



# Affordable Office Interiors dba Business Office Systems

## “IT Disaster Recovery Plan”

## Table of Contents


Main Contact Information IL ……. 4-5
Main Contact Information WI …….. 6-7
Emergency Calling Tree ……... 8-9
Information Technology Statement of Intent ……. 10
Policy Statement …… 10
Objectives …… 10
Key Personal Contact Info …….. 11
External Contacts …… 12-13
1 Plan Overview …….. … 14
1.1 Plan Updating …….. 14
1.2 Plan Documentation Storage ……. 14
1.3 Backup Strategy …… 14
1.4 Risk Management …… 15
2 Emergency Response …… 15
2.1 Alert, escalation and plan invocation …… 15
2.1.1 Plan Triggering Events …… 15
2.1.2 Assembly Points ……. 15
2.1.3 Activation of Emergency Response Team …… 15
2.2 Disaster Recovery Team …….. 16
2.3 Emergency Alert, Escalation and DRP Activation ……. 16
2.3.1 Emergency Alert ……. 16
2.3.2 DR Procedures for Management ……. 17
2.3.3 Contact with Employees …… 17
2.3.4 Backup Staff …… 17
2.3.5 Recorded Messages / Updates …… 17
2.3.7 Alternate Recovery Facilities / Hot Site …….. 17
2.3.8 Personnel and Family Notification …….. 17
3 Media ……. 18
3.1 Media Contact ……..... 18
3.2 Media Strategies ……. 18
3.3 Media Team ……. 18
3.4 Rules for Dealing with Media ……. 18
4 Insurance …… 18
5 Financial and Legal Issues …….. 19
5.1 Financial Assessment …….. 19
5.2 Financial Requirements …… 19
5.3 Legal Actions ……. 19
6 DRP Exercising …… 19
Appendix A – Technology Disaster Recovery Plan Templates ……..... 20-21

## Table of Contents

Disaster Recovery Plan for Voice Communications …… 22
Appendix B – Suggested Forms …… 23
Damage Assessment Form ……... 23
Management of DR Activities Form …… 23
Disaster Recovery Event Recording Form …… 24
Disaster Recovery Activity Report Form …… 24
Mobilizing the Disaster Recovery Team Form …….. 25
Mobilizing the Business Recovery Team Form …… 25
Monitoring Business Recovery Task Progress Form …… 26
Preparing the Business Recovery Report Form ……..... 26
Communications Form …….. 27
Returning Recovered Business Operations to Business Unit Leadership …… 27
Business Process / Function Recovery Completion Form …….. 27-28

# Main Contact Information

**Affordable Office Interiors dba Business Office Systems**
501 S. Gary Avenue, Roselle, IL 60172
Main Phone: 630.784.7730 & 630.773.7777
Primary Emergency Contact:
Website: www.affordableoffice.com & www.bos.com
Facebook:
Twitter:

**AOI/BOS Roselle Building Contact**
Stephen Sabor, CBRE
Phone: 847.585.0682
Cell: 847.220.0938
stephen.sabor@cbre.com

**********

**Business Office Systems - Chicago**
328 S. Jefferson Street, Suite 110, Chicago, IL 60661
Main Phone: 312.670.8530
Primary Emergency Contact:

**BOS Chicago Building Contact**
Jennifer Valentini, Blue Star Properties
600 W. Van Buren Street, Suite 1000, Chicago, IL 60607
Phone: 312.855.2232
Jennifer@bluestarproperties.net
**********

# Main Contact Information

## ROSELLE EMERGENCY SERVICES

**Roselle Police Department**
103 S Prospect Street, Roselle Illinois 60172
Main Phone: 630.980.2025
Emergency Phone: 911 – Roselle Tested 2/2016

**Roselle Fire Department**
110 E. Maple Avenue, Roselle, IL 60172
Main Phone Fire Station: 630.980.2043
Emergency Phone: 911

**Nearby Hospitals For Roselle Office:**
Alexian Brothers (9.6 Miles – 14 Minutes)
800 Biesterfield Road, Elk Grove Village, IL 60007
Phone: 847.437.5550

Adventist Glen Oaks Hospital (6.3 Miles – 14 Minutes)
701 Winthrop Avenue, Glendale Heights, IL 60139
Phone: 630.545.8000

## CHICAGO EMERGENCY SERVICES

**Chicago Police Department Main Office**
3510 South Michigan Avenue, Chicago, IL 60653
Main Phone: 312.744.4000 (Non-Emergency Only)
**18th District**
1160 North Larrabee Street, Chicago, IL 60610
**********
Main Phone: 312.742.5870 (Non-Emergency Only)
Emergency Phone: 911

