4Thought Marketing
Disaster Recovery Plan

By Chris Metcalfe, 4Thought Marketing Security Officer

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	08/12/2014	Chris Metcalfe	Original Version
Update 1.1	06/19/2015	Chris Metcalfe	Updated Version
Update 1.2	9/8/2016	Chris Metcalfe	Updated Version
Update 1.3	6/13/2018	Chris Metcalfe	Updated Version

Table of Contents

Statement of Intent

This document delineates our policies and procedures for disaster recovery, both technical and physical, 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 in the process of disaster recovery.
- 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 plan is to develop, test and document a well-structured and easily understood process, 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:

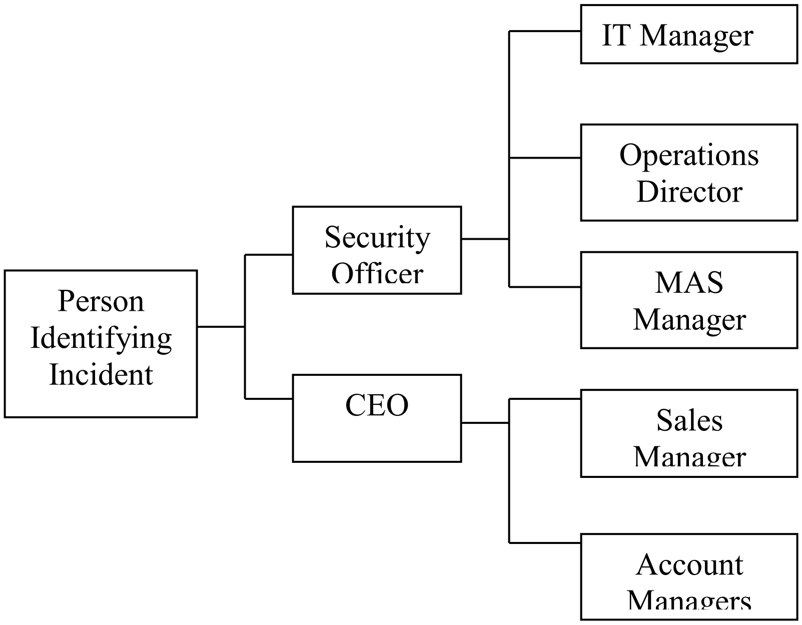
- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications 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
CEO/President	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version
CIO	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version
Security Officer	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version

Name, Title	Contact Option	Contact Number
IT Manager	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version
Operations Director	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version
MAS Manager	Work	Redacted for Public Version
	Alternate	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
	Alternate Email	Redacted for Public Version

