to such an event are documented in emergency and evacuation plans maintained for the facility. The primary goal of this plan is the rapid recovery of critical systems [in place] to support continued operations at the primary campus.

Plan Structure – This plan is divided into several sections. In the first section, core systems or applications are identified along with their criticality and the associated recovery time objective. The recovery time objective is similar in concept to a maximum allowable outage for the system. The second section of this plan identifies potential risks to systems and safeguards that are in place at Cumberland Heights that promote "disaster avoidance." This section should be reviewed regularly during the testing phase of the plan to ensure that significant risks have been considered and that appropriate safeguards are in place to mitigate those risks to acceptable levels. The third section of this plan details the manner in which critical systems, applications, and data are backed up. This section should be updated regularly as changes are made to backup schemas and cross checked to validate that ALL critical systems are being backed up appropriately. The fourth section of this plan is a listing of key items to be completed in an emergency or disaster situation. This section will serve as a high level guide to those involved in the recovery process. The final section of the plan outlines how and when testing of the plan should occur. Testing or "exercising" this plan will ensure that the plan is kept up to date as circumstances, systems, and personnel change at Cumberland Heights as well as identify any weaknesses in the plan that should be remediated.

The appendices at the end of the plan document provide various forms and listings that are to be used in the ongoing planning, recovery, and testing activities associated with this document.

Section 1 - Applications & System Criticality

The information technology department at Cumberland Heights supports the systems required for all of the locations (see overview) of the company. The majority of remote locations that serve as out-patient treatment centers only make limited use of core systems housed at the main campus on River Road. This use is primarily limited to e-mail. The main data center is housed in the administration building at the River Road facility. The Cumberland Heights campus is comprised of several free standing structures. These buildings are tied together in a local area network by means of subterranean Ethernet cabling or fiber optic cabling depending on distance and time of construction.

When considering the applications and supporting systems to be included in this plan, management determined the following to be critical to varying degrees to Cumberland Heights' operations:

- Windows based Local Area Network / Active Directory;
- File and Print Services;
- Microsoft Exchange – Email;
- Raiser's Edge/ Blackbaud - fundraising;
- Terminal Services;
- Tier – Clinical applications;
- DialDictate Dictation;
- HMS\AS400 patient accounting;
- HMS\MedHost EArchive.

When determining applications and systems criticality, special consideration has been given to systems that contain electronic protected health information, (EPHI). The primary systems that house or process EPHI are TIER and HMS.

TIER is a software package designed specifically for mental health and substance abuse oriented providers and serves as a primary repository for patient records and clinical information. Timely access to the information contained in TIER is key to clinicians involved in the care of patients at Cumberland Heights. As such, the recovery time objectives for TIER are relatively short (i.e. < 2 hours to recovery).

The HMS system is provided by Healthcare Management Systems in Nashville, Tennessee. This vendor is responsible for all maintenance of the hardware and software associated with this application and provides its customers with assistance in disaster scenarios by either obtaining and installing replacement hardware or obtaining backups from the customer and hosting the customer's system remotely until the customer is ready to return to normal operations at an alternate site or the primary site.

The criticality rankings and recovery time objectives for each application or service are defined in ***Figure 1***.

Criticality Matrix – Figure 1.

Ref.	Applications/Systems	Host	Critical	RTO	EPHI Y/N
1	Local Area Network / Directory Services	SVRADS3	Y	< 24 Hrs.	Y
2	File and Print Services	SVRADS3	Y	< 24Hrs.	N
3	Microsoft Exchange – Email	SRVEXCH02	Y	< 24 Hrs.	N
4	Razor / Blackbaud	RAZSVR2	N	< 72 Hrs.	N
5	Terminal Services	TS2SVR, TEMPTERM	Y	< 24 Hrs.	Y
6	TIER	SQLSVR	Y	< 2 Hr.	Y
7	Dial Dictate Dictation	N/A	N	< 72 Hrs.	Y
8	HMS	AS400 / IBM eServer	Y	< 24 Hrs.	Y
9	HMS – Earchive	AS400/Linux server	Y	< 24 Hrs.	Y

Section 2 - Risks and Availability Safeguards

As part of the planning process, Cumberland Heights recognizes the importance of deploying safeguards that minimize either the likelihood or the impact of a disaster event. We have considered a number of common or likely risks to our systems and deployed safeguards/controls as described below.

