

Datagraphic

Business Continuity and Disaster Recovery Policy

010



Business Continuity and Disaster Recovery Policy

Document Information

Version:	2.1
Status:	LIVE
Issue date:	22/04/2024
Classification:	Public
Approved by:	Robert Hoon – Managing Director
Author:	Mike Green – Chief Information Security Officer (CISO)
Owner:	Information Security Steering Committee (ISSC)

This policy is:

- A controlled document forming part of the Datagraphic ISO 27001 Information Security Management System (ISMS). All revisions must be made following the document control requirements of the standard.
- Effective from the Version and Issue date above. It supersedes previous versions, which are withdrawn and hard copies destroyed.
- Effective for Datagraphic Limited and Datagraphic Group Limited (hereafter referred to as “Datagraphic”).
- Uncontrolled when printed. The ‘master’ document is available under Datagraphic’s ISO 27001 ISMS Documentation Control Log.
- Subject to change by Datagraphic in line with changes in statutory law, case law and best practice.

Contents

Overview	3
Business Continuity (BC) defined	3
Disaster Recovery (DR) defined	3
Datagraphic's approach to BC and DR	4
BC Controls: on-site	5
DR Controls: off-site	6
BC and DR for Datagraphic IT Systems	7
Reciprocal DR	8
Biological Threats	9
Plans to minimise business disruption from a Pandemic	9
Impact on travel and business meetings	9
Measures to protect our production centre	10
Technical provisions	10
Key workers	10
Information Security in the BC/DR Management Process	11
Minimum security requirements for BC solutions	11
Minimum security requirements for DR solutions	11
Developing and implementing continuity plans, including Information Security	12
BC planning framework	12
Testing, maintaining and re-assessing BC plans	12
DR testing	12
Document History	13

Overview

Business Continuity (BC) defined

Business Continuity (BC) is a term used to describe mechanisms that minimise the impact on operations in the event of a disruption. A disruption can be caused by the failure of systems or components of these systems. In the context of this document, BC is taken to mean mechanisms in place at Datagraphic's office and factory locations. These mechanisms can be invoked at Datagraphic's office and factory locations without relocating systems or staff.

Disaster Recovery (DR) defined

Disaster Recovery (DR) is a term used to describe mechanisms that minimise the impact on operations in the event of severe disruption. Disruptions of this nature typically force the closure of Datagraphic premises. Thus, DR mechanisms require dedicated off-site locations and systems.

Datagraphic's approach to BC and DR

All Information processing facilities at Datagraphic have been risk analysed to identify events that could interrupt business processes. For a methodology for achieving this, please see our ISMS document **18 – Risk Assessments and Asset Register.doc**.

This BC and DR policy attempts to reduce the likelihood of these events occurring and/or the impact they would have if they were to happen.

This is achieved via the following guidelines:

- Implementing controls that reduce the likelihood of the event occurring
- Regularly testing these controls to ensure they are effective
- Avoiding risks by not allowing actions that would cause the risk to occur
- Reducing the impact on business processes if the event were to occur (i.e. backup systems)
- Transferring the risks to other parties (insurers/suppliers). It must be realised that this approach can still lead to losing customer confidence.
- Ultimately, if a risk cannot be reduced, it must be knowingly and objectively accepted by management in a formal signing-off process.

BC Controls: on-site

Datagraphic has a highly available IT infrastructure that can withstand BC and DR events, having been implemented and refined over decades.

Our ISO 27001 risk assessment methodology enabled us to identify single points of failure and implement controls that significantly reduce or mitigate risks associated with threats to availability.

Examples of threats include:

- Hardware failure
- Internet connectivity failure
- Network failure
- Cooling system failure
- Electrical supply failure
- Production device failure
- Key staff unavailability.

We continuously invest in BC controls to ensure critical systems and processes are resilient to failure. Investments have included on-site and off-site backup of Information processing facilities, the associated technology, and the skills to enable resilience.

