



MEP Holding Company

Business Continuity Plan

By Paul G. Morey



Emergency Notification Contacts

Name	Address	Home #	Mobile #
Morey, Paul G.	6707 Loveland-Miamiville Road, Loveland, OH 45140		317-491-2930
Bielefeld, Greg	8810 Bay Pointe Circle, Indianapolis, IN 46236		317-339-2013
Henning, Rob	1507 Winding Creek Trail, Brownsburg, IN 46112		317-428-7382
Koors, John	1209 Wesley Court, Thorntown, IN 46071		317-557-9135
Lengerich, Luke	412 N. State Street, Greenfield, IN 46140		317-753-4448
Schrader, Nancy	454 London Lane, Avon, IN 46123		317-491-2520
Stichler, Ted	9463 Auburn Court, Lapel, IN 46051		317-223-9068
Hall, Karla	619 Shortlead Drive, Avon, IN 46123		317-714-0396
Zimmerman, Ginger	921 W. Stopek Drive, Nineveh, IN 46164		317-339-9847



Revisions control page

Date	Summary of changes made	Changes made by (Name)



Purpose

The purpose of this business continuity plan is to prepare MEP Holding Company in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All MEP Holding Company sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended voice communications service outages. It is a plan that encompasses all MEP Holding Company system sites and operations facilities.

Scope

The scope of this plan is limited to Business Continuity in an event of natural disasters or man made events. This is a business continuity plan, not a daily problem resolution procedures document.

Plan objectives

- Serves as a guide for the MEP Holding Company recovery teams.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

Disaster definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by MEP



Holding Company operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

Recovery teams

- Emergency management team (EMT)
- Disaster recovery team (DRT)
- IT technical services (IT)

See Appendix A for details on the roles and responsibilities of each team.

Team member responsibilities

- Each team member will designate an alternate
- All of the members should keep an updated calling list of their work team members' work, home, and cell phone numbers both at home and at work.
- All team members should keep this plan for reference at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

Instructions for using the business continuity plan

Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

Disaster declaration

The senior management team, with input from the EMT, DRT and IT, is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by MEP Holding Company senior management. The EMT and DRT will respond based on the directives specified by senior management.

Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the EMT and DRT must be activated immediately in the following cases:



- Two or more systems and/or sites are down concurrently for three or more hours
- Five or more systems and/or sites are down concurrently for three or more hours
- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur

External communications

Corporate public relations personnel are designated as the principal contacts with the media (radio, television, and print), regulatory agency, government agencies, and other external organizations following a formal disaster declaration.

Emergency management standards

Data backup policy

Full and incremental backups preserve corporate information assets and should be performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

Department-specific data and document retention policies specify what records must be retained and for how long. All organizations are accountable for carrying out the provisions of the instruction for records in their organization.

IT follows these standards for its data backup and archiving:

Tape retention policy

Backup media is stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing the system.

Billing tapes

- Tapes greater than three years old are destroyed every six months.
- Tapes less than three years old must be stored locally off-site.
- The system supervisor is responsible for the transition cycle of tapes.

System image tapes

- A copy of the most current image files must be made at least once per week.



- This backup must be stored offsite.
- The system supervisor is responsible for this activity.

Off-site storage procedures

- Tapes and disks, and other suitable media are stored in environmentally secure facilities.
- Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
- Access to backup databases and other data is tested annually.

Emergency management procedures

The following procedures are to be followed by system operations personnel and other designated MEP Holding Company personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

Note: Anyone not recognized by the IT staff as normally having business in the area must be challenged by the staff who should then notify security personnel.

These procedures are furnished to MEP Holding Company management personnel to take home for reference. Several pages have been included to supply emergency contacts.

In the event of any situation where access to a building housing a system is denied, personnel should report to alternate locations. Primary and secondary locations are listed below.

Alternate locations

Workplace: Edwards Electrical & Mechanical – Columbus, Ohio

- Attempt to contact your immediate supervisor or management via telephone. Home and cell phone numbers are included in this document

Workplace: Edwards Electrical & Mechanical – Dow AgroSciences

- Attempt to contact your immediate supervisor or management via telephone. Home and cell phone numbers are included in this document



In the event of a natural disaster

In the event of a major catastrophe affecting MEP Holding Company facility, immediately notify the **President, Paul G. Morey**.

