



Document ID	POL038
Document Title	Business Continuity and Management Strategy and Policy
Author	Kevin Beadon
Version	1.40

Revision History		
Date	Version	Change
28/08/2019	0.1	New Document
29/08/2019	1.00	Update after internal review
08/06/2020	1.10	Annual review
30/06/2021	1.20	Annual review
30/06/2022	1.30	Annual review
28/06/2023	1.40	Annual review

Distribution		
Date	Version	Distribution
28/08/2019	0.1	Keith Richardson, Sara Mitchell
29/08/2019	1.00	Keith Richardson, Sara Mitchell
08/06/2020	1.10	All staff via Intranet and Library
30/06/2021	1.20	All staff via Intranet and Library
30/06/2022	1.30	All staff via Intranet and Library
28/06/2023	1.40	All staff via Intranet and Library

Signed			
Date	Version	Name	Role
28/08/2019	1.00	N/A	N/A
08/06/2020	1.10	Keith Richardson	CFO
30/06/2021	1.20	David Rawle	CTO
30/06/2022	1.30	David Rawle	CTO
28/06/2023	1.40	Sam Kynaston	Digital Transformation Director

Next Review: 30/06/2024

Contents

Introduction.....	1
Aims	1
Approach	1
Documentation	2
Risk Assessments.....	2
Disruption Scenarios	3
Building - Head Office	3
Building - Regional Office	3
Failure of Critical IT services or systems	3
Failure of Critical Suppliers	3
People	3
Recovery	3
Building	3
Failure of Critical IT services or systems	4
Critical suppliers.....	4
People	4
Testing.....	4
Building – Head Office and Regional.....	4
Failure of Critical IT services or systems	4
Critical suppliers.....	4
People	5
Review of Policy	5

Introduction

The purpose of this document is to define the strategy and policies that will enable Bytes Software Services (“Bytes” or “the Company”) to continue as an effective business in the event of disruption to services. This strategy ensures that service provision within Bytes follow the same framework for Business Continuity.

This strategy addresses the arrangement for business continuation for the first two weeks of operation. If disruption is expected to take longer than two weeks this time will be used to identify further arrangements.

Aims

The aim of this strategy is to:

- Help ensure the continuity of service provision in the event of business disruption
- Save time and reduce an initial confusion
- Minimise general disruption to customers and employees
- Preserve the company’s image and reputation

Approach

The diagram illustrates the Company’s approach to business continuity.



The process starts with a risk assessment of the business which includes potential disruptions.

Once risks are understood these can then be analysed for their impact to the business which then informs the strategy requirements and what the strategy should be.

Once strategy is devised plans can be developed and tested. On completion of testing they are reviewed for suitability and the process starts again to ensure continued improvement.

Documentation

The delivery of the business continuity strategy and policy is detailed in the following documents:

- P:\Administration\ISO Standards\Forms\CURRENT Forms\QMF 07 Disaster Recovery Plan.docx – contains EMT, DR Team, restoration of building services and contact details
- L:\GDPR\Backup Policy - POL009.pdf - Details what data is backed up, how, frequency, retention, exceptions, transportation of media for offsite storage, disposal and verification
- P:\Internal Systems\System Support\1. 0 Documentation\5.0 DR Plan\Disaster Recovery Plan vxx.y – Contains important information about systems in the event of an issue, including software, hardware, power up and down orders, key support information and server software
- P:\Internal Systems\System Support\1. 0 Documentation\5.0 DR Plan\DR Activation Procedures Vxx.y – contains procedure to activate systems in the DR site for live and test.
- P:\Internal Systems\System Support\1. 0 Documentation\5.0 DR Plan\DR Failover Checklist – *Month Year.xlsx* – Testing and Activation checklist for IT Systems DR Plan
- P:\Internal Systems\System Support\1. 0 Documentation\5.0 DR Plan\Testing Register vxx.y.xlsx – Register IT Systems DR testing

Risk Assessments

The following documents outline the risks identified within Bytes and mitigating strategies. These form an input into the business continuity management strategy.

