BCP

The **Interclass** Group Business Continuity Management Plan

Introduction

Information and Communication Technology (ICT) continuity management supports the overall Business Continuity Management (BCM) process of our Organisation. BCM seeks to ensure that The Interclass Group processes are protected from disruption and that The Interclass Group is able to respond positively and effectively when disruption occurs.

The Interclass Group sets out its BCM priorities, and it is within this context that ICT continuity management activities take place.

ICT continuity management ensures that the required information and communications technology and services are resilient and can be recovered to predetermined levels within timescales required by and agreed with directors of The Interclass Group. Thus, effective BCM depends on ICT continuity management to ensure that The Interclass Group can meet its objectives at all times, particularly during times of disruption.

To be successful, both BCM and ICT continuity management have to be embedded within the culture of the Group

ICT Continuity Policy

The Interclass Group Information Communications Technology strategy is to improve information security provision i.e. the confidentiality, support, security, reliability and availability of ICT systems and the information processed by those systems – reducing the likelihood of data breaches and/or the loss of confidential or personal data;

ICT continuity management is an important strategy to protect the stakeholders of The Interclass Group, including shareholder value, customer service, profitability and jobs.

The person in charge of the adherence to the ICT continuity policy is the BCP Manager and he or she is responsible for ensuring that the policy is continued to be carried out and that any changes in the ICT strategy are implemented within ICT continuity management.

The policy is to be reviewed each year including the scope of service covered as part of a continuous improvement strategy. It will also be reviewed for its integration into the wider Business Continuity Plan (BCP) for the rest of the business and amended accordingly for any changes in business activity or identified risk.

ICT Requirements

The ICT services to The Interclass Group have been individually identified and linked to the servers which support them. The Interclass Group have undergone a review of each service and identified the maximum Return Time Objective (RTO) and Recovery Point Objective (RPO) for each which can be tolerated by The Interclass Group before a material impact on profitability, customer service and shareholder value would be incurred by the business.

RTO – the time taken to get a system fully tested and available to all users to useful work from the point of the disruption (including any decision time)

RPO – the time difference between point of the disruption and the point when the latest useable backup data can be recovered.

The **Interclass** Group Business Continuity Management Plan

Aim of this Plan

This document is designed to assist planning with emergencies that result in access being restricted to the Head Office premises, or emergency situations that affect all or a significant part of the Company's operations.

Objectives

- To define and prioritise the Critical Functions of the business
- To analyse the emergency risks to the business
- To detail the agreed response to an emergency
- To identify Key Contacts during an emergency

The Company Secretary and Managing Director David Jones shall be responsible for maintaining specific arrangements covering potential emergencies. These shall include, but not be limited to:

Priority	Critical Function
1	Fire – Safety
2	Structure or Building
3	IT Failure
4	Vehicle Accident
5	Gas leaks
6	Flu Pandemic
7	Asbestos Release
8	Fire – Environmental
9	Fuel Spillage
10	Flooding
11	Chemical / Paint Spillage

This list can be used during an emergency to assist your decision making when compiling an Action Plan as to which function needs to be reinstated first.

Business Continuity Strategy

(BCS) is structured to ensure that the most important or time critical business processes are tackled first, once we have secured the safety of our workforce and the general public (if affected).
With other processes being brought back as time permits. In general, the following priority list is correct:

- Service & Delivery of Project/Schemes
- Company Data and ICT Network Systems
- Finance Services
- Human Resources (HR)

The Disaster Recovery Plan

The DRP is to be included within the BCP and be the enabler through the reestablishment of critical communications and processes to a successful implementation of the BCP.

Recognising that The Interclass Group is a SME company with finite resources it cannot plan for every contingency, this plan details some recent scenario and recorded on the Log Sheet .Other scenarios will be added as part of the review process and principle of continuous improvement.

Personnel, Roles and Responsibilities

The Business Continuity Management (BCM) has overall responsibility for the maintenance of the Disaster Recovery Plan (DRP) and the Business Continuity Plan personnel have responsibility for ensuring that the DRP adequately protects the IT Services that are within their control.