Notification Calling Tree

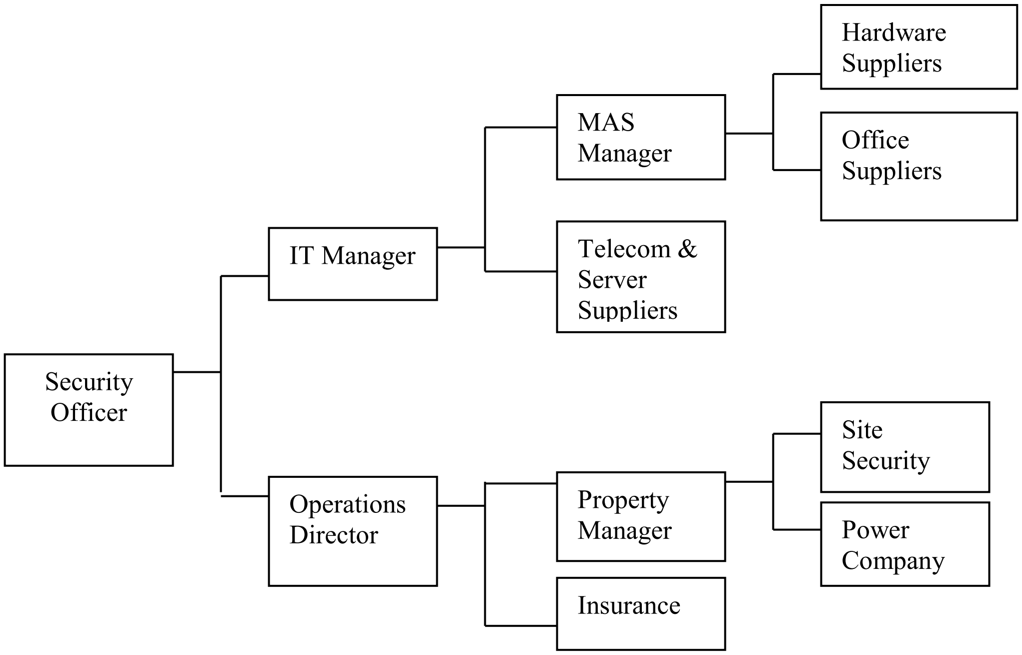


External Contacts

Name, Title	Contact Option	Contact Number
Landlord / Property Manager		
Account Number None		
Redacted for Public Version	Work	Redacted for Public Version
	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
Power Company		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
Telecom Carrier 1		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Fax	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
Telecom Carrier 2		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
Hardware Supplier		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Emergency Reporting	Redacted for Public Version
	Email Address	Redacted for Public Version
Server Supplier		
Account Number.	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Fax	Redacted for Public Version
	Email Address	Redacted for Public Version
Office Supplies 1		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version

Name, Title	Contact Option	Contact Number
Insurance – Name		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version
Site Security –		
Account Number	Work	Redacted for Public Version
Redacted for Public Version	Mobile	Redacted for Public Version
	Home	Redacted for Public Version
	Email Address	Redacted for Public Version

External Contacts Calling Tree



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 Security Officer.

1.2 Plan Documentation Storage

Electronic copies of this plan will be stored in <Path Redacted for Public Version>. Each member of senior management will be sent an electronic copy of this plan to be filed at their office and at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued an electronic copy and hard copy of this plan. A master protected copy will be stored in <Path Redacted for Public Version>.

1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the company's offices in Costa Rica. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Tech Support - Software	Fully mirrored recovery site
Email	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Web Site	Fully mirrored recovery site

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	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	4	3	All critical equipment is located 5 meters (15 feet) above street level. Risk of flood very low.
Fire	3	3	Fire suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Electrical storms	1	5	As electrical storms are common, infrastructure is in place to prevent impact to business system.
Act of sabotage/theft	5	4	Highly unlikely in high security office park. Clean device and clean desk policies will prevent secure data to be lost in an event occurs.
Electrical power failure	2	4	No critical servers located on site. Power back up units will allow for network to continue for short outages. Work from home policy will allow day to day services to continue remotely.
Loss of communications network services	3	4	Two ISP in place to act as back up if one communication network fails.
Seismic Event	3	2	Evacuation and communication plan in place. In the case of a major event, clean device policy will prevent the loss of critical/secure data.
Volcanic Eruption	5	3	Evacuation and communication plan in place. In the case of a major event, clean device policy will prevent the loss of critical/secure data.

Probability: 1=Very High, 5=Very Low

Impact: 1=Total destruction, 5=Minor annoyance

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 – Far end of main parking lot; away from covered parking area
- Alternate – Parking lot of company across the street

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 24.0 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
- “Redacted for Public Version”
- “Redacted for Public Version”
- “Redacted for Public Version”

If not available try:
- “Redacted for Public Version”
- “Redacted for Public Version”

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 hot site at SunGard will be activated and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site as necessary.

