

Appendix II

IT Disaster Recovery Plan for LTC Language Solutions

Updated: June 11, 2020

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	6/11/20	G. Fernandez & T. Conkright	
2.0			
3.0			

Table of Contents

Information Technology Statement of Intent	4
Policy Statement.....	4
Objectives	4
Key Personnel – Emergency Response Team	5
Notification Calling Tree for incidents affecting more than one client	6
External Contacts	7
1 Plan Overview	8
1.1 Plan Updating.....	8
1.2 Plan Documentation Storage	8
1.3 Backup Strategy	8
1.4 Risk Management	9
2 Emergency Response.....	9
2.1 Alert, Escalation and Plan Invocation	9
2.1.1 Plan Triggering Events	10
2.2 Assembly Point	10
2.3 Emergency Alert	11
2.3.1 Contact with Employees	11
2.3.2 Backup Staff	11
2.3.3 Alternate Recovery Facilities / Hot Site	11
2.3.4 Personnel and Family Notification	11
3 Insurance	11
4 Financial and Legal Issues	12
4.1 Financial Assessment	12
4.2 Financial Requirements	12
4.3 Legal Actions	12

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, adjustments may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data security and integrity, as well as, 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 consider changing circumstances.

Objectives

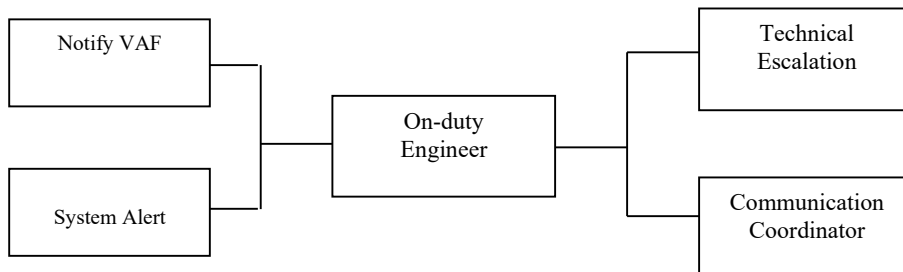
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business 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 – Emergency Response Team

[illegible]

Notification Calling Tree for incidents affecting more than one client



External Contacts

[illegible]

1 Plan Overview

1.1 Plan Updating

It is necessary for the Disaster Recovery Plan 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 Director.

1.2 Plan Documentation Storage

Each member of senior management, plus the IT vendor, will be issued a hard and soft copy of this plan to be filed at home. In addition, each member of the Disaster Recovery Team (as defined in the 'Key Personal -Emergency Response Team' section of this document) will be issued a soft copy of this plan. The master copy will be stored, for editing purposes, in the Director's user files.

1.3 Backup Strategy

IT Operations are maintained at the headquarters. Key business platforms and the backup strategy for each are listed below. The headquarters (LTCHQ) is located at 5750 Castle Creek Parkway, Suite 150, Indianapolis, IN 46250. All primary data is Cloud based, and is replicated throughout Microsoft's multi-site, world-wide operations. The strategy chosen is to mitigate most technical Disaster Recovery needs by utilizing the inherent stability and redundancy of Cloud based solutions where applicable, as detailed below.

Number	KEY BUSINESS PLATFORMS	BACKUP STRATEGY	PRIORITY CODE
1	OneDrive (Cloud)		1
2	O365 (Cloud)		1
3	Exchange Online (Cloud)		1
4	Mitel VoIP (Cloud)		2
5	Salesforce (Cloud)		2
6	Interpreter Intelligence (Cloud)		3
7	LearnSpeed (Cloud)		3
8	FLOW (Cloud)		3
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

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 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
Water Damage	4	Leak from roof or conduit, malfunctioning pipes or systems.
Fire	4	Electrical fire in cabinet or nearby.
Tornado	5	Tornado or wind damage
Electrical storms	1	
Act of terrorism (cyber or other)	3	
Act of sabotage (cyber or other)	3	
Electrical power failure	1	Power problems
Loss of communications network services	2	Local or wide-scale voice or internet issues
Financial solvency of vendor	4	Data center provider or other locks us out

Probability: 1=Very High, 5=Very Low

2 Emergency Response

The IT Vendor's Technical Support Team is responsible for first response to problems with IT systems. Response to IT related problems should follow the following prioritization schedule. As defined in section 1.3, systems with a PRIORITY CODE of 1 will receive resources until all PRIORITY 1 systems are operational. This includes the use of hardware systems previously in use for other operations. Under the most difficult of scenarios, including the loss of the headquarters, the goal is to restore operations in no more than 2 weeks. In addition, the goal will be to obtain limited functionality and emergency access to the servers and data within 24 to 48 hours.

Systems with a PRIORITY CODE of 2 should receive next PRIORITY and those systems should receive resources only after systems with a PRIORITY CODE of 1 are fully operational. A similar procedure should be followed for systems with PRIORITY CODE 3.

2.1 Alert, Escalation and Plan Invocation

Most problems will be detected by a user or a system alert. During business hours, the procedure for users is to notify the call center for a support call to be entered the system. If the system is not available, all staff members should be aware that the policy is to notify the IT Director, and/or other members of the Emergency Response Team as listed in this document.

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. Members of management and a member from Purchasing will serve important roles as quick authorization and procurement of critical components may be necessary for the company to return to normal operating mode.

In the event of an emergency, the following steps should be executed:

1. Located and deploy key technical personnel and determine the immediate plan of action;
2. Determine plan for notifying clients and managers;
3. Locate this document;
4. Open a conference call for key personnel to connect into;
5. Respond immediately to a potential disaster and call emergency services;
6. Assess the extent of the disaster and its impact on the business, data center, etc.;
7. Decide which elements of the DR Plan should be activated;
8. Establish and manage disaster recovery team to maintain vital services and return to normal operation;
9. Gather equipment and software required and determine a 'needs' list;
10. Ensure employees are notified and allocate responsibilities and activities as required.

Recovery Timeline

Establish priority 1 and priority 2 platforms within 24 hours;

Establish additional high priority platforms, for an emergency level of service, within 24 to 48 hours;

Restore key services within 2 weeks of the incident;

Recover to business as usual within 4 weeks after the incident;

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
- Water damage of the premises
- Loss of the building

2.2 Assembly Point

Where the LTC premises need to be evacuated, the DRP invocation plan identifies an evacuation assembly point: Main Lobby – TBD

2.3 Emergency Alert

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

Emergency Response Team

- Martin George

If not available try:

- Sadie Clark

2.3.1 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.

The receptionist oversees maintaining and distributing a laminated contact card with Manager Extensions, home phone numbers and mobile numbers. This card is to be updated and distributed annually. Managers should always carry their laminated contact list card with them.

2.3.2 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.

2.3.3 Alternate Recovery Facilities / Hot Site

No Facilities exist currently.

2.3.4 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 Insurance

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

If insurance-related assistance is required following an emergency out of normal business hours, please contact: Martin George or Sadie Clark.

4 Financial and Legal Issues

4.1 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

4.2 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

4.3 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; the possibility of claims by or against the company for regulatory violations, etc.