Disaster Recovery Policy

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

- ProEarth 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
Nick Addison, CEO	Work	01273 467 607
	Mobile	07730 803876
	Home	01903 40074
	Email Address	nick.addison@pro-earth.co.uk
	Alternate Email	nick.addison@outlook.com
Alex Addison, Director	Work	01273 467 607
	Mobile	07961 336895
	Home	01903 410074
	Email Address	alex.addison@pro-earth.co.uk
	Alternate Email	alexandraaddison@outlook.com

External Contacts

Name, Title	Contact Option	Contact Number
Landlord / Property Manager		
Serviced offices providing all services		
BasePoint Business Centre	Work	01273 467600
Little High Street	Mobile	-
Shoreham-by-Sea	Home	-
BN43 5EG	Email Address	amanda.jones@basepoint.co.uk
Gresham Insurance		
Policy Number GIB164032	Work	01903 211462
Site Security – NOD32 Antivirus 9		
Account Number	Work	07968 423692
Off-Site Storage 1 – Dropbox Business		
	User ID	alex.addison@pro-earth.co.uk
	Password	Tottenh@m0
Off-Site Storage 2 – Knowhow Cloud		
	User ID	alex.addison@pro-earth.co.uk
	Password	LillyM@y22

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 formalised 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 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 for a fully mirrored recovery site at the company's offices in Shoreham-by-Sea. 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
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Purchasing	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
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	5	5	All critical equipment is located on 2nd Floor
Fire	4	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

1.5 Alert, escalation and plan invocation

1.5.1 Plan Triggering Events

Key trigger issues 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

1.5.2 Assembly Points

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

- Primary – car parking outside back of building

1.5.3 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.

1.6 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.

1.7 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.

Emergency Alert

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

Emergency Response Team

• Nick Addison

If not available try:

- Alex Addison

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.

2 Financial and Legal Issues

2.1 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

2.2 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, NI etc.

3 Availability of company credit cards to pay for supplies and services required post-disaster

4 DRP Exercises

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.