- P:\Administration\ISO Standards\Forms\CURRENT Forms\QMF 36 Risk Matrix - internal doc ONLY.docx – contains the identified risks to the business and mitigation strategies
- P:\Administration\ISO Standards\Forms\CURRENT Forms\QMF 51 Fire Risk Assessment - Bytes House.docx – Considers the risks of fire within the Bytes Head Office building and mitigating strategies
- P:\Administration\ISO Standards\Forms\CURRENT Forms\QMF 56 Risk Assessment - Bytes House.docx – Considers the risks within the Bytes office to staff and mitigating strategies

Bytes regional offices are hosted within a shared office environment and as such each of these offices maintain their own Fire Risk Assessment and mitigating strategies. These are reviewed as part of the take up of new office space.

Disruption Scenarios

Prior to developing business continuity plans different disruptions scenarios must be identified to build a strategy to deal with them.

A number of incidents can affect business for example, fire, flood and server failure each of which can result in disruption. Disruptions have been grouped into five categories:

Building - Head Office

A disrupting incident can take two forms:

- People are unable to access the building, but systems may be unaffected. For instance, this can be caused through incidents such as security threats, environmental contamination or a nearby serious incident such as a fire.
- Structural damage cause by fire or flood that makes the building unusable. This may affect systems.

Building - Regional Office

A disrupting incident can take two forms:

- People are unable to access the building. For instance, this can be caused through incidents such as security threats, environmental contamination or a nearby serious incident such as a fire. Systems will not be accessible from the building but will be available through other means.
- Structural damage cause by fire or flood that makes the building unusable. Systems access may not be available from the building but will be available through other means.

Failure of Critical IT services or systems

Critical IT systems could become unavailable. For example, server failure, storage failure, network issues or loss of Internet.

Failure of Critical Suppliers

Bytes rely on third party suppliers to supply and deliver services to our customers. An example of supplier disruption could be liquidation, fire affect their premises or failure of their systems.

People

Staff that support critical business activities may become available due to unplanned absence. Example include, personal injuries or debilitating illness.

Recovery

For each of the disrupting scenarios there must be a recovery plan. For each scenario the Emergency Management Team will decide to invoke the business continuity plan and will consider the nature, extent and estimated duration of the disruption.

Building

The recovery strategy for a disruption affecting access to all Bytes offices:

- Staff will be asked to work from home

The recovery strategy for a disruption caused by structural damage to all Bytes offices:

- Staff will be asked to work from home

Failure of Critical IT services or systems

All production IT systems are regarded as critical to the business and therefore covered by the company's Business Continuity Plan (BCP) Disaster Recovery (DR) Plan. Details of system recovery is available in the Disaster Recovery Plan and Disaster Recovery and Activation Plans. In the event of a:

- Disruption to all systems, for example fire, then all production systems must be available in an alternate location within one working day
- Failure to a component of the IT system, for example server or network switch failure then the architecture must facilitate redundancy to prevent loss of service
- Disruption caused by loss of data, for example data has been deleted, then backups must be retained.
- Supplier suffering disruption then Bytes will rely on the supplier's business continuity plans or in the case where purchasing is via distribution -alternative suppliers if this is an option.

Critical suppliers

Critical suppliers will be asked to supply details of their BCP. Evaluation of supplier BCP will form part of the tender process or onboarding if no such tender is required.

People

Key people are those who have been identified as being critical to the completion of key activities within the business. The BCP will identify such people and detail the succession plan if the primary resource is not available.

Testing

Testing of the Plan is required to ensure that the business continuity arrangements are viable, that staff understand and are rehearsed in their roles within the Plan so that disruption is minimised.

Building – Head Office and Regional

Remote working is a core service provided by Bytes and therefore is continually tested.

Failure of Critical IT services or systems

- An all system IT disaster recovery test is performed at least annually. This will prove that systems can be made available in a timely manner
- Redundant architecture and components are tested as far as possible at the point of implementation. This will ensure that systems will remain available in the event of component failure
- Generator is tested weekly to ensure that the generator is available in the event of a power failure
- UPS is monitored daily to ensure that it is available in the event of a power failure
- Backup recovery is performed on randomly selected data monthly. This will prove that backup data can be restored

Critical suppliers

Bytes will rely on the critical suppliers own testing strategies which will be evaluated when they supply their own business continuity plans.

People

Succession plans are in place. Training is carried out for key people and succession personal. It is imperative that all staff involved in DR planning and recovery receive relevant training and rehearsal time.

Review of Policy

The Business Continuity and Management Strategy must be reviewed annually to ensure it is still suitable. In addition, it will be reviewed after any activation and rehearsal to discuss and understand lessons learned.

The review is conducted by:

- David Rawle – Chief Technology Officer
- Kevin Beadon – Head of IT