Power Loss – All of Cumberland Height's critical shared systems are located in the main data-center. Each critical server and infrastructure component is protected from spikes in power and intermediate losses of power via un-interruptible power supplies (battery backups). The facility also employs an emergency generator in case of an extended power loss.

Physical Security – The data center is located in an administrative wing that is off-limits to patients and un-escorted visitors. This wing is locked after hours and when unoccupied. In addition, the door to the data center is secured with a numeric key pad lock. The combination is only known to individuals with a need to access the data center. The code is changed periodically. The data center is located below ground in a basement level and there are no windows or alternate points of ingress other than the main door.

Logical Security – Access to the internal network from the Internet is controlled via a firewall. The internal network utilizes non-routable IP addresses to further minimize the risk of intrusion from the Internet. The local area network requires authentication via Microsoft's Active Directory and users must enter a unique user name and password to gain access to the network. Users are granted access to network resources based on their role in the organization and are assigned group memberships that control their rights based on these roles. All critical applications require the use of a unique user name and password. Individuals with administrative privileges on the network and within applications are limited only to those with a business need for a high level of privilege.

Internal Flood – Although the data center is below grade which presents a risk for flooding from floors above, equipment is maintained in racks which keep the equipment off of the floor. There is no significant plumbing either on the floor above the data center or above the ceiling in the data center.

External Flood – Although the Cumberland Heights campus property is located on the Cumberland River, the elevation is such that it is extremely unlikely that flooding could occur due to river flooding or ground water flooding from excessive rain. The facility IS NOT on a flood plain.

Fire – Fire suppression is accomplished by means of hand-held fire extinguishers and an Ansul Sapphire Suppression System. Fire detection is tied into the building's security alarm and monitoring system. With a Ansul fluid based suppression system there is a low risk of significant damage to systems due to fire in the data center.

Tornado / Wind – The Middle Tennessee area is relatively prone to tornadic activity, especially in the spring months. While the structure that houses the data center is of typical construction, the data center is located in the basement of the building which should offer reasonable protection from tornadic storms of light to moderate intensity (1 – 3). While hardware may be intact after such a storm, it is likely that communications will be disrupted and a direct hit to the building may render it unsafe for continued operations.

Ice / Winter Weather – The primary risk, other than the availability of support personnel during winter weather is an extended power outage. Cumberland Heights maintains an emergency generator that will supply power to critical areas during such an outage.

Excessive Heat – The data center at Cumberland Heights is a relatively small room (approximately 10 x 15). It is cooled by an auxiliary cooling unit that maintains the temperature acceptable levels. There is no redundancy built into this system and should it fail, the data center door would need to be left open to rely on the building's cooling system until the dedicated unit could be repaired.

Lightning – Lightning arresters have been placed at critical junctions where communications and power enter the data center. Additionally, lightning arresters have been installed on Ethernet circuits at each building on campus.

Hardware Failure – With the exception of the AS400, all systems at Cumberland Heights operate on "WinTel" platforms. As such, replacement hardware can be readily obtained from numerous sources to support recovery time objectives. The AS400 is supported and maintained by a local vendor who has agreed to provide for ongoing operations by either replacing the equipment or loading Cumberland Heights' data in their hosted environment. The primary safeguard for recovering from hardware failure is nightly backups of systems and data. These backups will be restored on replacement hardware.

Viruses / Malware – All servers and workstations at Cumberland Heights are protected by anti-virus software. Updates to virus definitions are applied on a regular basis.

Telecommunications Failure – From an information systems standpoint, primary telecommunications risks relate to connections to the Internet, to HMS (software vendor), and to the Thompson Lane location. While these circuits are important in terms of email communications and supporting other users and business partners, brief downtime is not crippling in terms of critical systems. The impact of an extended communications outage on the broader business in terms of telephone service and call center operations is outside the scope of this plan. In the event of a disaster that affects telecommunications, the recovery team has been instructed to make use of cellular communications.