Procedure

STEP	ACTION
1	Notify EMT and DRT of pending event, if time permits.
2	<p>If the impending natural disaster can be tracked, begin preparation of site within 48 hours as follows:</p> <ul style="list-style-type: none">• Deploy portable generators with fuel within 100 miles.• Deploy support personnel, tower crews, and engineering within 100 miles.• Deploy tractor trailers with replacement work space, antennas, power, computers and phones.• Facilities department on standby for replacement shelters• Basic necessities are acquired by support personnel when deployed:• Cash for one week• Food and water for one week• Gasoline and other fuels• Supplies, including chainsaws, batteries, rope, flashlights, medical supplies, etc.
3	<p>24 hours prior to event:</p> <ul style="list-style-type: none">• Create an image of the system and files• Back up critical system elements• Verify backup generator fuel status and operation• Create backups of e-mail, file servers, etc.• Fuel vehicles and emergency trailers• Notify senior management



In the event of a fire

If fire or smoke is present in the facility, evaluate the situation, determine the severity, categorize the fire as major or minor and take the appropriate action as defined in this section. Call 9-1-1 as soon as possible if the situation warrants it.

- Personnel are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
- In the event of a major fire, call 9-1-1 and immediately evacuate the area.
- In the event of any emergency situation, system security, site security and personal safety are the major concerns. If possible, the operations supervisor should remain present at the facility until the fire department has arrived.
- In the event of a major catastrophe affecting the facility, immediately notify senior management.

Procedure

STEP	ACTION
1	Dial 9-1-1 to contact the fire department.
2	Immediately notify all other personnel in the facility of the situation and evacuate the area.
3	Alert emergency personnel on: See Emergency Notification Contacts Provide them with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given.
4	Alert the EMT and DRT. <i>Note:</i> During non-staffed hours, security personnel will notify the Senior Executive responsible for the location directly.
5	Notify Building Security. Local security personnel will establish security at the location and not allow access to the site unless notified by the Senior Executive or his/her designated representative.



6	Contact appropriate vendor personnel to aid in the decision regarding the protection of equipment if time and circumstance permit.
7	All personnel evacuating the facilities will meet at their assigned outside location (assembly point) and follow instructions given by the designed authority. Under no circumstances may any personnel leave without the consent of supervision.

In the event of a network services provider outage

In the event of a network service provider outage to any location, the guidelines and procedures in this section are to be followed.

Procedure

STEP	ACTION
1	Notify senior management of outage. Determine cause of outage and timeframe for its recovery.
2	If outage will be greater than one hour, route all calls via alternate services. If it is a major outage and all carriers are down and downtime will be greater than 12 hours, deploy satellite phones, if available.



In the event of a flood or water damage

In the event of a flood or broken water pipe within any computing facilities, the guidelines and procedures in this section are to be followed.

Procedure

STEP	ACTION
1	Assess the situation and determine if outside assistance is needed; if this is the case, dial 9-1-1 immediately.
2	Immediately notify all other personnel in the facility of the situation and be prepared to cease voice operations accordingly.
3	Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly.
4	Water detected below the raised floor may have different causes: <ul style="list-style-type: none">• If water is slowly dripping from an air conditioning unit and not endangering equipment, contact repair personnel immediately.• If water is of a major quantity and flooding beneath the floor (water main break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow management's instructions.

Plan review and maintenance

This plan must be reviewed semiannually and exercised on an annual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, with the dynamic environment present within MEP Holding Company, it is important to review the listing of personnel and phone numbers contained within the plan regularly.

The hard-copy version of the plan will be stored in a common location where it can be viewed by site personnel and the EMT and DRT. Electronic versions will be available via MEP Holding Company network resources as provided by IT. Each recovery team will have its own directory with change management limited to the recovery plan coordinator.



Alert/Verification/Declaration phase (x-x hours)

Plan checklists

Response and recovery checklists and plan flow diagrams are presented in the following two sections. The checklists and flow diagrams may be used by IT members as "quick references" when implementing the plan or for training purposes.

Insert checklists and
other relevant procedure
documents here.



Plan checklists

[illegible]



Flow diagrams

Insert flow diagrams and other relevant procedure documents here.

Notification of incident affecting the site

On-duty personnel responsibilities

If in-hours:

Upon observation or notification of a potentially serious situation during working hours at a system/facility, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the EMT and DRT.

If outside hours:

IT personnel should contact the EMT and DRT.

Provide status to EMT and DRT

Contact EMT and/or DRT and provide the following information when any of the following conditions exist: (See Appendix B for contact list.)

