
BUSINESS CONTINUITY POLICY

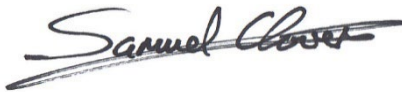
Prepared on: 18 February 2019

Last Review: 19 March 2024

To be reviewed on: 31 March 2025

Prepared by: Ralph Elliott-King – Financial Controller

Reviewed and accepted on behalf of Marisco South Ltd and Marisco Electricals Ltd (the Company) by:



On: 19 March 2024

Samuel Clover - Director

Introduction

Any number of unforeseen events can adversely affect the ability of a business to continue operating as usual. Many businesses fail within a matter of months following the loss of a head office and all its contents through vandalism, fire or flood. A business that depends on mission-critical and continuing access to telephone and Internet networks can quickly grind to a complete halt if the service is lost or unauthorised entry allows the system to be compromised. Ransomware attacks always remain an issue for businesses that rely heavily on electronic storage of data. The sudden loss of key personal through illness or death can have unforeseen adverse consequences for a business through the sudden loss of their day-to-day contribution to the running of the business.

Marisco has implemented a continuity and recovery plan that will allow it to continue operating without any significant disruption of its service in the event of one or more of the above events.

Contingency Planning for the Unforeseen Loss of our Operational Head Office and/or Services:

Our permanent office staff is less than 10 people and can work from home with portable PCs just as effectively as they would be required to work in an office. Most of our field operatives travel directly to remote work sites that are only active for short periods of time measured in days to a few weeks. The loss of the physical use of our office base at Unit J5 would be inconvenient, but not catastrophic in terms of maintaining the day-to-day operation of the business.

Dependency on Internet and IT services

Marisco is heavily dependent on the electronic storage of all our administrative and operational systems, including client and supplier contact and transactional data. Every manager should ideally have a functioning broadband service to enjoy convenient access to the Company's services and stored data (Marisco One-Drive).

The critical IT service software and operational data is mainly cloud-based and stored in secure and backed-up locations, with reputable IT support companies that offer assured multiple redundancy options to protect the integrity and access of that software and operational data in the event of the loss of service at one or more nodes.

Furthermore, managers each take home their own laptops each day and are reminded to take personal responsibility for taking multiple and regular backups of their essential software systems and data to protect against the loss of the centrally stored systems.

The critical Systems Marisco depends upon include:

- Cloud Sage Line 50 – Data backed up at three separate remote locations.
- Our payroll software – Data backed up at two separate remote locations.
- Office 365 – Managed and backed up by SPC-IT (independent and retained IT specialist) and stored on multiple laptop PCs.
- We use a Cloud based Telephone system that can easily be switched to work on any number of locations with a broadband connection – Supported by multiple mobile telephone accounts that could serve as temporary conduits for operational telephone calls if needed.

Our IT Office 365 cloud access and email services are managed off-site by SPC-IT, which will assist us 24-7 with any changes to our operational base in the event of the loss of Unit J5.

Although the loss of our day-to-day transactional paperwork would cause some inevitable inconvenience, many physical copies of key documents (HMRC, insurance, property and vehicle leases, sales invoices, contracts, etc.) also exist in electronic format and are stored in the Cloud.

Our director and key business managers already carry their 'electronic office' on a set of Cloud-connected and secure Microsoft Surface PCs as a contingency against the unexpected loss of the head office and its content.

We have immediate access to a sufficient continuity contingency fund that would allow us to cover the cost of buying the new office furniture and IT equipment we might need to establish a new office either at the original site or a new office in the area.

Contingency Planning for the loss of Key Personnel

Provisions have been made to ensure that the critical tasks carried out by our individual senior managers that allow our business to continue operating on a day-to-day basis have all been identified and could be taken over by another person in the event of a sudden and unplanned loss of one of their contribution for any reason.

The planned contingencies for the sudden loss of a key manager include:

- All senior managers are required to update a secure and shared, password-protected data vault stored on our Office 365 Cloud system, with important passwords and access information about the business services they are responsible for.
- All our bank accounts have multiple authorities to avoid the loss of access to those bank accounts if one authority-holder should be lost for any reason.

- In the event of a sudden loss of one of our senior managers, their immediate commitments and appointments would be reviewed and reassigned to ensure they are responsibly managed to a satisfactory conclusion.
- Although we have the capacity and shared knowledge to temporarily absorb the extra workload caused by the sudden loss of any of our senior managers, the nature of our business means we would not anticipate any difficulty searching for and finding a suitable replacement to fill the vacated role.

Our internal procedures are reviewed regularly and published on our www.mariscosouth.co.uk website.

This policy is posted on the Company Notice Board and references are made to it in the staff handbook.

Contact for IT:

support@spcit.co.uk

01202 935593

Contact for telephone system:

support@juicebroadband.freshdesk.com

01202 332331