**Chicago Fire Department – District #1 Headquarters**
55 West Illinois Street, Chicago, IL 60654
**********
Main Phone: 312.744.5742 (Non-Emergency Only)
Emergency Phone: 911

**Nearby Hospital For Chicago Office: Rush University Medical Center**
1653 W. Congress Parkway, Chicago, IL 60612
Main Phone: 312.942.5000

# Main Contact Information

**Affordable Office Interiors - Madison**
2425 S. Stoughton Road, Madison, WI 53716
Main Phone: 608.442.0430
Primary Emergency Contact:

**AOI – Madison Building Contact**
Don Hornung – 608.242.2991 X303 (Main) – 608.220.3068 (Cell) - Email: djh@tds.net

**Affordable Office Interiors - Milwaukee**
1575 N. Barker Road, Brookfield, WI 53045
Main Phone: 262.777.2000
Primary Emergency Contact:

**AOI – Milwaukee Building Contact**
Thorsten Wienss, Trace-A-Matic, 21125 Enterprise Drive, Brookfield, WI 53045 – 262-797-7300
Email: twienss@traceamatic.com

**Insurance Agent: Wine Sergi & Co, LLC**
225 Smith Road, St. Charles, IL 60174
Main Phone: 630.513.6600
Contact: Richard W. Ryan
Account #

# Main Contact Information

## MADISON EMERGENCY SERVICES

**Madison Police Department**
South District
825 Hughes Place, Madison, WI 53716
Main Phone: 608.266.5938

**Madison Fire Department**
Blooming Grove Fire Department
1880 S. Stoughton Road, Madison, WI 53716
Main Phone: 608.222.4155

**Nearby Hospital For Madison Office**
Dean Clinic – East Urgent Care
1821 S. Stoughton Road, Madison, WI 53716
Main Phone: 608.250.1525

**Madison Alarm Company**
Midwest Security
Main Phone: 608.233.5039

## BROOKFIELD EMERGENCY SERVICES

**Brookfield Police Department**
655 N. Janacek Road, Brookfield, WI 53045
Main Phone: 262-796-3798

**Brookfield Fire Department**
645 N. Janacek Road, Brookfield, WI 53045
Main Phone: 262-796-3792

**Nearby Hospital For Brookfield Office**
Elmbrook Memorial Hospital
19333 W. North Avenue, Brookfield, WI 53045
Main Phone: 262.785-2000

# Emergency Calling Tree

**In case of any emergency or disaster where the company needs to be made notified for direction or a number of steps should be implemented:**

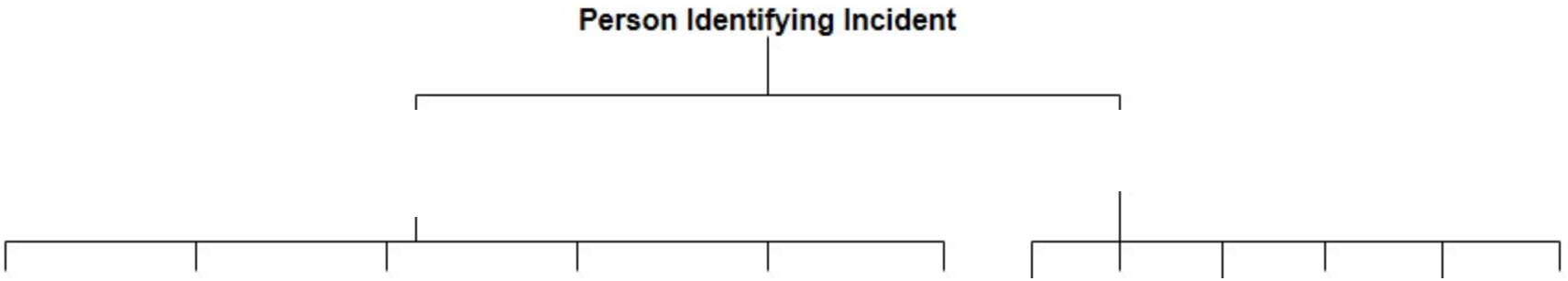
- **Notification will go out on LinkedIn to AOI LinkedIn account:**

- **Notification will go out via e-mail, if available.**

- **Notification will go out via Facebook.**

- **Phone contact via calling tree (see attached).**

# Calling Tree




Note: All phone numbers listed are cell phones.

## Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

## Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

## Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

## Key Personnel Contact Info

| Name, Title | Contact Option | Contact Number |
|---|---|---|
| | Work | |
| | Alternate | |
| | Mobile | |
| | Home | |
| | Email Address | |
| | Alternate Email | |
| | | |
| | Work | |
| | Alternate | |
| | Mobile | |
| | Home | |
| | Email Address | |
| | Alternate Email | |
| | | |
| | Work | |
| | Alternate | |
| | Mobile | |
| | Home | |
| | Email Address | |
| | Alternate Email | |
| | | |
| | Work | |
| | Alternate | |
| | Mobile | |
| | Home | |
| | Email Address | |
| | Alternate Email | |

## External Contacts

| Name, Title | Contact Option | Contact Number |
|---|---|---|
| **Landlord / Property Manager** | | |
| CBRE (Roselle) | Work | Stephen Sabor - 847.585.0682 |
| Account # | Mobile | Stephen Sabor - 847.220.0938 |
| | Fax | |
| | Home | |
| | Email Address | stephen.sabor@cbre.com |
| | | |
| **Power Company** | | |
| Glacial Energy (Chicago Only) | Work | 888.452.2425 |
| | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| ComEd (Roselle) | Work | 877.426.6331 |
| | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Telecom Carrier 1** | | |
| Mitel | Work | 800.722.1301 |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | micloudsupport@mitel.com |
| | | |
| **Internet Carriers** | | |
| RCN (Chicago) | Work | 570.270.1154 |
| AT&T (Roselle) | Work | 312.241.8851 |
| Evergent (Roselle/Wireless Back-Up) | Work | 262.818.3785 |
| | Home | |
| | Email Address | |
| | | |
| **Hardware Supplier 1** | | |
| | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Emergency Reporting | |
| | Email Address | |
| | | |
| **Server Supplier 1** | | |
| Dell | Work | 800.999.3355 |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Workstation Supplier 1** | | |
| Dell | Work | 800.999.3355 |
| Microsoft | Work | 847.466.2830 |
| Account # | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Office Supplies 1** | | |
| | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |

## External Contacts (continued)

| Name, Title | Contact Option | Contact Number |
|---|---|---|
| **Insurance** | | |
| | Work | Sue Wolfe: |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Site Security** | | |
| N/A | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Off-Site Storage 1** | | |
| Pickens-Kane | Work | Jim Munroe: 630.924.4400 |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | Jim Munroe: jmunroe@pickenskane.com |
| | | |
| **Off-Site Storage 2** | | |
| | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **HVAC** | | |
| Mercury Mechanical | Work | Tim: 708.409.8655 |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Emergency Reporting | |
| | Email Address | |
| | | |
| **Power Generator** | | |
| | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |
| | | |
| **Other** | | |
| | Work | |
| Account # | Mobile | |
| | Fax | |
| | Home | |
| | Email Address | |

# 1 Plan Overview

## 1.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Director.

## 1.2 Plan Documentation Storage

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

## 1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is real time replication of project data to a backup facility and imaging of other server systems. This strategy entails the maintenance of a backup site which will enable instantaneous access to project data, and maintenance of backup images allowing quick recovery to a variety of hardware platforms for other systems.

| KEY BUSINESS PROCESS | BACKUP STRATEGY |
|---|---|
| IT Operations | Nightly offsite image |
| Tech Support - Hardware | One full time technical support employees |
| Tech Support - Software | One full time technical support employees |
| Facilities Management | Backup facility |
| Email | Nightly offsite image |
| Purchasing | Nightly offsite image |
| Disaster Recovery | Bootable media for recovery of images |
| Finance | Nightly offsite image |
| Contracts Admin | ********** |
| Warehouse & Inventory | Nightly offsite image |
| Product Sales | Nightly offsite image |
| Maintenance Sales | Nightly offsite image |
| Human Resources | Nightly offsite image |
| Testing Fully Mirrored Recovery site - | Real time replication tested daily |
| Web Site | Hosted offsite with onsite backup |

## 1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

| Potential Disaster | Probability Rating | Brief Description Of Potential Consequences & Remedial Actions |
|---|---|---|
| Flood | 1 | All critical equipment is located on 1st Floor |
| Fire | 2 | Server room isolate from most of facility by firewall. If lost, wiring closet could act as temporary server room. If wiring closet is lost, server room can host network via WiFi |
| Tornado | 3 | <see above> |
| Electrical storms | 4 | Server room is interior to building, entire room and wiring closet is protected by UPS with manual generator backup |
| Act of terrorism | 2 | Resort to backup facility |
| Act of sabotage | 3 | Full server images taken every night. Restore to backup hardware |
| Electrical power failure | 4 | Entire server room and wiring closet is protected by UPS with manual generator backup |
| Loss of communications network services | 4 | Primary data comes from Comcast. Backup data comes from AT&T via different external paths. If both are lost, wireless options or remote facility may be employed |

