



MAYDEN Health
Policies and Procedures

IG09

Business Continuity Plan

Information Governance

August 2010

IG Policy Index	
IG01	Information Governance
IG02	Information Security
IG03	Personal Information Handling
IG04	Confidentiality Code of Practice
IG05	Data Quality Policy
IG06	Risk Management
IG07	Security Incident Policy
IG08	Lifecycle Management
IG09	Business Continuity Plan

Current Version

Responsibility of	Information Governance Lead
Reviewed by	
First Issued	November 2009
Last Review Date	August 2010
Next Review Date	August 2011

Version History

Version	Date	Comment	Initials	Signature
1.0	3/12/09	Initial version following wide comment	CM	
1.1	23/8/10	Update to reflect latest position and practices	CM	

Roles and Responsibilities

Information Governance Lead	Chris May
Information Security Lead	Chris Eldridge

CONTENTS

1	Purpose	1
2	Introduction	1
3	Policy statement.....	1
4	Definitions	1
5	The business continuity planning process	2
6	Impact Analysis and Mitigation Planning	2
7	Records Management	2
8	Roles and Responsibilities	3
8.1	Managing Director	3
8.2	All Employees.....	3
9	Implementation and Review	3
9.1	Implementation	3
9.2	Review.....	3
10	Equality and Diversity statement	3

PART ONE

1 Purpose

This document sets out the general principles and processes for the creation and revision of business continuity and service recovery plans for Mayden Health. Furthermore, key individuals/roles are defined to ensure clarity is provided regarding authority to involve business continuity plans and to highlight roles and responsibilities in the event of a disaster.

2 Introduction

Mayden Health must ensure that the highest level of service to clients is maintained regardless of what might happen to the infrastructure of facilities, human resources or internal procedures. Business continuity is an important part of Mayden Health's risk management arrangements.

There are many varied possible causes of service disruption. As a general guide, business continuity planning must be carried out to minimise the effects of a number of potentially disruptive events, for example:

- Loss of IT utilities
- Application failure
- Major disruption to the server
- Burglary
- Major disruption to staffing

It must be understood that these events may not be mutually exclusive; for example a major disruption to the server may result from burglary and so on.

3 Policy statement

Mayden Health will take all reasonable steps to ensure that in the event of a service interruption, essential services will be maintained and normal services restored as soon as possible. To ensure that this happens it is our policy to have in place robust business continuity and service recovery plans that are regularly reviewed and tested.

4 Definitions

A service interruption is defined as:

“Any incident which threatens personnel, buildings or the operational procedures of an organisation and which requires special measures to be taken to restore normal functions.”

An appropriate response would aim to maintain essential services and restore normal services as soon as possible in the circumstances prevailing at the time.

Business continuity management can be defined as:

“The identification and management of risk and threats faced by Mayden Health (due to disruption and interruption), taking steps to control and reduce the risks, assessing the impact on the organisation if the risks should materialise, and providing a plan to be followed to ensure that the activities of the organisation continue.”

The goals of business continuity can be defined as:

- Resuming business operation in a reduced but controlled manner after a disaster which impacts on operation – until full recovery is achieved
- Resuming IT operations after a disaster which impacts on IT operation – until full recovery is achieved

5 The business continuity planning process

The Business Continuity Institute has developed a five-stage approach that has been incorporated into a British Standards Institute Publicly Available Specification (PAS 56). The process is widely accepted as ‘industry standard’.

The five stages are:

- Understanding your business; defining the critical/core functions of the organisation
- Identifying risks and how they are to be managed
- Developing a response to risks
- Raising awareness and embedding plans
- Maintaining and auditing plans

Mayden Health has adopted this process. The core functions analysis, risk identification and business plans that form part of Mayden Health’s Business Impact Analysis must be reviewed and amended at least annually, or sooner if there is a major service development.

6 Impact Analysis and Mitigation Planning

It is important that all individuals have ownership of the hazard review and mitigation implementation that falls out of the Business Impact Analysis. Resulting plans will be cascaded to all staff within Mayden Health as appropriate. The Managing Director is responsible for ensuring that employees are given adequate training to assist them with the implementation of business continuity plans. This training will vary in accordance with employee responsibility and the general content of each required plan.