Section 3 – Data Backup Plan

Cumberland Heights performs full backups each weeknight of MS Windows based servers on the local area network as well as backups of the HMS applications and data on the AS400. Backups for the network and Windows based hosts are managed by Cumberland Heights. Backups for HMS and the AS400 are managed by Healthcare Management Systems. Cumberland Heights is responsible for the storage and rotation of backup tapes for both systems. Backup tapes from the previous night's backup jobs are retrieved and stored in a separate building (Lodge) from the building that houses the data center in a media rated safe. From a recovery standpoint, the organization's maximum exposure is one day's or one weekend's worth of data as backups are not performed on Saturdays or Sundays. System configurations, applications, and application data are backed up and retrievable should systems need to be completely restored "from scratch."

Details regarding nightly backups of Windows based systems (everything but HMS) are listed below.

Backup Server: TEMPTERM Backup Software: Symantec Backup Exec 12 v.14.0 rev. 1798
Backup Schedule: Mon-Fri 7:00 PM CST
Backup Type: Full

Backup Selections:

RAZSVR2\C:\*.* /SUBDIR
RAZSVR2\Utility Partition
RAZSVR2\System State
SQLSVR\ C:\*.* /SUBDIR
SQLSVR\ D:\*.* /SUBDIR
SQLSVR\SQL Server Databases including TIER
SVRADS3\ C:\*.* /SUBDIR
SVRADS3\ D:\*.* /SUBDIR
SRVEXCH02\ C:\*.* /SUBDIR
SRVEXCH02\ D:\*.* /SUBDIR
SRVEXCH02\Microsoft Exchange Information Store
SRVEXCH02\Microsoft Exchange Mailboxes

Section 4 – Systems Recovery Procedures

A SQL Server with monitor, key board and mouse is housed in the server room in the basement of the FLC. In the event of a loss of data information due to power outages or any other disaster event this server is designed to be easily moved to a safe location, powered by emergency generators to give on site staff the ability to readily access patient

medical and therapeutic information. (See Policy and Procedure Emergency Data Recovery)

Ref	Activity	Resp. Party
Disaster Declaration and Emergency Response		
1	Upon disaster event - If necessary, notify emergency response personnel (i.e. dial 911). Be prepared to provide address, nature of disaster, and building(s) involved.	Safety Committee
2	Implement evacuation procedures per facility emergency plan if necessary. THE FIRST PRIORITY IS THE PROTECTION OF THE HEALTH AND SAFETY OF PATIENTS AND STAFF.	
3	If time and the nature of the emergency allow, remove critical media in data center (backup tapes, etc.) to a safe location.	
4	Coordinate with emergency response personnel arriving on-site. Notify emergency response team of location of critical assets including computer systems and backup media along with combination to keypad for data center if appropriate.	
5	Declaration of Disaster by authorized individual. Authorized individuals include: ▪ Jimmy Jamison, Jermaine Smith, and Chris Lindsay	
6	In case of damage to property or injury to staff or patients, a member of Executive Management should notify insurance agent/carrier.	
7	Notify Recovery Team – Utilize Recovery Team Calling Tree – ***Form DR-1.*** If office telecommunications are affected, utilize cell phones to reach team members.	
8	Perform Damage and Impact Assessment – Utilize ***Form DR-2***	
9	Report Status to Executive Management ▪ Recovery Possible On Site < 4 Hours ▪ Recovery Possible On Site > 4 Hours < 12 Hours ▪ Recovery Possible On Site > 12 Hours ▪ Recovery Not Possible On Site (Site Destroyed) ▪ Other	
10	Notify end-user department heads as directed by executive management – Utilize ***Form DR-5*** (Employee Calling Tree). Have departments revert to manual procedures as necessary.	
S9ystems Recovery		
11	Notify critical vendors of emergency situation – Utilize ***Form DR-3***	
12	If Telecommunication equipment or service is down, contact vendors to facilitate repairs or replacement equipment. ***See Form DR-3***	

