



Business Continuity Management (BCM) Policy

Version 1.0

February 2019

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
DOCUMENT CONTROL	3
DOCUMENT OWNER	ERROR! BOOKMARK NOT DEFINED.
DOCUMENT HISTORY.....	ERROR! BOOKMARK NOT DEFINED.
INTRODUCTION	4
OBJECTIVE	4
SCOPE.....	4
GENERAL RESPONSIBILITIES	4
GLOSSARY OF TERMS.....	4
STATEMENTS	5
BUSINESS IMPACT ANALYSIS.....	5
BUSINESS CONTINUITY PLANNING	5
BUSINESS CONTINUITY TESTING	6

DOCUMENT CONTROL

This is a controlled document.

All changes must be authorised by the document owner and tracked below.

DOCUMENT OWNER

Owner:	Robert Nathan
Phone:	1800 876 642
Email:	admin@cloudtronics.com.au

DOCUMENT HISTORY

Version	Date	Summary of changes
0.1	7 February 2019	Robert Nathan – Initial version.
1.0	8 February 2019	Approved by Robert Nathan.

INTRODUCTION

OBJECTIVE

This objective of the *Business Continuity Management (BCM) Policy* is to counteract interruptions to business activities including the effects of major failures or disasters and to ensure timely resumption when they occur.

SCOPE

This policy applies organisation-wide including:

- information created or received by the company in hardcopy or electronic form
- systems (e.g. hardware & software) used to store, process or transmit company information
- people accessing company information (employees, contractors and external parties)
- physical assets used to protect company information
- suppliers that store, process or transmit company information on behalf of the company

GENERAL RESPONSIBILITIES

Role	General responsibilities
Executive	<ul style="list-style-type: none">• Approve the Information Security Management Framework (ISMF) policy and monitor performance
ISGC	<ul style="list-style-type: none">• Approve this and other policies, standards and procedures
Managers	<ul style="list-style-type: none">• Apply policies and associated procedures on a risk-managed basis
All	<ul style="list-style-type: none">• Conform with company policies such as this and associated procedures• Report suspected or actual deviations to management: (e.g. via security@cloudtronics.com.au)

Further specific responsibilities are assigned in each policy.

GLOSSARY OF TERMS

Refer to the glossary of terms as required.

STATEMENTS


The *Business Continuity Management (BCM) Policy* addresses the following topics:

- Business impact analysis
- Business continuity planning
- Business continuity testing

Other topics are addressed in complimentary policies, standards, guidelines and procedures.


BUSINESS IMPACT ANALYSIS

The *Executive*:


Ref	Statement	
BCM-1	<p>Assesses the impact of downtime of business processes after significant change or at least <u>annually</u> including consideration of:</p> <ol style="list-style-type: none"> 1. Maximum Tolerable Downtime (MTD) – how long can it be unavailable? 2. Recovery Time Objective (RTO) – how long can recovery take? 3. Recovery Point Objective (RPO) – how much data can be lost? <p>Note: Analysis of MTD, RTO and RPO can be found in the Information Asset Register for each system with a High availability classification.</p>	

BUSINESS CONTINUITY PLANNING

The *Executive*:

Ref	Statement	
BCM-2	Maintains a Business Continuity Plan and reviews the plan after significant change or at least <u>annually</u> including consideration of security related scenarios (e.g. Denial of Service, Ransomware).	

System Managers:

Ref	Statement	
BCM-3	Maintain a Disaster Recovery Plans and reviews their plans after significant change or at least <u>annually</u> including recovery procedures for security controls (e.g. firewalls, authentication services, logging etc).	

The CISO:

Ref	Statement	
BCM-4	Store backups of critical information, along with associated recovery procedures, at a remote location secured in accordance with the requirements for the Confidentiality classification of the information.	ISM

BUSINESS CONTINUITY TESTING

The *Executive*:

Ref	Statement	
BCM-5	Tests (or arranges for testing of) the Business Continuity Plan after significant change or at least <u>annually</u> . Note: A test may be a desk check (walk through the Business Continuity Plan and recovery procedures).	