We've eliminated single points by:

- Building resilience into IT Infrastructure
- Fully virtualising IT Infrastructure
- Operating a High Availability network
- Implementing two separate data rooms at our Rugby production site
- Implementing an off-site DR facility
- Ensuring critical infrastructure replicates every 12 hours on-site and off-site
- Taking twice daily system-level backups of all IT systems
- Having multiple, highly reliable, diverse Internet connections
- Installing resilient climate control systems in all data rooms
- Maintaining extra printing/enclosing capacity during a machine failure
- Having on-site staff to routinely service and maintain fulfilment equipment
- Carrying on-site spares for critical systems
- Protecting critical systems from power loss by Uninterruptible Power Supplies (UPS)
- Maintaining an on-site generator to keep services running in a power cut
- Cross-training key staff and recording detailed procedures within an in-house Intranet.

DR Controls: off-site

Datagraphic is prepared should DR measures need to be implemented in a worst-case scenario where our main site cannot function.

We replicate all critical Information over an encrypted Wide Area Network (WAN) link to our head office in Derbyshire, a secure DR data location. This facility is 70 miles from Datagraphic's Warwickshire production and technology centre. As a default, every 12 hours, critical systems replicate to this ISO 27001 certified secure location. In DR invocation, this 'warm standby' can be turned on, to achieve the agreed Recovery Point Objective (RPO). Where required by specific client contracts, bespoke replication and RPOs are put in place.

In addition to the off-site Information processing facility, we maintain a contract and close working relationship with Critical Mail Continuity Services (CMCS). CMCS provide printing and document enclosing in a disaster. CMCS hold ISO 27001 and CPAS Standard 55.

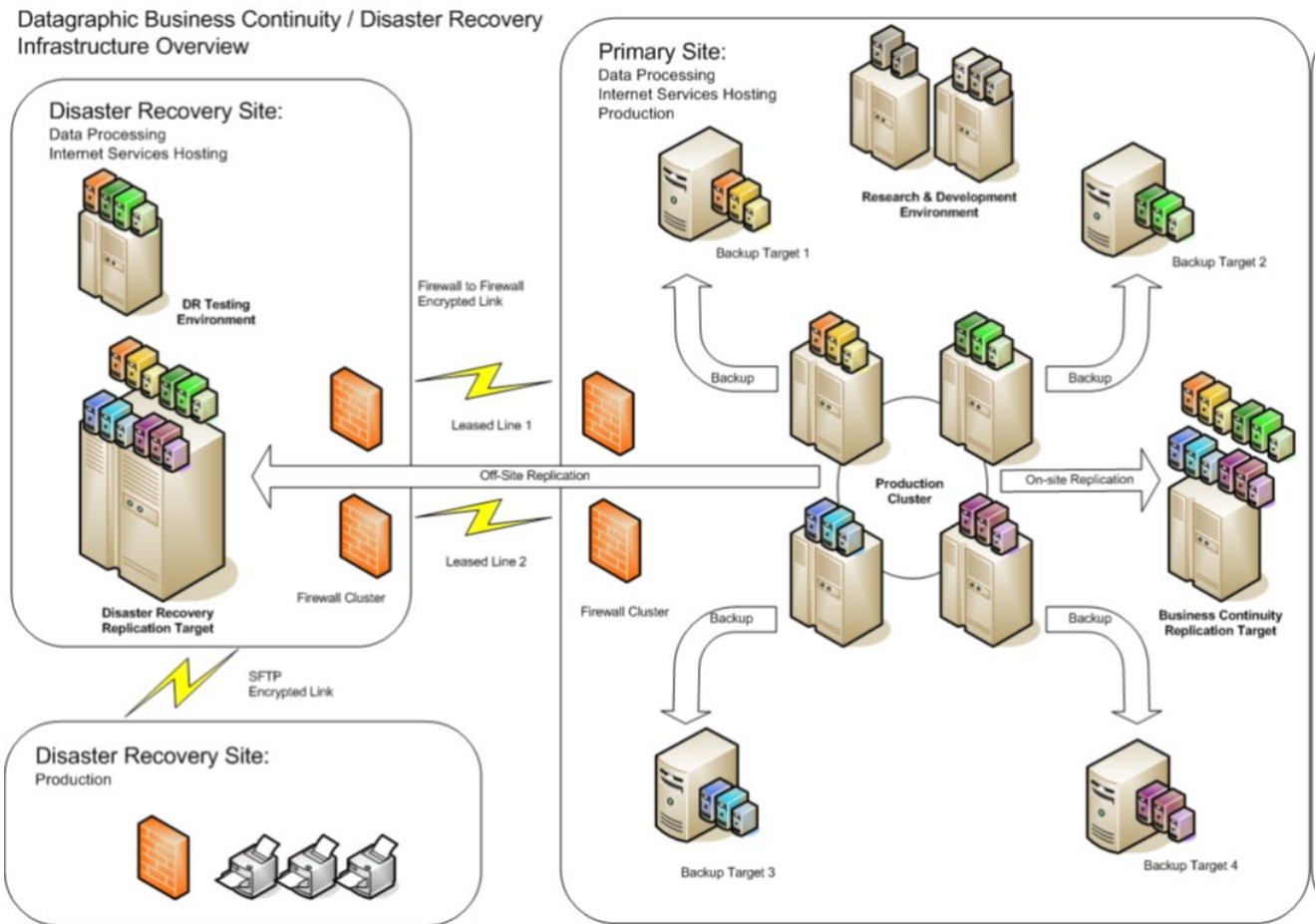
Datagraphic conducts regular testing to ensure CMCS remains a viable and efficient option in a worst-case scenario. CMCS is 60 miles from our Rugby centre. When required, key Datagraphic staff can operate from CMCS and assist CMCS staff in fulfilling client printing and mailing requirements.