Ref	Activity	Resp. Party
13	Disasters that may affect the availability of systems come in many forms ranging from simple data corruption that can be resolved by restoring data from tape, to the loss of the main computing facility and destruction of hardware. Based on the disaster event, identify resources (hardware, applications, operating systems, supplies, people, facilities, etc.) needed for systems recovery. Utilize ***Form DR-4***	
14	Validate and confirm recovery priorities with management. It is possible that all systems may not be affected by a disaster event. This plan recommends the following recovery order: 1. TIER 2. Windows Directory Services / AD Server 3. MS Exchange / Email (backup server) 4. File and Print Services 5. Terminal Services 6. HMS 7. Image Viewer/eArchive 8. Dictation 9. RAZSVR2 / Blackbaud	
15	If necessary, order replacement equipment from vendors and assure expedited shipping (overnight or same day). ***See Form DR-3***	
16	Based on damage / impact assessment performed in ***step 8***, identify strategy for delivering critical application access to users on a limited basis if necessary. TIER is of key concern in that the application supports clinical activities and contains information key in the treatment of Cumberland Height's patients. Having at least one terminal available with access to TIER is critical. The nature of the event will dictate the ultimate recovery strategy, however the following options should be considered. ***If communications are cut between treatment locations and the data center***, the TIER server and a hub could be relocated from the Data Center to a secure area where clinical activity is taking place. Existing / undamaged PCs could access the software via temporary cabling ***If the data center or the TIER server is destroyed,*** a temporary stand-alone installation of TIER can be deployed in or near a treatment area. Data would be restored from backups. SEQUEST TECHNOLOGIES recommends the following as a minimum configuration for a server housing TIER.	

Ref	Activity	Resp. Party
	• Dual Pentium II processors at 1GHZ or better • 1GB RAM • RAID controller • 64MB (configured for RAID 5) • 100GB 7200 RPM Hard Drive x 3 • DDS4 or DLT 100/200GB Tape Drive • 100/1000 NIC • Windows 2008 Server R2 • Microsoft SQL Server 2008 It is believed performance could be sacrificed in an emergency situation making the need for dual processors and a RAID configuration, optional. *To meet recovery time objectives for TIER, Cumberland Heights has identified a "hot spare" PC that can be used temporarily to host TIER. It is located ________________.* An attached laser printer will also be needed.	
17	Obtain most recent backup tapes from: 1. Tape drive(s) in data center if possible 2. Media safe in the Lodge	
18	Obtain original software media including: 1. Windows / Network Operating Systems 2. Microsoft Exchange Server software 3. Blackbaud / Raiser's Edge Application software 4. SQL Server software 5. MS Terminal Services/Server 6. TIER Application Software 7. Printer Drivers / Setup Disks 8. Symantec Backup Exec Software *This original media along with other important software such as device drivers, setup disks, etc. is located in a locked cabinet and/or media safe in the A/R Cottage.* *Cumberland Heights maintains a hot/spare tape drive compatible with / or identical to primary tape drive. This drive and the software drivers (if any) are located with the backup tapes in the the Lodge*	
19	Coordinate vendor support personnel to assist with restoration of infrastructure and applications.	
20	Upon receipt of replacement equipment begin restoration of systems utilizing original media and backups as necessary. See	

Ref	Activity	Resp. Party
	step 14 for order of restoration. Important considerations for restoring servers: ▪ Restore times typically take much longer than backup times. ▪ While restoring the operating system, use the ASR files and the most recently performed full backup of the operating system and the system state. ▪ First, restore the full backup and then any differential backup to bring the system back to original state. ▪ Restore data to a domain controller only using the data that was originally backed up from that domain controller. Non-authoritative restore is the default method for restoring Active Directory. After a non-authoritative restore, the domain controller is updated using normal replication techniques. An authoritative restore can be used in situations such as when human error is involved and the domain controller being restored is the only domain controller or when the purpose is to propagate the changes from a prior backup. ▪ If you restore the system state data and the licensing database to the same Terminal Server Licensing Server computer, any un-issued licenses are restored correctly as long as you have not replaced the operating system on the computer. If you do not restore to the same computer, any un-issued licenses that are detected are not restored and an event will appear in the System log of the Event Viewer. You can still restore the un-issued licenses by contacting the Microsoft Customer Support Center by phone and requesting them to reissue the licenses.	