- Two or more facilities are down concurrently for three or more hours.
- Any problem at any system or location that would cause the above condition to be present or there is certain indication that the above condition is about to occur.

The EMT will provide the following information:

- Location of disaster
- Type of disaster (e.g., fire, hurricane, flood)
- Summarize the damage (e.g., minimal, heavy, total destruction)
- Meeting location that is a safe distance from the disaster scene
- An estimated timeframe of when a damage assessment group can enter the facility (if possible)



- The EMT will contact the respective market team leader and report that a disaster involving voice communications has taken place.

The EMT and/or DRT will contact the respective MEP Holding Company team leader and report that a disaster has taken place.

Decide course of action

Based on the information obtained, the EMT and/or DRT need to decide how to respond to the event: mobilize IT, repair/rebuild existing site (s) with location staff, or relocate to a new facility.

Inform team members of decision

If a disaster is not declared, the location response team will continue to address and manage the situation through its resolution and provide periodic status updates to the EMT/DRT.

If a disaster is declared, the EMT and/or DRT will notify IT Tech Services immediately for deployment.

Declare a disaster if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one backup person who is also authorized to declare a disaster in the event the primary person is unavailable.

Contact general vendors (see Appendix I)

Disaster declared: Mobilize incident response/Technical services teams/Report to command center

Once a disaster is declared, the DRT is mobilized. This team will initiate and coordinate the appropriate recovery actions. Members assemble at the designated location as quickly as possible. See Appendix E for emergency locations.



Conduct detailed damage assessment (This may also be performed prior to declaring a disaster.)

1. Under the direction of local authorities and/or EMT/DRT, assess the damage to the affected location and/or assets. Include vendors/providers of installed equipment to ensure that their expert opinion regarding the condition of the equipment is determined ASAP.
 - A. Participate in a briefing on assessment requirements, reviewing:
 - (1) Assessment procedures
 - (2) Gather requirements
 - (3) Safety and security issues

NOTE: Access to the facility following a fire or potential chemical contamination will likely be denied for 24 hours or longer.

- B. Document assessment results using assessment and evaluation forms contained in Appendix G.

Building access permitting:

- Conduct an on-site inspection of affected areas to assess damage to essential hardcopy records (files, manuals, contracts, documentation, etc.) and electronic data.
 - Obtain information regarding damage to the facility (s) (e.g., environmental conditions, physical structure integrity, furniture, and fixtures) from the DRT.
2. Develop a restoration priority list, identifying facilities, vital records and equipment needed for resumption activities that could be operationally restored and retrieved quickly.
 3. Recommendations for required resources.

Contact DRT: Decide whether to continue to business recovery phase

The EMT and DRT gather information regarding the event; contacts senior management and provides them with detailed information on status.

Based on the information obtained, senior management decides whether to continue to the business recovery phase of this plan. If the situation does not warrant this action, continue to address the situation at the affected site(s).



Business recovery phase (xx hours - full recovery)

This section documents the steps necessary to activate business recovery plans to support full restoration of systems or facility functionality at an alternate/recovery site that would be used for an extended period of time. Coordinate resources to reconstruct business operations at the temporary/permanent system location, and to deactivate recovery teams upon return to normal business operations.

MEP Holding Company system and facility operation requirements

The system and facility configurations for each location are important to re-establish normal operations. A list for each location will be included in Appendix F.

Notify IT staff/Coordinate relocation to new facility

See Appendix A for IT staff associated with a new location being set up as a permanent location (replacement for site).

Secure funding for relocation

Make arrangements in advance with suitable backup location resources. Make arrangements in advance with local banks, credit card companies, hotels, office suppliers, food suppliers and others for emergency support.

Notify EMT and corporate business units of recovery startup

Using the call list in Appendix B, notify the appropriate company personnel. Inform them of any changes to processes or procedures, contact information, hours of operation, etc. (This may be used for media information.)

Operations recovered

Assuming all relevant operations have been recovered to an alternate site, and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the recovery location.



Appendixes

Appendix A: MEP Holding Company recovery teams

Emergency management team (EMT)

Note: See Appendix B for contact list. Suggested members to include: senior management, human resources, corporate public relations, legal, IT services, risk management and operations

Charter:

Responsible for overall coordination of the disaster recovery effort; evaluation and determining disaster declaration; and communications with senior management.

