Cibus Capital LLP

Disaster Recovery Policy

LEGAL DISCLAIMER. PLEASE READ BEFORE CONTINUING:

This document is confidential, provided for informational purposes only and is not legally binding on Cibus Capital LLP ('Cibus') or any of its affiliates.

None of Cibus or any of its affiliates accept responsibility to any third person in connection with, and no third person shall have any right to enforce, any performance or non-performance of any of the provisions of this document.

This document relates to Cibus Capital LLP's current operations as of 24 November 2022 but is liable to change at any time without notice.

24 November 2022

Scope

This Disaster Recovery/Business Continuity Plan prepares for continuation of Cibus' business in the event of calamities such as (natural) disasters, terrorist attacks and failures of infrastructure. This document is available as a separate document.

Background

The nature of Cibus' business is such that its Disaster Recovery Plan centres on confidentiality of data and making necessary files available to staff at all times so that they can carry out their roles efficiently, rather than making provision for the replication of parallel computing facilities. The following provisions look to ensure that any lost data can be recovered in a complete form within a relatively short period of time.

The relevant Fund Administrator (Vistra Guernsey or IQEQ) keeps the prime records of all the Cibus funds as well as the underlying investors know-your-customer ("KYC") and identification information, as well as details of all investments (including evidence of securities, original legal documents and all other documentation). In the event of a disaster at Cibus Capital, there will be no impact on the Cibus funds daily functioning.

Administrators are responsible for storing, protection and archiving portfolio company and fund data, share certificates, books and records of the fund for a minimum of seven years.

The rest of this DRP note centres on Cibus Capital's data, which is backed up and available in a variety of ways:

Cibus, in its role as Investment Adviser to the Cibus funds conducts a full offsite backup using Datto backup software, of all files and data including email, investment data and administrative files. Datto enables a full restoration of data to be performed quickly and with minimal data loss. All laptops are synced to cloud-based file storage on OneDrive.

There are three key systems used.

Email: Cibus' email is run on the Microsoft Office 365 service. Primary copies of mailboxes are held in UK data farms but if those are compromised then there is a secondary back-up location (for redundancy) in Europe; all managed and maintained by Microsoft. These mailboxes are available 24/7 on all the following platforms:

Microsoft Office web portal; desktop email software (primarily Microsoft Outlook) and on users' smartphones and tablets. The mailboxes are resilient, with full data recovery and redundancy but in addition to this, Cibus maintains a daily cloud backup of every user's mailbox using a secure cloud service called Datto Backupify. This is done entirely in the cloud directly from Office 365 and allows the restoration of individual emails or an entire email box. Microsoft Office 365 offers full online availability and issue reporting and logging.

OneDrive: Cibus staff are all set up with a Microsoft Office 365, E5 license that includes OneDrive as a cloud-based storage system for their files. The office laptops that have been issued to all staff members have been set up in such a way that saved files automatically sync with OneDrive which are then securely stored on the cloud and are accessible through the Office 365 portal. There are no on site, Cibus owned servers.

Archives: All email files are stored on the cloud for seven years. All Cibus' email files are archived in the cloud and stored in a UK data centre with redundancy in Europe per regulatory requirements.

1. All staff members have remote access to the Office 365 portal. Key members of staff also have administrator permissions on the portal in case the need to restore lost files ever occurs.

2. In the event of a disaster resulting in lack of access to office premises, all data can be recovered by remote access from offsite workplaces or temporary offices.

In the event of a disaster in London, staff will temporarily operate either from their homes or from the house of Mr Robert Appleby in London and/or the house of Mr Jeremy Alun-Jones in Sussex. During the Covid-19 crisis, all members of staff were required to work from home and communicate daily through Microsoft Teams, email and telephone calls so these procedures have been tested and found to function adequately for Cibus' business needs.

Non-UK Staff:

For those staff members who are consultants that operate from a permanent address outside the UK, following the announcement of a localised or nationwide evacuation or emergency in these countries, staff are primarily advised to seek safety at all costs. Once it has been established which travel options are available, Cibus will make arrangements for affected staff to travel to a nearby safe office location or to the London Headquarters of Cibus or the offices of Asia Debt Management Hong Kong, whichever is more appropriate. Accommodation will be arranged by UK based Cibus support staff as necessary in the final destination.

The aim of the above procedures is to be fully functional within 24 hours of a disaster with zero loss of key administrative data.

Disaster Recovery Group

Cibus has formed a Disaster Recovery group which should be contacted in the event of any Disaster comprising:

London Office:

Jeremy Alun-Jones	mobile: +447775505152	email: jeremy.alunjones@cibuscap.com
Annie Rainsford	mobile: +44 7901853108	email: annie.rainsford@cibuscap.com

UK Technical Consultants:

James Buist	mobile: +44-742-707-1597	email: james.buist@admcap.com
Simon Pardo	mobile: +44-799-057-3707	email: simon@computerc.co.uk

All staff should contact either Jeremy Alun-Jones or Annie Rainsford in the event of any disaster situation or other emergency while at work.

Actions – Cibus Capital LLP

1. If appropriate, Jeremy Alun-Jones (or as applicable senior staff in the vicinity of the disaster) to notify the Police/Fire/Ambulance service.

2. Susie Harrison to notify HSBC of Disaster occurrence and plan accordingly. Jeremy Alun-Jones to notify fund administrators to discuss retrieving all relevant administrative data from them as well as other service providers.

3. Annie Rainsford to notify applicable regulatory body if relevant – Financial Conduct Authority.

4. Fred Appleby to notify Cibus' IT Consultants and arrange transfer of offsite data to PCs in the temporary offices. Cibus' IT Consultants to assist in procuring additional IT hardware as necessary.

5. All staff to carry their mobile phones at all times.

6. Staff must inform Jeremy Alun-Jones or Annie Rainsford of their location within 24 hours of a disaster.

7. Jeremy Alun-Jones will negotiate longer-term office space if required.

8. Cibus' IT consultants to arrange additional PC and communications support in the temporary space as necessary. The alternative offices will be equipped with broadband and secure wireless networking. Remote access to main office computers to be connected if those computers are still operational.

9. Susie Harrison to arrange collection/diversion of post.

10. The Investor Relations Team to contact all existing investors and update them on the office status.

11. Susie Harrison and Jeremy Alun-Jones to contact service providers with details of Cibus' temporary arrangements.

12. Jeremy Alun-Jones to determine the status of main office on an on-going basis to decide on longer-term arrangements, if necessary.

13. Susie Harrison to request phone companies to forward all voice calls from fixed lines in the old premises to new fixed lines/mobile phones.

14. Jeremy Alun-Jones to organise a visit (if possible) the London main office in order to gather essential information and documents as necessary.