FOVEAL LLP

BUSINESS CONTINGENCY PLAN

This business contingency and IT security plan presents an orderly course of action for managing and, in the event of failure, restoring critical computing capability to Foveal LLP ("the Firm").

OVERVIEW:

Business Description

Foveal LLP is owned by Amit Roy and Puspa Roy. The role of the Firm is to carry out pharmaceutical research and advise investors within this industry. The Firm's services are directed at professional investors.

Firm Policy

The Firm's IT security and disaster recovery policy is designed to respond to a Significant Business Disruption ("SBD") by safeguarding employees' lives and Firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the Firm's books and records, and allowing the Firm's customers to transact business. In the event that the Firm determines that it is unable to continue its business, the Partners and employees of the Firm will be able to continue business via remote access.

Procedure for dealing with SBD

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. The Firm's emergency contact person is: **Amit Roy** (tel: +44 20 3637 1007 email: amit@foveal.uk). This name will be updated in the event of a material change.

1) Data Back-Up and Recovery

Salvage Operations at Disaster Site

Early efforts will be targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, diskettes) will be identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site
At the same time, a survey of the disaster scene will be carried out by the appropriate personnel to estimate the amount of time required to restore the Firm to functionality. Work will begin almost immediately at repairing or rebuilding the site. This work may extend to a number of months, the details of which are beyond the scope of this document.

Purchase New Equipment
The security and recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. Orders for equipment, supplies, software, and any other needs will be placed as quickly as possible.

Begin Reassembly at Recovery Site
Salvaged and new components will be assembled and, once the equipment reassembly phase has been completed, work will focus on the data recovery procedures.

Restore Data from Backups
Data backup media will be recalled from off-site storage to enable data recovery to take place. Data recovery relies entirely upon the use of backups. Early data recovery efforts will focus on restoring the operating system(s) for each computer system. Subsequently, first line recovery of application and user data from the backup tapes will be undertaken.

2) Communication with third parties

In the event of a SBD, the Firm will immediately identify the means that will permit it to communicate with its customers, employees, critical business constituents, critical banks, critical counter-parties, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options the Firm will employ will include letter, fax, telephone voice mail, mobile phone and/or secure e-mail.

Preventative measures taken to mitigate the threat of Significant Business Disruptions ("SBD"s)

Foveal LLP's plan anticipates two types of SBD - internal and external. Internal SBDs affect only the Firm's ability to communicate and do business, such as a fire in its building. External SBDs prevent the operation of the markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption. The Firm's response to an external SBD relies more heavily on other organizations and systems.

Fire:

In order to prevent and detect fire a number of provisions have been made:

- The building is equipped with a fire alarm system, with ceiling-mounted smoke detectors dispersed throughout the building.
- Hand-held fire extinguishers are in place in visible locations throughout the building.
- Staff members are required to undergo training on the proper actions to take in the event of a fire.
- Staff members are required to demonstrate proficiency in periodic, unscheduled fire drills.

Computer Crime:

Computer crime is becoming more of a threat as systems become more complex and access more highly distributed. The onset of new networking technologies means that there is greater potential for improper access than previously. Consequently, all systems have security products installed to protect against unauthorised entry. All systems are protected by username and passwords, especially those permitting updates to data. All users are required to change their passwords on a regular basis. Invalid access attempts to systems are monitored through systems logs.

All systems are backed up on a daily basis.

Theft

The maintenance of good building physical security is highly important. All files and laptops are locked away at the end of each day. All visitors are signed both in and out of the building.

Backups

All company data, files and emails are stored on the central network fileserver. This fileserver is backed up on a regular cycle. The backup cycle allows for the retrieval of files. The back up system backs up all user data saved onto the file server, the exchange store as a whole, and exchange store as individual mailboxes; consequently, the entire email database can be restored in the event of a failure, or a single email can be restored if deleted in error. The system also backs up critical server data so that the server itself can be restored to a comparable working state in the event of failure.

There is no duplicate physical version of the system maintained off site. However, the Firm's Partners have remote access to all its systems and servers through an offsite internet connection through a laptop or PC. Thus, should physical access not be possible for any reason, this is unlikely to result in data/systems issues.

Plan Location and Access

Foveal LLP will maintain copies of its BCP, the annual reviews and the changes that have been made to it for inspection. A copy of the plan can be found at the Firm's registered office in London.

Updates and Annual Review

Foveal LLP will update this plan whenever there is a material change to its operations, structure, business or location or to those of its clearing firm. In addition, the Firm will review this BCP annually to modify it for any changes in the Firm's operations, structure, business or location.