Business Continuity and Disaster Recovery Plan

Company Policy No: 58
Company: Mayday Healthcare Ltd
Issue No: 5
Revision Date: April 2026
Review Date: April 2027

Business Continuity and Disaster Recovery Plan

Policy Statement

The Managing Director is responsible for ensuring that disaster recovery plans are in place for all systems. He will direct risk assessments and provide a suitable response to the issues of business continuity.

Objectives & Scope

To ensure the effective availability of our services, we have anticipated the key areas of risk and provided instructions regarding what to do if they occur with a view to ensuring continuity of our services and minimum disruption for clients and candidates.

Our Business Continuity Policy is designed to ensure that key staff know what to do in the event of a disaster or issue which could impact our ability to deliver our recruitment services. It is reviewed and updated at least annually and in light of any changes in circumstances to ensure we are ready to respond quickly and effectively to maintain safety and minimise business disruption.

Key Contacts

In the event of a disaster or business continuity issue, the first port of call should be the Office Manager. If they are not available, you should contact relevant people on this list:

Job Title	Name	Telephone	Area of Responsibility
Office Manager	Mary O'Reilly	07825 174704	Offices and Facilities
Managing Director	Christopher Coyle	07958 660074	The business as a whole.
Operations Director	Ashling Coyle	07796 301738	Business Operations
IT Director	Gursewak Dusanjh	07718 658389	IT and Telecoms Systems

Total Power Failure

In the event of a total power failure, you should:

- Report the issue to the Office Manager using the contact details provided above.
- Establish with the building landlord/power supplier how long the power is anticipated to be off for.
- If the power is to be off for more than 2 hours, staff will be instructed to either work from home or go to one of our other offices as an alternate location.

As all our business systems are Cloud-based, IT and communications will not be affected by any form of power outage. All staff are provided with company laptops and mobile phones to enable working from home. Everyone is set up on Microsoft Teams which aids collaboration by providing additional messaging and video conferencing capabilities.

Virus Protection

We have taken the following precautions to prevent viruses, trojans and malware from infecting our systems:

All systems within the organisation have a form of antivirus software installed on them which is set to proactively update and scan systems when required.

For all backend (servers) and frontend systems (end-user devices), Falcon Crowdstrike software is deployed and set to update when new update packages containing virus definitions are released.

Falcon Crowdstrike is set to actively scan and use machine learning to pick up abnormal functions being carried out as well as look for security threats which could potentially be damaging. This is monitored by the internal IT team as well as the software vendors who run a 24-hour proactive monitoring service for real time protection.

Access to the web-based Falcon Crowdstrike dashboard is only accessible by selected members of the IT Team, and authentication uses a 2FA system which requires a code to be entered that changes every 30 seconds.

The firewalls which are positioned within the organisation are set to only allow access which is required and to block ports or functions which are not needed. Senior members of the internal IT Team monitor IT news channels to look for new threats and find ways to mitigate these threats using the firewalls. This could include, but is not limited to, disabling certain ports, or blocking access to sites which could potentially pose a threat.

The IT team is available 24-hours a day and actively monitor threats. Email alerts are set up to alert the IT team of any security breaches; if any notifications are set out, the IT team is to respond as quickly as possible.

If it becomes apparent that a virus or similar has infected an end-user's device on the network, users are instructed to carry out the below steps as the IT Team ringfence the device using Falcon Crowdstrike.

- Disconnect the device from the office network/internet
- Notify the IT team via phone
- Do not use your laptop until advised otherwise
- Log down what you did last before the notification was released about a virus/malware infection

Due to all our systems being hosted in various locations across the Cloud infrastructure, our IT team can swiftly switch to alternate hosting environments. Enabling us to seamlessly continue servicing our clients.

Back Ups and Cloud Based Systems

The security of our client and candidate data is critical to our business and as such we operate a robust system to prevent loss of such data.

The core systems are configured in a hybrid model with the CRM, documents and some core services such as our financial systems being Cloud based; other systems such as our domain controllers are virtual systems located in the head office and in the cloud in a hybrid set up.