Section 5 – Testing Plan

Cumberland Heights recognizes the benefits associated with regular testing of its Disaster Recovery plan. Care is taken to design the nature and timing of tests so as to minimize the impact to ongoing operations. As such, we have developed a three phased approach to testing which includes the following types of tests:

1. Annual walkthrough testing of DR plan
2. Monthly test restores of randomly selected files from backup media
3. Annual test restore of select critical applications

Annual Walkthrough – This test involves all of the individuals on the IT Recovery team (see ***Form DR-1***). These individuals will meet to discuss potential disaster scenarios and discuss each person's roles and responsibilities before, during, and after the disaster event. The DR Plan Administrator will be responsible for taking notes of the proceedings and making any recommended changes to the plan resulting from the walkthrough. This exercise is designed to make sure that the plan is kept up-to-date as well as keep the recovery team members trained in how the plan will be implemented when a disaster event is declared.

Monthly Test Restores – The IT Recovery Plan Coordinator is responsible for choosing files and media to test each month. The objective of these tests is to verify the restorability of backups and the integrity of the data contained on backup media. The RPC will create a test restoration folder on the file and print server and restore the selected files to that location. The RPC will then verify that the files are restored and "readable", documenting such by keeping a log of these tests that includes the dates and success or failure of files to restore properly.

Annual Test Restoration of Critical Applications – On an annual basis, the RPC will coordinate test restorations of key systems including:

1. Local Area Network (active directory)
2. MS Exchange (email)
3. TIER
4. HMS

If during the course of the year, these systems have been restored successfully due to unforeseen or scheduled events, these restorations will be documented and considered sufficient to meet the testing requirement.

With all testing, results will be logged and anomalies noted. Any relevant procedures developed as part of the testing will be incorporated into recovery procedures of this document.

APPENDICES

FORM DR-1 Recovery Team Calling Tree

Team Member	Role	Home Address	Home Phone	Cell Phone	Pager	Office Extension
Jermaine Smith	Recovery Coordinator	209 Annesbury Lane Cane Ridge, TN 37013	615-4242908	615-456-5426		3300
Jimmy Jamison	Recovery Administrator	1301 Twin Circle Drive, Nashville, TN 37217	615-554-4848	615-405-7402		3304

FORM DR-2 Damage / Impact Assessment Report

Date and Time of Report	
Name of Submitter	
General Description of Disaster	
External Support Requirements	

Impact Level on Key Resources: (High, Med, Low)	Damage Magnitude (Severe, Moderate, Light)	Extent Nature of Damage	Estimated Recovery Time
Utilities and Services (List affected utilities)			
Hardware (List affected hardware)			
Building Structure (List affected areas)			

Impact Level on Key Resources: (High, Med, Low)	Damage Magnitude (Severe, Moderate, Light)	Extent Nature of Damage	Estimated Recovery Time
Personnel Injuries (List affected people)			
Vital Records (List affected vital records)			
Other Resources (List other affected resources)			

Overall Disaster Magnitude
_____ Serious
_____ Moderately Serious
_____ Inconvenient

Other Information Regarding the Disaster Event:
____
____
____

Form DR-3 Vendor Calling Tree

Vendor Name	Product /Service Provided	Contact	Daytime Phone	Emergency Phone	Account # / Other
HMS	HMS Software / AS400	Main Line	615-286-2400		
Sequest Technologies	TIER	Kellie Currie	630-577-9003		
	Blackbaud / Razor	Worth Beacham	800-468-8996		
	Lanier Dictation				
Hiscall Communications	Phone System (s)	Dispatch	615-741-7770		
Bell South	Internet Service				
	Phone Service				
	Data Circuits				
Bill Piercy	Electrical Contractor				
	Data Center HVAC				
	Property & Casualty Insurance				
	Legal Counsel				
	Building Security Systems / Keypads				

Form DR-4 Recovery Resource Requirements

Resource Type / Desc.	Quantity	Need By Date	Duration in Hours	Est. Cost
Hardware – Servers	9			
Hardware – Networking	NA			
Hardware – Security				
Hardware – Other (printers, peripherals, etc.)	40			
Software – Operating Systems				
Software – Applications				
Software – Utilities				
Personnel – Cleanup				
Personnel – IT Consultants	2			
Personnel – Security				
Personnel – Other				
Other (forms, supplies, etc.)				