7 Records Management

All records created during the implementation of a business continuity plan must be kept in line with overarching Information Governance Policies.

8 Roles and Responsibilities

8.1 Managing Director

The Managing Director has overall responsibility for ensuring that Mayden Health has in place effective arrangements to respond to an incident that has a potential to affect service provision

8.2 All Employees

All employees must make themselves familiar with their individual roles and responsibilities as set out in:

- This policy and procedure
- Any required business continuity plans

9 Implementation and Review

9.1 Implementation

This policy and procedure will be distributed to all employees with an accompanying letter setting out any individual responsibilities as required. This policy and procedure will be available on the Mayden Health's intranet and hard copies will be kept at the office in the relevant policy folder.

9.2 Review

This policy and procedure will be reviewed annually, or sooner as required.

10 Equality and Diversity statement

This document complies with Mayden Health's Equality and Diversity statement.

PART 2 – Business Impact Analysis templates [update required]

Hazard	Situation	Impact	Mitigation in place	Risk Matrix Score
Application Failure	Two servers in operation, with data mirrors on both servers. Currently no application mirror.	Loss of application function for circa 4 days.	<ol style="list-style-type: none"> 1. Data mirrors do already exist on the servers, thereby providing a backup solution if one were to fail. There is a future plan to install an additional pair of servers, reflecting the data and application information for each original server. Further plans are in place to add an additional application and data mirror on an offsite server. 2. Maiden Health data is backed up each night onto an offsite server at a data centre and via USB. 3. Maiden Health guarantee performance will be resumed within 4-days. 4. If application were to fail, users could still access the backup data via key fob entry. 	B
Burglary	Mayden Health's office is highly secure with the building locked and alarmed.	<ol style="list-style-type: none"> 1. Loss of employee data. 2. Loss of client data. 3. Loss of hardware 	<ol style="list-style-type: none"> 1. No patient identifiable or sensitive information is stored on the office server unless in a secure TrueCrypt vault. 2. Details to alarm system are restricted. 3. Windows are secured with screw locks. 4. At least double door entry is required to access the server room. 5. All folders retained on the office server are password protected. 6. Email system is password protected. 	B
Loss of entire team resource		<ol style="list-style-type: none"> 1. Loss of team knowledge. 2. Client inability to access data or application. 	<ol style="list-style-type: none"> 1. Web servers are owned by another company and therefore would continue to run. 2. Back up server is managed by another company offsite (SCI-TEQ). 3. Maiden Health plans to develop an escrow agreement with SCI-TEQ, which will eventually allow backup data to be released to clients. 	B
Loss of Managing Director		<ol style="list-style-type: none"> 1. Loss of knowledge. 2. Loss of consultancy function. 	<ol style="list-style-type: none"> 1. Managing Director seeking Deputy Director to ensure continuity of business if this scenario were to occur. 2. Aware of other companies that undertake similar work and could provide interim continuity if required. Plan to strengthen relationships with these companies. 	D
Loss of Employees		<ol style="list-style-type: none"> 1. Inability to fulfil client requirements 	<ol style="list-style-type: none"> 1. Plans to expand team to counteract potential loss of workforce. 2. Good relationship with a consultancy company so could, at short notice, expand workforce. 	B
Loss of SCI-TEQ	The company that store the backup server for Maiden Health is run and managed by a single person.	<ol style="list-style-type: none"> 1. Loss of access to Backup server 	<ol style="list-style-type: none"> 1. Undertaking conversations with SCI-TEQ to discuss options for expansion of this company. 	B

Emergency Response Checklist

For use during an emergency

- Start a log of actions taken
- Liaise with Emergency Services
- Identify any damage
- Identify Functions disrupted
- Convene your Response/Recovery Team
- Provide information to staff
- Decide on course of action
- Communicate decisions to staff and business partners
- Provide public information to maintain reputation and business
- Arrange a Debrief
- Review Business Continuity Plan