The backup solution for the hybrid solution is all Cloud based and runs-on Azure, either using a backup subscription called Backup Simple from SoftwareOne or the built-in backup with Azure itself.

For systems located in head office, backup agents are installed on all virtual systems which then connects into the Cloud backup solution to run backups. Incremental backups are run every weeknight from 11pm onwards with full backups taking place every Saturday at 11pm.

Backups are stored for a length of time which varies from 30 days to 1 year depending on the system being backed up. The restores for these backups can be done in various ways.

- Full backups require a host which is connected to the domain; this allows a full restore of the system to take place
- Partial restore allows up to restore partial parts of a system, this includes full hard drives or folders
- File restores allow specific files to be chosen and restored when required

The type of restore required will determine the length of time it will take as well as the required bandwidth. Tests have shown the full restore of the financial systems can take between 8-16 hours due to the immense size of it.

Other systems which are located on the Azure platform have full server snapshots being taken as well as backups. Snapshots can be restored nearly instantaneously for a period up to 5 days; anything outside of this will depend on the size of the system being restored.

The CRM system runs in a similar fashion with incremental backups taking place each night followed by a full back up during the weekend. Additional smaller database backups are carried out throughout the day to ensure up to date data is kept. Once again, the restore for this will be in the same manner and can be restored as a full system, partial system, or file recovery.

SoftwareOne are the providers of the Backup Simple solution which is hosted on the company's Azure platform. The solution is not connected to the domain and uses backup agents installed on our systems to connect and back them up.

The Backup Simple solution is GDPR compliant and even though the vendor has access to the backups, they will not be able to access the physical data on the backups as their infrastructure is not domain authenticated. Any work being carried out goes through a change management process and limited access is granted to the system.

The Backup Simple solution has been put through rigorous testing to ensure the below:

- The data contained in the backup is viable
- The backups do not lose integrity and can be restored
- Restore times match with what the business expects.
- The backups are secure and only accessible using pre-defined accounts which have 2FA (2 Factor Authentication) enabled on them

Network Resilience & Servers

For resilience of systems, all core services are placed on the Azure Platform with limited reliance on any single office. The main purpose of the systems being on the cloud platform is to ensure that there is always high availability of the services if something was to happen to an office.

Backups are regularly checked, and all servers are enabled with a 5-day snapshot which reduces recovery time. We have checked the process of recovering servers several times all with great success.

Recovery time is dependent on the size of the server with smaller servers taking less time to recover compared to larger servers.

All CRM functionality is placed on a Cloud platform with minimal access so it is not affected by any systems located in offices which could be compromised. All documentation is located on Microsoft SharePoint Online and is backed up online. Version History is activated so it can be easily restored if required with more in-depth backups available if required.

All server hardware has a service level agreement attached, which means they will be repaired within 24 hours if a fault is found. The internal IT team aim to have the systems restored as quickly as possible and work around the clock to ensure this.

All Cloud-based systems, which usually would require domain authentication to connect to via the VPN, are temporarily opened so they can be accessed by a wider variety of external IP addresses.

The network firewalls are also configured in a High Availability cluster, meaning, if the primary firewall were to fail, the secondary would turn active automatically restoring network functionality.

All remote offices are connected into the Cloud systems and are not reliant on any single office-based system – as long as there is an internet connection in the offices; they will be able to authenticate to the domain and function normally.

BACS/Payroll/Invoicing Failure

Our in-house payroll runs every week – processing both paper and electronic timesheets using Access Dimensions and Select Pay PAYE software. This process generates the invoices automatically.

Should the main office become inoperable, staff can access the system from any one of our other offices or from home – ensuring any disruption to the payroll and invoicing process is kept to an absolute minimum.

Paper timesheets are scanned and stored electronically on InVu. This is backed up incrementally daily with full backups every Saturday. Original timesheets are attached to any invoices that are sent out.

All payments are made via BACS. In the event of a BACS system failure, workers can be paid via individual manual same-day payments, instead.