Probability: 1=Very Low, 5=Very High

# 2 Emergency Response

## 2.1 Alert, escalation and plan invocation

### 2.1.1 Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

### 2.1.2 Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – Holiday Inn Express & Suites (Next Store to Roselle Office)
- Alternate –

### 2.1.3 Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

## 2.2 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 48.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

## 2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

### 2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

### 2.3.2 DR Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

### 2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

### 2.3.4 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

### 2.3.5 Recorded Messages / Updates

***For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.***

### 2.3.7 Alternate Recovery Facilities / Hot Site

If necessary, the site in Chicago will be activated and notification will be given via recorded messages or through communications with managers.

### 2.3.8 Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

# 3 Media

## 3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

## 3.2 Media Strategies

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
    - What happened?
    - How did it happen?
    - What are you going to do about it?

## 3.3 Media Team

## 3.4 Rules for Dealing with Media

**Only** the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

# 4 Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers liability, general liability, and business interruption insurance.

*If insurance-related assistance is required following an emergency out of normal business hours, please contact:* _____

| Policy Name | Coverage Type | Coverage Period | Amount Of Coverage | Person Responsible For Coverage | Next Renewal Date |
|---|---|---|---|---|---|
| **Wine Sergi** | | | | **Sue Wolfe** | |
| | | | | | |
| | | | | | |

# 5 Financial and Legal Issues

## 5.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

## 5.2 Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

## 5.3 Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

# 6 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

**Appendix A – Technology Disaster Recovery Plan Templates**

**Disaster Recovery Plan for Servers**

**Physical Host Description:**

| | |
|---|---|
| **Chassis** | Dell VRTX |
| | 8x1 GbE Switch |
| | 25 x 2.5" Drive Bays |
| | 1.2TB 10K 2.5" 6Gbps SAS Drives x 22 (RAID 6) |
| | Hotplug Backplane with Dual Controller |
| | DVD+/-RW |
| | 4x1100W Power |
| **Servers** | **CS-HOST1** |
| | Dell PowerEdge M520 |
| | 12G iDRAC7 Express |
| | SAS Backplane / H310 Controller |
| | Xeon E5-2450 2.5GHz 20M Cache 8 Core CPU x 2 |
| | 16GB RDIMM 1600MT/s Low Volt Dual Rank x4 Data Width x 8 |
| | 300GB 10k 2.5" 6Gbps SAS Drives x 2 (RAID 1) |
| | **CS-HOST2** |
| | Dell PowerEdge M520 |
| | 12G iDRAC7 Express |
| | SAS Backplane / H310 Controller |
| | Xeon E5-2450 2.5GHz 20M Cache 8 Core CPU x 2 |
| | 16GB RDIMM 1600MT/s Low Volt Dual Rank x4 Data Width x 8 |
| | 300GB 10k 2.5" 6Gbps SAS Drives x 2 (RAID 1) |

| | |
|---|---|
| **Operating System** | Microsoft Windows 2012 R2 Datacenter |
| | CS-HOST1 and CS-HOST2 are nodes in live failover cluster CS-CLUSTER01 |
| **Backup Solutions** | Symantec System Recover 2013 for images |
| | Veeam Backup and Recovery for virtual machines |
| **Data Protections** | TIER1: All server systems protected by RAID1 / server data protected by RAID6 |
| | TIER2: RAID6 protected with multiple automatic online hot spares |
| | TIER3: Non-database data replicated in real-time to sat. offices with live failover |
| | TIER4: User data incremental backups 2-4x during working hours |
| **Backup Methodology** | Full nightly image backup of hosts |
| | Full nightly image backup of backup and recovery system |
| | 2-4x workday incremental backups of all virtual machines, full image on Friday |
| **Offsite Storage** | All backups removed from facility nightly |
| | Daily backups retained for 1 week |
| | Weekly backups retained for 1 month |
| | Annual backups retained for 5 years |
| **Recovery Metric** | Full server recovery in 12 hours tested quarterly |
| **Recovery Procedures** | |
| **Loss of user data** | TIER1: Check satellite office volumes for lost data |
| | TIER2: Use Veeam to recover individual files |
| **Loss of virtual machine** | Use Veeam to recover guest machine |
| **Loss of email VM** | Use Symantec System Recovery to restore guest machine |
| **Loss of host machine** | Use Symantec System Recovery to restore host machine |
| **Loss of backup server** | Use Symantec System Recovery to restore backup server |
| **Loss of hardware** | Use Symantec System Recovery to restore to 2xPowerEdge 2900 cold spares |