Support activities:

The EMT:

- Evaluate which recovery actions should be invoked and activate the recovery teams
- Evaluate damage assessment findings
- Set restoration priority based on the damage assessment reports
- Provide senior management with ongoing status information
- Act as a communication channel to corporate teams and major customers
- Work with vendors and IRT to develop a rebuild/repair schedule

Disaster recovery team

Note: See Appendix B for contact list

Charter:

Responsible for overall coordination of the disaster recovery effort; establishment of the emergency command area; and communications with senior management and the EMT.

Support activities:

- Coordinate with EMT and senior management
- Determine recovery needs
- Establish command center and assembly areas
- Notify all company department heads and advise them to activate their plan(s) if applicable, based upon the disaster situation
- If no disaster is declared, take appropriate action to return to normal operations using regular staff



- Determine if vendors or other teams are needed to assist with detailed damage assessment
- Prepare post-disaster debriefing report
- Coordinate the development of site-specific recovery plans and ensure they are updated semi-annually

IT technical services (IT)

Charter

IT will facilitate technology restoration activities.

Support activities

- Upon notification of disaster declaration, review and provide support as follows:
 1. Facilitate technology recovery and restoration activities, providing guidance on replacement equipment and systems, as required
 2. Coordinate removal of salvageable equipment at disaster site that may be used for alternate site operations

Appendix B: Recovery team contact lists

Emergency management team (EMT)

Name	Address	Home	Mobile/Cell Phone
Morey, Paul G.	6707 Loveland-Miamiville Road, Loveland, OH 45140		317-491-2930

Disaster recovery team (DRT)

Name	Address	Home	Mobile/Cell Phone
Morey, Paul G.	6707 Loveland-Miamiville Road, Loveland, OH 45140		317-491-2930

IT technical services

Name	Address	Home	Mobile/Cell Phone
Henning, Rob	1507 Winding Creek Trail, Brownsburg, IN 46112		317-428-7382
Lengerich, Luke	412 N. State Street, Greenfield, IN 46140		317-753-4448



Appendix C: Emergency numbers

First responders, public utility companies, others

Name	Contact Name	Phone
See Attachment Appendix C		

Appendix D: Contact list

Name	Address	Home	Mobile/Cell Phone
See Attachment Appendix C			



Appendix E: Emergency command center (ECC) locations

Emergency command center – Columbus Office

Primary: 1782 Dividend Drive
Columbus, OH 43228
Office (614) 485-2003
Contact: Paul G. Morey, President (317) 491-2930



Appendix F: Forms

Incident/disaster form

Upon notification of an incident/disaster situation the on-duty personnel will make the initial entries into this form. It will then be forwarded to the ECC, where it will be continually updated. This document will be the running log until the incident/disaster has ended and “normal business” has resumed.

TIME AND DATE

TYPE OF EVENT

LOCATION

BUILDING ACCESS ISSUES



PROJECTED IMPACT TO OPERATIONS

RUNNING LOG (ongoing events)

[illegible]



Critical equipment status form

**CRITICAL EQUIPMENT STATUS
ASSESSMENT AND EVALUATION FORM**

Recovery team: _____

<u>Equipment</u>	[-----STATUS-----]		<u>Comments</u>
	<u>Condition</u>	<u>Salvage</u>	
1. _____	_____	_____	_____
2. _____	_____	_____	_____
3. _____	_____	_____	_____
4. _____	_____	_____	_____
5. _____	_____	_____	_____
6. _____	_____	_____	_____
7. _____	_____	_____	_____
8. _____	_____	_____	_____
9. _____	_____	_____	_____
10. _____	_____	_____	_____
11. _____	_____	_____	_____
12. _____	_____	_____	_____
13. _____	_____	_____	_____
14. _____	_____	_____	_____
15. _____	_____	_____	_____

Legend

Condition: OK - Undamaged
 DBU - Damaged, but usable
 DS - Damaged, requires salvage before use
 D - Destroyed, requires reconstruction



Appendix G: Building evacuation information

See Attached Appendix G
Schedule

Appendix H: Inventory of primary equipment and network services

See Attached Appendix H
Schedule

Appendix I: Inventory of backup equipment and systems

Dell PowerEdge T310 with Quantum SuperLoader3 LTO-4 with 8 slot tape vault attached. Backup Exec v2011 installed on server which runs Full Backup of all production servers nightly (M-F) at 11:00 pm. Nightly backup runs for approximately 6 hrs. Each morning, previous night's backup media is taken off site until following workday.