All payroll and invoicing data is held on our SQL server, which is backed up incrementally daily with full backups every Saturday. These are then stored in the cloud which is based on an Azure platform and carried out by Backup Simple as mentioned in the Backup Section of this document.

Telephone Systems

Our phone system is Microsoft Teans. This is a Cloud based system and enables all users to be able to receive calls wherever they are logged in – as well as diverting calls to mobiles in the event of an emergency. The system can also be accessed remotely should there be a fault in any of our buildings.

The core Microsoft Teams product is covered by the Microsoft themselves and we can reach out to them to log any faults we may face. The lines are provided by a company called Pure-IP who not only provide us with primary connection lines, but also secondary back up lines which are set to auto fail over, giving us a full resilient system.

The day-to-day functional use of Microsoft Teams is supported by the Internal IT Team who action any requests or issues related to set ups, hunt groups and dropped calls.

Critical Documents

As we have fully facilitated secure Cloud storage systems throughout our business, there is no longer a requirement for us to store physical paper copies of critical documents.

Everything is held securely across a range of Cloud-based servers and is backed up on a daily basis to off-site premises.

Office Premises Inoperable

In the event of a fire or flood and the office becoming inoperable, staff will be instructed to either work from home or go to one of our other offices as an alternate location.

We have provided our staff with company laptops and mobile phones to enable them to either work from home or another one of our offices. Microsoft Office365, OneDrive and Teams enable them to access their emails, documents and collaborate with their colleagues wherever they are.

Industrial Action

Whilst we do not recognise any specific union, the company recognises the role played by third party representatives in communicating and supporting employee interests and supports the continued right of employees to retain the assistance of such representation in industrial processes.

As a recruitment business providing temporary and contract workers to a broad range of clients, we respect the industrial relations policies held by our clients and will support such policies wherever possible, however we will not supply an employee, temporary worker or contractor to a client to replace an individual taking part in an official strike or any other official industrial dispute in line with Regulation 7 of the Conduct of Employment Agencies & Employment Businesses Regulations 2003.

To minimise the impact of potential industrial action, we will encourage employees, clients, temporary workers and contractors to take a positive and constructive approach to industrial relations by use of consultation and negotiation procedures to resolve industrial disputes as they may arise.

We will:

- Engage with the client's Industrial Relations Representative to ensure that IR strategies, practices and risks are managed in a co-ordinated manner;
- Ensure that it complies with all current labour market legislation;
- Employ and engage individuals under ethical, fair, reasonable and market competitive terms and conditions;
- Foster positive, productive and respectful relationships with employees, temporary workers and contractors;
- Build effective partnerships with all stakeholders to achieve improvements in business performance, terms & conditions and staff involvement;
- Provide employees, temporary workers and contractors with the opportunity to give feedback in relation to their terms & conditions of employment/engagement;

- Fulfil its responsibilities in terms of health & safety at work legislation and best practice and develop, implement, maintain and communicate safe working practices;
- Neither discourage nor prevent staff, temporary workers or contractors from joining a relevant trade union;
- Discuss and agree the pay and conditions for its contractors and temporary workers to minimise potential instability and ensure that all temporary workers and contractors within the scope of the Agency Workers Regulations are given “equal treatment” after 12 weeks in a given assignment;
- Encourage employees, clients, temporary workers and contractors to take a positive and constructive approach to industrial relations by use of consultation and negotiation procedures to resolve industrial disputes as they may arise.

We will also:

- Keep the client informed of any relevant agreements and policies (and changes to these) that apply to employees, contractors or temporary workers;
- Provide information to the client in relation to the contracts in place between ourselves and our contractors and temporary workers;
- Participate as required in client forums and meetings to support consistent and correct application of policies and procedures and to co-ordinate the approach to Industrial Relations during periods of potential or actual disputes;
- Inform any contractor or temporary worker of any planned strike action to take place at the location at which they are assigned to work;
- Remove any contractor or temporary worker from an assignment where they are either doing the work of someone taking part in official industrial action or where they are doing the work of someone who has been transferred by the hirer to perform the duties of a person taking part in industrial action;
- Ensure that temporary workers and contractors are provided with written confirmation of their pay rate, overtime/bonuses if applicable, holiday pay and hours of work in advance of the assignment start date;
- Operate a fair and consistent grievance & disciplinary procedure for employees and complaints procedure for temporary workers and contractors to support resolution of individual and collective issues;
- Engage with the client to ensure a co-ordinated and compliant approach to Health & Safety;
- Make temporary workers/contractors aware of their obligations.