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

- “Redacted for Public Version”
- “Redacted for Public Version”

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: “Redacted for Public Version”

Policy Name	Coverage Type	Coverage Period	Amount Of Coverage	Person Responsible For Coverage	Next Renewal Date
“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”
“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”	“Redacted for Public Version”

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 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 representation 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 <System One>

SYSTEM	**“Redacted for Public Version”**

OVERVIEW	
PRODUCTION SERVER	Location: “Redacted for Public Version” Server Model: “Redacted for Public Version” Operating System: “Redacted for Public Version” CPUs: “Redacted for Public Version” Memory: “Redacted for Public Version” Total Disk: “Redacted for Public Version” System Handle: “Redacted for Public Version” System Serial #: “Redacted for Public Version” DNS Entry: “Redacted for Public Version” IP Address: “Redacted for Public Version” Other: “Redacted for Public Version”
HOT SITE SERVER	“Redacted for Public Version”
APPLICATIONS (Use bold for Hot Site)	“Redacted for Public Version”
ASSOCIATED SERVERS	“Redacted for Public Version”

KEY CONTACTS	
Hardware Vendor	“Redacted for Public Version”
System Owners	“Redacted for Public Version”
Database Owner	“Redacted for Public Version”
Application Owners	“Redacted for Public Version”
Software Vendors	“Redacted for Public Version”
Offsite Storage	“Redacted for Public Version”

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	“Redacted for Public Version”
Monthly	“Redacted for Public Version”
Quarterly	“Redacted for Public Version”

SYSTEM ONE DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	“Redacted for Public Version”
Scenario 2 Total Loss of HW	“Redacted for Public Version”

ADDENDUM

CONTACTS	“Redacted for Public Version”
	“Redacted for Public Version”
	“Redacted for Public Version”

File Systems “Redacted for Public Version”

File System as of “Redacted for Public Version” Minimal file systems to be created and restored from backup: “Redacted for Public Version”	**Filesystem kbytes Used Avail %used Mounted on** “Redacted for Public Version”
Other critical files to modify	“Redacted for Public Version”
Necessary directories to create	“Redacted for Public Version”
Critical files to restore	“Redacted for Public Version”
Secondary files to restore	“Redacted for Public Version”
Other files to restore	“Redacted for Public Version”

Disaster Recovery Plan for <System Two>

SYSTEM	**“Redacted for Public Version”**

OVERVIEW	
PRODUCTION SERVER	Location: “Redacted for Public Version” Server Model: “Redacted for Public Version” Operating System: “Redacted for Public Version” CPUs: “Redacted for Public Version” Memory: “Redacted for Public Version” Total Disk: “Redacted for Public Version” System Handle: “Redacted for Public Version” System Serial #: “Redacted for Public Version” DNS Entry: “Redacted for Public Version” IP Address: “Redacted for Public Version” Other: “Redacted for Public Version”
HOT SITE SERVER	“Redacted for Public Version”
APPLICATIONS (Use bold for Hot Site)	“Redacted for Public Version”
ASSOCIATED SERVERS	“Redacted for Public Version”

KEY CONTACTS	
Hardware Vendor	“Redacted for Public Version”
System Owners	“Redacted for Public Version”
Database Owner	“Redacted for Public Version”
Application Owners	“Redacted for Public Version”
Software Vendors	“Redacted for Public Version”
Offsite Storage	“Redacted for Public Version”

BACKUP STRATEGY for SYSTEM TWO	
Daily	“Redacted for Public Version”
Monthly	“Redacted for Public Version”
Quarterly	“Redacted for Public Version”

SYSTEM TWO DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	“Redacted for Public Version”
Scenario 2 Total Loss of HW	“Redacted for Public Version”

ADDENDUM

CONTACTS	“Redacted for Public Version”
	“Redacted for Public Version”

File Systems “Redacted for Public Version”

File System as of “Redacted for Public Version” Minimal file systems to be created and restored from backup: “Redacted for Public Version”	**Filesystem kbytes Used Avail %used Mounted on** “Redacted for Public Version”
Other critical files to modify	“Redacted for Public Version”
Necessary directories to create	“Redacted for Public Version”
Critical files to restore	“Redacted for Public Version”
Secondary files to restore	“Redacted for Public Version”
Other files to restore	“Redacted for Public Version”

Appendix B – Forms

All ERP forms are kept and updated on our Engyte remote system. In the case of emergency all forms are accessible by responsible staff members at the office or at home through this this external storage system as long as a network connection is available.