Business Continuity Plan

Money Gap Group Limited trading as CashLady

For year ending 2016

1. **About us -**
   Money Gap Group Limited trading as CashLady

   We are located at Spectrum House, Dunstable Road, Redbourn, St Albans, AL3 7PR. at Spectrum House is a fully serviced office.

   At the offices documents are received and scanned electronically. Documents are then posted to our repository.

   The premises have a security system in place and fire protection systems.

2. **Strategy**

   Our business continuity plan relies on making sure the business is resumes as quickly as possible using standard implementation and mitigation procedures where possible. We use leading infrastructure suppliers with backup facilities for all business critical processes. This includes all communication forms (e.g. telephone, email), document storage, reporting systems, financial software and fully managed offsite servers.

3. **Personnel**

[Information Stored Offline]

4. **Records**

   The firm's records are mainly electronically stored.

   - Paper-based – all paperwork is scanned and stored electronically
   - Paper-based files are received in the office, scanned and forwarded electronically. We operate a clear desk policy.
   - Once scanned, everything promotional is shredded. All company related documents, including all documents bearing an original signature, e.g. client compliance questionnaire, terms of business and bank and credit card statements are kept in a secure location. Then these documents collated and sent a central storing location.
   - Documents are shared electronically using a central password protected, user specific, company drop box folder.

5. **Systems**

   Client data is maintained on Rackspace systems (with Rackspace Hosting) on a Failsafe SQL Database cluster behind a dedicated cisco hardware firewall.
   We use Outlook for emails.
   Google Chrome or Internet Explorer for web browsing
   Dropbox Pro/Business is used to store and share files internally.

6. Business Continuity Risk Assessment

Risk Event	Impact	Mitigation
Loss of access to premises e.g. fire or flood	Difficulty in completing work. Clients not able to visit. Potential loss of business.	Fire precautions/alarm system fitted to premises. Work from home opportunities. Infrastructure in the cloud or hosted in a safe data centre.
Failure of IT system	Inability to access client data, accounting records, failure of web services – loss of business	Use of data backup facilities, maintenance contract with system supplier. Infrastructure hosted in a safe data centre.
Computer Virus	Corruption or loss of business records. Disruption to ongoing business and client contacts	Computers fitted with anti-virus systems that are regularly updated (Avast)
Loss of telephone service	Inability of clients/regulator/compliancy services to contact the firm	Back up arrangement to forward calls to mobile or alternative number i.e. home telephone
Theft of IT equipment	Loss of operations data, causing difficulty in completing work and risk of being unable to demonstrate compliance with FCA rules where this information is stored locally Possible Data Protection consequences	Security measures – use of back up facilities etc. Central protected shared storage for documents.
Damage to or loss of paper records e.g. flood damage	Loss of client data, causing difficulty in completing cases in progress and risk of being unable to demonstrate compliance with FCA rules	Scanned copies held electronically in a central shared location and backed up.
Explosion due to Terrorists Acts	• Loss of premises • Loss of client data/business records • Loss of business	• Copy records obtained • Work from home in the short term • Arrange new premises
Loss of Key personnel	Loss of knowledge, man power and control of the company	The other key stakeholders will assume responsibility and recruit additional and sufficient man power. Knowledge transfer will take place with the remaining stakeholders.

7. **Key Personnel**

The Key Individuals are the directors and operations manager.

The process to be followed will be:
Operations manager to telephone those affected (e.g. clients to reschedule/relocate appointments)
Operations Manager will inform product providers
Company Director will inform FCA, if appropriate
Operations Manager will activate contingency plan
Any other relevant activity

8. **Review and Testing**

Company Operations Manager is responsible for the maintenance of this plan, a copy of the plan is held in the Compliance folder and relevant individuals will have access to a copy off site. The policy for testing the appropriateness or availability of contingency plans will be reviewed annually.

9. **Sign Off**

This Business Continuity Plan is signed off by the Directors. It is noted that this plan will be reviewed on an annual basis, however should any substantial changes occur in between times, then an amendment to the plan will be attached and signed off.

Date:
15/03/2016