EVACUATION AND DISASTER RECOVERY PLANS

This document sets out our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure.

1. Emergency Evacuation of the Premises

Where the premises need to be evacuated, we have fire wardens nominated and all employees are required to follow that person's direction. The evacuation plan will identify the evacuation assembly point. Fire wardens would be easily spotted during an emergency as they will be wearing a hard hat and red vest kept at the office.

2. Disaster Recovery Plan (DRP)

The objective is to ensure information system uptime, data integrity and availability, and business continuity. We will ensure that key staff members are made aware of the disaster recovery plan and their own respective roles and that the disaster recovery plan is to be kept up to date and reviewed each year as part of our annual Compliance Plan review.

3. Safekeeping and Access to the DRP

This plan is to be uploaded to the secure section of our website where it can be accessed by any staff member using their login. This server is hosted in the cloud. In addition to this, a hard copy of the plan will be held by the Responsible Manager at their home as well as a hard copy in a secure location in the office.

4. Server Backup Strategy

Our systems are backed up in the cloud via Amazon web services. The system and database are backed up daily. All folders and subfolders are backed up automatically.

5. What Triggers the Disaster Recovery Plan (DRP)?

The disaster recovery plan describes what action we will take given a certain set of circumstances and who is responsible for managing the DRP.

We have categorized events into two major sections. The first is Category A and is for major disasters that would take a long time to recover from and have a major effect on the

business, while category B would be for events that have a lower impact on the business and may only affect a small part of our operations or last less than one day.

Category A - Critical

- Total loss of power
- Flooding of the premises
- Loss of the building
- Fire
- Act of terrorism

Category B - Moderate

- Total loss of all communications
- Evacuation of the building
- Bomb Scare
- Break and Enter

6. Notification of An Incident

When an incident occurs, the person who has identified the issue should immediately refer the incident to any one of the Internal DRP (IDRP) contacts and any one of these people are authorised to decide to what extent any DRP must be invoked.

7. Responsibilities of the IDRP

- Respond immediately to the incident and if required call emergency services (000) and ensure staff safety
- Assess the extent of the disaster and its impact on the business, data centre, etc.;
- Decide which elements of the DRP should be activated;
- Establish and manage employees to maintain vital services and return to normal operation;
- Ensure employees are notified and allocated responsibilities and activities as required.

8. IDRP Team Objectives

The team will be contacted, and their 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 hours after the incident;
- Communicate with staff, affected clients, referrers and other business partners
- Coordinate activities with disaster recovery team, first responders, etc.

9. Emergency Alert, Escalation and DRP Activation

The IDRP 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.

10. 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.

11. Contact with our Borrowers

The IDRP will act to notify customers that are affected by the incident, if the incident is likely to affect them for a period of more than 24 hours. This will include:

- Asking our website hosting company to make an announcement on our website
- Sending an email to all customers and referrers who have subscribed to our email database
- Asking employees to call customers who have lodged an application that has not settled but is in process (this data may need be recovered from their calendars or server backup, or mobile phone)
- Ask our telephone provider to divert calls to another number or to a call centre

12. Updates

For the latest information on the disaster and the company's response, staff members can call their reporting line manager for information on the nature of the disaster, assembly sites, and updates on work resumption.

13. Work Continuation

If necessary, employees will work from home and continue business as usual until the office premises is re-established. Our daily business processes are conducted via web-based applications, which all employees can access by using their secure usernames and passwords.

14. 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.

15. Media Contact

Only a Director is to coordinate with the media in the event of a disaster.

16. Insurance

As part of the company's disaster recovery and business continuity strategies, insurance policies have been put in place. These include workers compensation, contents insurance and business interruption.

17. Disaster and Action Checklist

1. Plan Initiation

- ✓ Notify senior management
- ✓ Contact and setup disaster recovery team
- ✓ Determine degree of disaster
- ✓ Implement proper application recovery plan dependent on extent of disaster
- ✓ Monitor progress
- ✓ Contact all necessary personnel both user and data processing and establish schedules
- ✓ Contact vendors--both hardware and software
- ✓ Notify users of the disruption of service

2. Follow-Up Checklist

- ✓ Review the entire DRP
- ✓ List teams and tasks of each

- ✓ Create temporary office if required
- ✓ List all personnel and their telephone numbers
- ✓ Establish user participation plan
- ✓ Set up the delivery and the receipt of mail
- ✓ Rent or purchase equipment, as needed
- ✓ Determine applications to be run and in what sequence
- ✓ Identify number of workstations needed
- ✓ Check out any off-line equipment needs for each application
- ✓ Check on forms needed for each application
- ✓ Set up primary vendors for assistance with problems incurred during emergency
- ✓ Check for additional magnetic tapes, if required
- ✓ Take copies of system and operational documentation and procedural manuals
- ✓ Ensure that all personnel involved know their tasks
- ✓ Notify insurance companies

18. Financial and Legal Considerations

18.1 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 cheque books, credit cards, etc.
- Loss of cash
- Loss of client's files and personal information

18.2 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, commissions, taxes, etc.
- Availability of credit cards to pay for supplies and services required post disaster
- Insurance policy claims

18.3 Legal Actions

The company management will review the aftermath of the incident and take advice on whether there may be legal actions resulting from the event; the possibility of claims by or against the company for regulatory violations, etc.