To adequately prepare for a DR incident, we recommend that clients consider the following DR controls:

- **Off-site stock:** specialist stocks often have significant manufacturing lead times. If using specialist stock, performing a stock review and locating some stock at the off-site facility may be advisable. This could be used in a DR Invocation
- **DR testing:** we can support clients to prove their DR plans are compatible with DR controls through bespoke DR testing activities.

BC and DR for Datagraphic IT Systems

This diagram illustrates Datagraphic's approach to BC and DR for our IT systems.



All systems are:

- Virtualised
- Provisioned on High Availability of host systems
- Replicated on-site every 24-hours
- Backed up on-site every 24-hours
- Replicated to our DR facility every 24-hours

If the Production Cluster hosts fail, guest systems can be brought online using the BC Replication Target.

Live systems can be migrated between hosts in the production cluster without downtime.

Should the Primary Site be unavailable, systems can be brought online at our DR site.

We operate a dedicated Research and Development Environment.

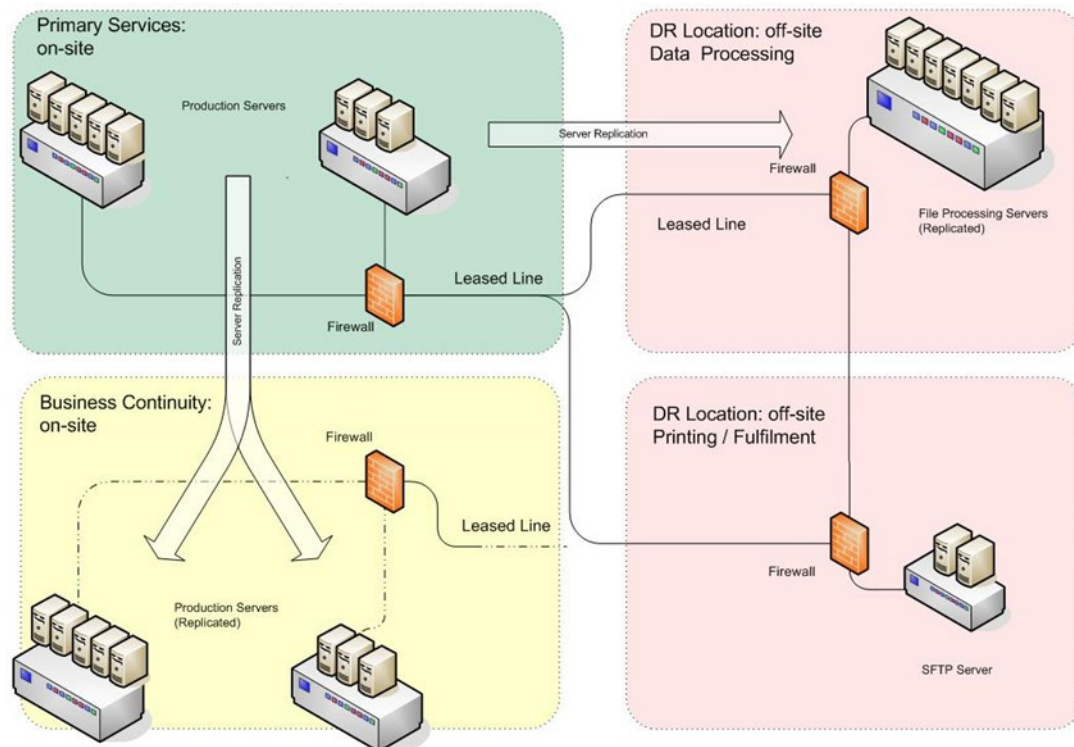
Reciprocal DR

Datagraphic in Rugby and Chesterfield share reciprocal DR arrangements regarding key infrastructure and Information Processing facilities.

The following criteria should be met:

- All key systems should be replicated regularly on the other premises
- Systems should replicate based on their required Recovery Point Objective (RPO)
- Business-critical systems should be replicated every 24-hours
- Non-business critical systems should be replicated weekly
- System-level encryption should be in place at Datagraphic Chesterfield
- All drives on the DR hypervisor are encrypted
- DR networks must remain independent and segregated from other networks.

IT Infrastructure Overview



Biological Threats

In a pandemic disease event (as classified by the World Health Organisation) affecting the UK, the following Biological BC plan shall be invoked:

As a business-critical communications provider, we have comprehensive BC plans.