## Disaster Recovery Plan for Voice Communications

| SYSTEM | |
|---|---|

| OVERVIEW | |
|---|---|
| EQUIPMENT | Location:<br>Device Type:<br>Model No.:<br>Technical Specifications:<br>Network Interfaces:<br>Power Requirements;<br>System Serial #:<br>DNS Entry:<br>IP Address:<br>Other: |
| HOT SITE EQUIPMENT | Cell phone backup |
| SPECIAL APPLICATIONS | |
| ASSOCIATED DEVICES | |

| KEY CONTACTS | |
|---|---|
| Hardware Vendor | Provide details |
| System Owners | Provide details |
| Database Owner | Provide details |
| Application Owners | Provide details |
| Software Vendors | Provide details |
| Offsite Storage | Provide details |
| Network Services | Provide details |

| BACKUP STRATEGY for SYSTEM TWO | |
|---|---|
| Daily | Provide details |
| Monthly | Provide details |
| Quarterly | Provide details |

| SYSTEM TWO DISASTER RECOVERY PROCEDURE | |
|---|---|
| Scenario 1<br><br>Total Loss of Switch | Provide details |
| Scenario 2<br><br>Total Loss of Network | Provide details |

## Appendix B – Suggested Forms

### Damage Assessment Form

| Key Business Process Affected | Description Of Problem | Extent Of Damage |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

---

### Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

| **Activity Name:** |
|---|
| **Reference Number:** |
| **Brief Description:** |

| Commencement Date/Time | Completion Date/Time | Resources Involved | In Charge |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

---

## Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

| |
|---|
| **Description of Disaster:** |
| **Commencement Date:** |
| **Date/Time DR Team Mobilized:** |

| Activities Undertaken by DR Team | Date and Time | Outcome | Follow-On Action Required |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| |
|---|
| **Disaster Recovery Team's Work Completed:** <Date> |
| **Event Log Passed to Business Recovery Team:** <Date> |

---

## Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

---

## Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

| **Description of Emergency:** |
|---|
| Date Occurred: |
| Date Work of Disaster Recovery Team Completed: |

| Name of Team Member | Contact Details | Contacted On (Time / Date) | By Whom | Response | Start Date Required |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Relevant Comments (e.g., Specific Instructions Issued) | | | | | |

---

## Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

| **Description of Emergency:** |
|---|
| Date Occurred: |
| Date Work of Business Recovery Team Completed: |

| Name of Team Member | Contact Details | Contacted On (Time / Date) | By Whom | Response | Start Date Required |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Relevant Comments (e.g., Specific Instructions Issued) |
|---|
| |

## Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period of time.
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

*Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.*

| Recovery Tasks (*Order of Priority*) | Person(s) Responsible | Completion Date | | Milestones Identified | Other Relevant Information |
|---|---|---|---|---|---|
| | | Estimated | Actual | | |
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| 4. | | | | | |
| 5. | | | | | |
| 6. | | | | | |
| 7. | | | | | |
| | | | | | |

## Preparing the Business Recovery Report Form

- On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed.
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be distributed to senior management, as appropriate.

The contents of the report shall include:

- A description of the incident
- People notified of the emergency (including dates)
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan

- Lessons learned

## Communications Form

- It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed.
- The information given to all parties must be accurate and timely.
- In particular, any estimate of the timing to return to normal working operations should be announced with care.
- It is also very important that only authorized personnel deal with media queries.

| Groups of Persons or Organizations Affected by Disruption | Persons Selected To Coordinate Communications to Affected Persons / Organizations | | |
|---|---|---|---|
| | Name | Position | Contact Details |
| Customers | | | |
| Management & Staff | | | |
| Suppliers | | | |
| Media | | | |
| Stakeholders | | | |
| Others | | | |

## Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

## Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

| **Name Of Business Process** | |
|---|---|
| **Completion Date of Work Provided by Business Recovery Team** | |
| **Date of Transition Back to Business Unit Management**<br>*(If different than completion date)* | |

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____

Signature: _____

Date: _____

*(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)*

I confirm that above business process is now acceptable for normal working conditions.

Name: _____

Title: _____

Signature: _____

Date: _____