Tapes are LTO-4 and are kept in a '1/day, 4 week' series. All tapes that are not in active week sequence (in the SuperLoader vault) are stored in fireproof safe, either in IT Server Room or Paul's office. Monthly Full backups occur during the 2nd weekend of each calendar month, Quarterly Full backups occur on the same sequence, and one Yearly backup is performed the 1st week of January each year. All M/Q/Y backups are stored in fireproof safes.

Provide list of equipment

Appendix J: Approved vendor list

Server and computer equipment suppliers

Company Name	Contact	Work	Mobile phone
Dell computers	Garrett Sullivan	800-274-3355 Ext5139816	
ESI Technology	Bryan Bulthaup	317-596-9891	317-596-9894
CDW	Mark Deen	866-239-4370	
Van Ausdall Ferrar	Ryan Langfeld	800-467-7474	317-974-7271



Communications and network services suppliers

Company Name	Contact	Work	Mobile phone
Sprint	Beth Miller	317-705-8360	317-339-1001
Midwest Wireless	Melissa Adams	317-876-7373	
Grant Communications	John Spaulding	317-536-0754	317-514-3008
ATT Tech	Jeff		317-966-4492
Lightbound Comm	Richard Coonfield	877-291-7210	317-777-7715
Lightbound Comm	Jathan Haggard	877-271-5214	317-777-7713
Lightbound Noc	Tech on call	317-777-7155	
Advanced Network Solutions	Dave Fox	317-859-8290	317-216-8162
Indatus- Planet Telecom	Debbie Halverson	800-727-4246	812-945-6355
Trimble At Road	Mark Allen	510-668-1638	510-714-8209
ATT/SBC repair Center	Tech on call	877-888-5622	
Vision InfoSoft	Aaron Cobb	800-258-7752	
Esco Communications	Mark McCarty	317-298-2975	317-532-1310

Appendix H Schedule:

Primary Network Equipment

SERVER01	PowerEdge 2850
SERVER02	Precision 520
SERVER03	GX520
SERVER04	PowerEdge T310
SERVER05	PowerEdge T310
SERVER06	Gx260
SERVER07	Poweredge 2850
SERVER08	Poweredge 2850
SERVER09	Poweredge 2850
Cisco 2821	Internet load balance
Cisco ASA5510	Edge Firewall
Cisco ASA5505	VPN Routing Cincy
Adtran T1	Columbus T1
Baystack	Columbus T1
Dell PowerEdge 100/1000	Lan Switching
Quantum Superloader3	LTO4 Backup



Cisco IAD2400 2- Bonded T1
Netopia DSL 3347

Lightbound Voice Data
DSL Internet

APC Smart UPS Battery BU
Anon 70KW Nat Gas Generator

Smart UPS 2200
Server Room Aux Pwr

Further Narrative of Network Servers:

Server01

Windows 2003 Std R2 w/2003 Active directory domain controller. File and Print Server.

Programs host, RRAS

Start Life 1/01/05

Power Edge 2850 U-Rack Server with redundant P/S and Raid 5 (6 drives)

Hosting

P:\ personal logon.bat user folder map

R:\Shared company dept resources and files

S:\Cad files

T:\QR app

U:\User share dept folders

Hosting

Quickpen Drawing /Take off app

QRapp database

AllTrak tool manager database

Epic pricing/EBM estimating (Not in use as of June1 2010, no support)

DCA collector for Van Ausdall Printer meters

Server 01 is a primary production server that cannot afford any downtime. It gets a full backup M~F starting at 11:00pm using BUexec 2011 remote agent to tape on Server05.

Need to document share permissions on R:\ in excel.

Server01 cannot be rebooted without interrupting production. Reboots must be planned and after hours unless an emergency situation is occurring. Notification must be given to ensure file closure at desktops to prevent possible data loss.

All servers(and desktops) that talk back to 10.104.x.x or 10.105.x.x need -p route adds
Route Add -p 10.104.0.0 mask 255.255.0.0 10.100.0.10



Route Add -p 10.105.0.0 mask 255.255.0.0 10.100.0.12

ASA5510 firewall does not route to those segments above.

Server02

2003 Std server is a file/app sharing server hosting the Websense URL filtering software. Dell Precision 530 with Mirror drives.

Fresh install 5/05/10

Hardware 1/01/03

Two Nics are installed one is primary server IP with 2nd listening for http requests for websense.

D drive hosts the "admin" share for "new machine installs.

Server is ok to reboot anytime with no interruption to production. Websense URL filter will go offline temporarily during reboot and will autostart.

Server is backed up monthly, Qtrly, Yrly to server 05 BU Exec 2011 remote agent.