In a pandemic event, a team of key Datagraphic staff will monitor pandemic updates. We will follow guidance from the UK government, regulatory agencies and health professionals. As advice changes, we will be ready to fast-track decision-making via our leadership team.

We will have key staff coordinating internal roles and responsibilities during an outbreak. Should this team fall ill or cannot carry out its responsibilities, we will also have a backup team.

Plans to minimise business disruption from a Pandemic

We will aim to deliver services as close to business-as-usual as possible during a pandemic. We have tested preparations for office closures, production limitations and critical service disruptions.

Should we need to restrict access to offices, we have secure remote connections to business systems, allowing staff to work from home. Phone lines can also be diverted to avoid disruption to inbound call handling.

Impact on travel and business meetings

We will restrict travel and meetings, suspending travel to, from, or through affected countries to reduce the infection risks. All non-essential UK travel will be under review.

People returning from a country affected by a pandemic must self-isolate for at least 14 days.

Face-to-face meetings will, where practical, take place using video or telephone conference channels.

Measures to protect our production centre

Restrictions in our production centre would stop access by non-essential visitors/suppliers.

Should production staff be ill or unable to complete their duties, we have extra staff cross-trained to operate equipment and to complete client orders.

If our production centre is significantly affected by a pandemic, we will invoke incident/recovery protocols to ensure business operations continue.

We will also monitor raw material supplies. Should supply chains lengthen, we will endeavour to acquire extra stock so production can continue.

Technical provisions

Our IT infrastructure and web-based applications have built-in resilience. Our system virtualisation and replication processes ensure services will continue should the primary resource be unavailable.