Form DR-5 Employee/End User Calling Tree

End User / Dept Head	Role	Home Address	Home Phone	Cell Phone	Pager	Office Extension

Form DR-6 Data Center Key Equipment Inventory

Equipment Type	Quantity	Purpose	Lead Time to Replace
7 ft Equipment Racks	3	Houses datacom and server hdw	1 to 2 days
48 Port Patch Panel	2	Ethernet termination points / patch	Same day local suppliers
24 Port Patch Panel	1	Ethernet termination points / patch	Same day local suppliers
Dell Poweredge 2550 Servers	2	ADS, Exchange, File & Print Servers	1 to 2 days
Dell Poweredge 1650 Server	1	Blackbaud / Razor Server	1 to 2 days
Dell Poweredge 2650 Servers	2	Terminal Servers	1 to 2 days
Dell Poweredge 2850 Server	1	Terminal Server	1 to 2 days
Dell Poweredge 2950 Server	1	TIER Server	2 to 3 days
Dell Poweredge 750	1	Avia BCMS, Call Mgt Server	1 to 2 days
Symmetra RM UPS – APC UPS w/ 4 Battery Units	1	Battery Backup	2 to 3 days
KVM Switches 8 Port	2	Shared Kbd, Video, Mouse	1 to 2 days
Netgear Fast Ethernet Hubs/Switches 24 port	2	End user LAN connections	Same day local suppliers
Fortigate 200 Firewall	1	Firewall	1 to 2 days
Transition Networks 8 slot Fiber to Ethernet Converter	1	Convert Fiber to UTP	1 to 2 days
Leviton Fiber Termination Box	1	Terminate Fiber runs (4 ports used)	1 to 2 days
17 Inch CRT	1	Monitor for servers	Same day local suppliers
Keyboard	1	Keyboard for servers	Same day local suppliers
HP Storage Works Ultrium 640 Tape Drive	1	Backup tape drive	1 to 2 days
Lucent Portmaster Synchronous Router	1	Unknown (either HMS or Thompson Ln)	1 to 2 days
Smart UPS 1400 (APC)	2	Battery Backup	1 to 2 days
Linksys 16 port 10/100 hub	1	End user LAN connections	Same day local suppliers
IBM 33.6 Data Fax Modem	1	HMS connectivity to AS400	1 to 2 days (HMS)
IBM 7858	1	Unknown, Possibly CSU/DSU	1 to 2 days (HMS)
17 Inch CRT	1	AS400 Console	Same day local suppliers
Keyboard	1	AS400 Console	Same day local suppliers
HP/Compaq Tower PC	1	Dictation Server	1 to 2 days
Dell Workstation PC	1	AS400 Console	1 to 2 days (HMS)
IBM eServer (AS400)	1	HMS Software	1 to 2 days (HMS)
IBM Tape Drive	1	AS400 Backup	1 to 2 days (HMS)
Mitsubishi Electric Mr. Slim AC Unit with Auto Temp	1	Data Center Cooling	2 to 5 days

Form DR-7 Off-Site Storage Inventory

Off Site Storage Location (s)	
Street Address(s)	
Contact(s)	
Phone(s)	
Authorized individuals with access to Off-Site Storage Location(s).	

Description	Quantity	Location ID	Responsibility
Backup Tapes / Network Servers			
Backup Tapes / AS400			
Hot Spare Server/PC for TIER			
Hot Spare Laser Printer			
Hot Spare Tape Drive for Network Servers			
Copy of Disaster Recovery Plan			
Copies of Original Software Media			
Copies of Configuration / Software documentation			
Software Licensing Information			

Form DR-8 Emergency Contact Listing

Organization	Description	Contact Name	Phone Day/Night	Contact Date/Time
Police Department	Metro		911 or 862-7400	
Sheriff	Davidson County		862-8170	
Fire Department	Metro		911 or 862-5421	
Hospital	St. Thomas		222-6733	
Red Cross	Nashville		250-4300	
Civil Defense	Washington DC		202-646-3492	
Post Office	Nashville		615-885-9332	
FEMA	Washington DC		800-462-9029	
TV	WKRN		259-2200	
Radio	WLAC		664-2400	
Newspaper	Tennessean		259-8000	
	Legal Counsel			
	Risk Mgt./Insurance			
Electric	NES		747-3981	
Gas	Nashville Gas		734-0734	
Water	Metro Water		862-4800	
Sewer	Metro Water		862-4800	