Systems Testing

All systems are tested and reviewed by the Head of IT on a 6 monthly basis to ensure business continuity in the event of significant issues relating to systems or premises.

Following regular testing, should any issues be identified, the Managing Director will determine how best these can be resolved. Any such changes or improvements will be subsequently tested (without risk to the system). Only when they are found to resolve the issue and be reliable will full implementation take place.

Security

We understand that there is always a risk of malicious attack on our systems, and as such we ensure that all sensitive equipment and data is kept in a secure area.

Core systems which are office based are located in a communications room which is only accessible by selected staff within the organisation which includes the IT team and the office manager only. Access is granted via touch card system which is supported by Paxton and on the level of access required will determine the times the room is accessible.

The same system is in place for access to the main office and all entries to the office are recorded within the Paxton Net2 application. Together with the touch card access system, there is CCTV located in the office which records 24 hours a day and keeps 5 days' worth of footage.

The office has an alarm fitted which is turned on every evening and turned off every morning. The alarm system has motion detectors assigned to it, and these are located in key areas to ensure full coverage.

The systems themselves have limited access which is isolated to the IT team only and no other access is granted to end users. Any Cloud-based system has 2FA (2 factor authentication) applied to it, so the platform which hosts the systems must have correct credentials as well as the 2FA code before access is allowed.

For the Cloud-based systems hosted by the organisation, all external access is disabled and only internal access is enabled.

For end users, a password policy exists which covers the below:

- Passwords expire after 60 days
- Minimum characters required are 8
- Complex password is enabled so must include symbols, numbers, upper and lowercase letters
- Remembers last 5 passwords so they cannot be used
- Lockouts of accounts after 4 wrong attempts

Passwords can be reset on by users either by being on a domain joined device and being on the organisations network; or by navigating to a Microsoft webpage and entering their details to change their password via Cloud based systems. The second option is protected by Microsoft's MFA (multi-factor authentication) system as an extra precaution.

We hold Cyber Essentials certification and have done so for the past several years. This is renewed on a yearly basis and systems are kept compliant. We have implemented ISO27001 compliant security policies which define best practice. Although we do not currently hold ISO27001 accreditation, the policies are kept up to date and reviewed on regularly.

Staff Training & Communication

Our staff are continuously involved in the development and testing of our business continuity plan together with receiving information updates on a regular basis to ensure engagement and full understanding of our business continuity measures. All key staff have also attended mandatory training on our procedures relating to business continuity and are in possession of a copy of this policy. Updates to procedures are communicated through training delivered in person/via video conference and followed up with written instructions.

Staff have undergone training to cover each other's roles/duties within teams in case of illness/absence. This has been undertaken "on the job" and by ensuring all processes and procedures are documented for reference.

If the nature of the disaster requires it, contractors and temporary workers will be provided with written instructions and be advised to tell us if they have any worries or concerns regarding their work or pay during any business disaster.

Insurance

The company holds the following insurances:

Employer's Liability – £10,000,000
Indemnity Limit Any One Accident restricted to £5,000,000 for asbestos, offshore or terrorism

Public Liability – £10,000,000
Indemnity Limit Any One Occurrence

Products/Pollution Liability – £10,000,000
Indemnity in the Aggregate

Professional Indemnity – £10,000,000
Indemnity Limit Any One Occurrence

The policies are reviewed annually with our insurance brokers and underwritten by Lloyds.

Review

This policy will be reviewed every 12 months and may be altered from time to time in light of legislative changes or other prevailing circumstances.

Signed: 

Name: Christopher Coyle

Job Title: Managing Director

Date: April 2026