Key workers

In response to a UK government announcement that people should stay at home – unless their work absolutely cannot be done at home – Datagraphic's position will be that:

Only essential members of Datagraphic's workforce will attend work daily. These are workers unable to work from home. Those involved in:

- The production and distribution of essential transactional and advice communications for key industries, including:
 - Health services
 - Financial services
 - Utilities
 - Local or central government authorities
- The production and distribution of cheques for expected payments
- The distribution of legally required payslips and P60s for clients
- Supporting the data and IT infrastructure to deliver the vital communications above
- A senior management role, safeguarding and supporting other essential workers defined above.

We would take every practical step to increase hygiene routines and support essential workers with social distancing, including split shift working to minimise contact.

Information Security in the BC/DR Management Process

Wherever a control is implemented to reduce the likelihood and/or impact of a vulnerability, the revised system must be risk analysed before implementation using Datagraphic's standard risk assessment methodology:

- If implementing such measures will create threats to business processes, these must be risk analysed and reduced to an acceptable level or knowingly and objectively accepted by management in a formal signing-off process.

Minimum security requirements for BC solutions

The minimum security requirements for BC solutions at Datagraphic are:

- All BC solutions must be compliant with ISO 27001 / Pay.UK CPAS Standard 55
- The invocation of such measures should not introduce a greater risk to the business process than initially accepted.

Minimum security requirements for DR solutions

The minimum security requirements for DR at Datagraphic are:

- Any DR site that produces the in-filled variable print must have ISO 27001 / Pay.UK Standard 55 certification.

Developing and implementing continuity plans, including Information Security

Plans are developed and implemented to maintain or restore operations and ensure the availability of Information at the required level and in the necessary timescales following an interruption to, or failure of, critical business processes.

Our policy is that all DR options must have an equal, commensurate or higher levels of Information Security.

BC planning framework

A framework of BC plans is maintained to ensure all procedures are consistent, address Information Security requirements consistently, and identify priorities for testing and maintenance.

Testing, maintaining and re-assessing BC plans

BC plans are tested and updated regularly to ensure they are up-to-date and effective. We undertake the following activities:

- Internal auditing
- Risk assessment of Information Processing facilities
- DR testing at off-site data processing and production facilities
- Generator/UPS testing
- Internal BC tests (at the CISO's discretion)
- Annual ISO 27001 external audits
- Ongoing third-party security reviews/testing
- Client-led security reviews/DR testing

DR testing

We support clients in helping prove their DR plans are compatible with our DR controls through bespoke DR testing activities.

Document History

Date	Version	Author	Description of change
01/03/2006	1.0	K Adams	Release
21/07/2009	1.1	M Green	The biological Threat section added
21/10/2013	1.2	M Green	Veeam Backup section added
02/12/2015	1.3	M Green	Reciprocal DR added
04/04/2018	1.4	M Green	Reviewed and updated to the standard format
03/03/2020	1.5	M Green	Reviewed and updated to reflect upgraded BC/DR controls
23/03/2020	1.6	M Green	Reviewed and updated to reflect updated pandemic controls
21/01/2021	1.7	M Green	Reviewed and re-approved
09/06/2022	1.8	T Harris	Updated on to the new template
03/04/2023	1.9	M Green	Full review/formatting changes
17/04/2024	2.0	S Beech	Updated on to the new template
22/04/2024	2.1	A Scholey	Updates to reflect replication of critical systems in now twice daily (every 12 hours) as a default.

Questions

If you have questions about the contents of this policy, please contact:

Mike Green
CISO

T: +44 (0)1788 535383
E: issc@datagraphic.co.uk

Datagraphic

Registered companies:

Datagraphic Group Limited (Reg No: 01215380) and Datagraphic Limited (Reg No: 02913191).

Both registered in England at: Ireland Industrial Estate, Adelphi Way, Staveley, Chesterfield, S43 3LS.

© Copyright Datagraphic (2024) This literature is not to be copied without the written consent of Datagraphic.