Server03

Windows 2003 Std server hosting the Websense email security application filter with Sql 2005 express. Optiplex GX620

Fresh Install 12/12/09

Hardware 1/01/07

This server is running on a Dell Optiplex 620 and can be rebooted without interrupting production. Email transport will go offline during the reboot, but will autostart after reboot. Websense passes SMTP traffic to and from Server08 to gateway and then internet. MX records are used to route emails to various smtp destinations.

Websense email filtering must be monitored throughout the day for Isolated, spam, NDR emails that might be trapped in Queue. Legitimate email must be manually released

Server04

Windows 2003 std R2 running Terminal services and hosting applications for remote users in Ohio offices and for select laptop users.

Poweredge T310 Quad core Xeon X3470 CPU w/4GB of Ram. 2 1TB drives in Mirror.



Fresh Install 8-18-2011

Applications are Timberline, S2K, Office 2003, Qrapp, Fishbowl Inventory Client for remote users.

Server can rebooted if all remote users are notified and logged off before hand. Shutdown sequence is documented on Admin desktop. User shutdown has been disabled on taskbar.

Server05

Windows 2003 Std R2 hosting Backup Exec 2011. Server is a Dell Poweredge T310 Quad core Xeon X3430 CPU w/4GB of Ram. 2 1TB drives in Mirror.

Start Life 4/04/10

C:\ 50GB partition

D:\ 882 GB partition

LSI SAS 3000 PCI-e card drives Quantum SuperLoader3 LTO-4 tape vault

LSI 320 PCI-e drives legacy Dell powervault if needed to access legacy backup media

Backup Exec 2011 runs M~F

Inventory runs @ 10:00 pm

Production Svrs 01;07;08 full backup runs @ 11:00 pm Daily BU goes offsite till next day

Monthly Full on all servers runs 2 or 3rd week into month for previous depending on Whip status. Goes off site till next monthly

Quarterly BU runs every 3 months. Goes to cold storage in Paul fire proof safe.

Yearly BU runs 1st week in Jan. before AD changes for previous year get made; goes to cold storage.

BU Exec Licenses are in Software Documentation folder (File Cabinet)

Server06

Windows 2000 SP4 hosting SpectreSoft CNE and database

Optiplex GX 240

OS Installed 3/17/02

80GB HD

8GB boot partition

58GB Data Partition



Hardware is Old and needs to be retired

CNE has upgrade version available that needs to be installed on another server.(Svr05 ?)
Server will not accept windows updates.

Server07

Windows 2003 Std R2 server hosting Business management apps
Timberline (Accounting), S2K (Dispatching), Fishbowl (Inventory)
Dell Poweredge 2850 Installed 1/05/05. Raid failed 7/02/09 restored from backup
* Raid Error Disk 0:1 on 1/6/11 rebuild failed, replaced drive 1/7/11 Array online but now
receiving various warnings about data blocks and sectors. Contact Dell to advise.

Power Edge 2850 U-Rack Server with redundant P/S and Raid 5 (6 drives)
C:\ 10 GB partition that is low on space
D:\ 673 GB

Shares
Programs
Restore
Timberline Office

This is a production server that cannot be rebooted during working hours unless required by an emergency condition. All users must have opportunity to log out and close apps.

Server07 is fully backedup daily at 11:00 pm M~F

Server08

Windows 2003 Std R2 server hosting Exchange Enterprise 2003 hosting email for edwards-
elec.com, e-solutions-inc.com and mepholding.com
OWA is configured for remote use, Exchange Active sync is configured for basic text Auth no
SSL.
Dell Poweredge 2850 Installed 1/05/05.

Power Edge 2850 U-Rack Server with redundant P/S and Raid 5 (6 drives)
C:\ 10 GB
D:\ 24GB
F:\ 409GB



This is a production server that cannot be rebooted during normal operations without advanced notice.

Gets a monthly reboot and full backup M~F 11:00pm with BU Exec 2011 (Exchange Agent installed)

Server09

Windows 2003 Std R2 server functioning as Cold Storage and a “Hot Swap” spare for Servers 01. 07, 08

Dell Poweredge 2850 Installed 1/05/05.

Power Edge 2850 U-Rack Server with redundant P/S and Raid 5 (3 drives)

C:\ 10 GB

D:\ 263GB

Cold Storage for Termed .PST and users files.

This server can be updated and/or rebooted at any time. Check for Cad connection to cold storage Cad Archives.