Currently, the individual owners are as follows:

Owner	Prime Responsibilities
Dave Jones	1. To decide, based on the apparent risks to the business, whether the DRP should be invoked 2. To safeguard Customer and Staff Interests 3. To provide commercial assistance to the DRP 4. To have read and fully understood all relevant portions of the DRP 5. To manage expectations of all interested parties including staff, suppliers, customers, press 6. To authorise adequate resource to ensure that a smooth and predictable execution of the DRP and BCP can be achieved
Stewart Watkins (External IT)	1. CRM 2. Exchange Servers
Helen Watkins	1. To have read and fully understood all relevant portions of the BCP 2. To manage and operate the BCP 3. To ensure that the business continues to review and mitigate risks to the business in line with the BCM

BCM members work closely to ensure that they are able to cover for each member of the Board should the need require. Projects are covered by in house teams and roles can be covered temporarily by other members within the project team. Accounts systems are documented to enable personnel to follow work flows with agency staff if required.

Frequency of Testing

The Interclass Group recognise that it is important to test our continuity mechanisms so that we can be sure that they will operate effectively in 'real' circumstances. We implement disaster recovery testing on our IT systems once a year. We maintain up to date Fire Marshall & First Aid training for allowing our site supervisors and some office based staff to fall in line with the minimum necessary requirements.

Revision Plan

The Disaster Recovery Plan (DRP) and the risk assessment will be formally reviewed on a yearly basis, timed to incorporate lessons learned from the most recent test. In response to this, the plan will be re-evaluated, and revised versions of it distributed to all employees with explicit roles and responsibilities in a DRP scenario**.**

Analysis Table & Risk Matrix

A = HIGH Likelihood and HIGH Impact
B = LOW Likelihood and HIGH Impact
C = HIGH Likelihood and LOW Impact
D = LOW Likelihood and LOW Impact

Hazard	Likelihood	Mitigation in Place	Impact	Risk Matrix Score	RTO	RPO
Major accident or incident, national disaster, epidemic, terrorist attack	Low	✓	High	B		
Fire	Low	✓	High	B		
Structure or building Collapse	Low	✓	High	B		
ICT Failure (loss of Utilities)	Low	✓	High	B		
Transport Disruption	Low	✓	Low	D		
Gas Leaks	Low	✓	Low	D		
Flu Pandemic	Low	✓	High	B		
Asbestos Release	Low	✓	Low	D		
Flooding (Extreme Weather)	Low	✓	Low	B		
Chemical Spillage	Low	✓	Low	D		
Industrial Action inability to recruit; mass resignations	Low	✓	High	B		

*We also recognise that at the time of a major disaster, these circumstances may be interdependent, and cannot be treated as a standalone entity

Emergency Response Checklist:

□ Start a log of actions taken: □

□ Liaise with Emergency Services: □

□ Identify any damage: □

□ Identify Functions disrupted: □

□ Convene your Response / Recovery Team: □

□ Provide information to Client / Staff / Stakeholders and Public : □

□ Decide on course of action: □

□ Communicate decisions to Client / Staff / Stakeholders and Public: □

□ Provide public information to maintain reputation

And business: □

□ Arrange a Debrief: □

□ Review Business Continuity Plan: □

Lead - Key Contact Sheet

Contact	Office Number	Mobile Number	Useful information
Chris Watkins	01902 324422	07970961977	CEO
Dave Jones	01902 324422	07813896606	Managing Director
Peter Hood	01902 324422	07971953467	Director Plc
Garth Watkins	01902 324422	07980851186	Director ICS
Simon Round	01902 324422	07740087767	Director Surfacing
Helen Watkins	01902 324422	07977404749	Human Resources
Nicola Piggot	01902 324422	07711356703	Environmental Manager
Nicola and Shirley	01902 324422	N/A	Reception and archiving
Stewart Watkins	020 7915 8318	07753692999	I.T Lighthouse Ext. Cons.

Log Sheet: Recent Scenarios 2017

Date	Time	Information / Decisions / Actions	Initials
15th May 2017	08.00	RansomWare and Your Servers. The WannaCrypt ransomware worm, aka WanaCrypt or Wcry, this weekend exploded across 74 countries, infecting hospitals, businesses including FedEx, rail stations, universities, at least one national telco, and more organizations. In response, Microsoft has released emergency security patches to defend against the malware for unsupported versions of Windows, such as XP and Server 2003, as well as modern builds. To recap, WannaCrypt is installed on vulnerable Windows computers by a worm that spreads across networks by exploiting a vulnerability in Microsoft's SMB file-sharing services. It specifically abuses a bug designated MS17-010 that Redmond patched in March for modern versions of Windows, and today for legacy versions – all remaining unpatched systems are therefore vulnerable and can be attacked. This bug was, once upon a time, exploited by the NSA to hijack and spy on its targets. Its internal tool to do this, codenamed Eternalblue, was stolen from the agency, and leaked online in April – putting this US government cyber-weapon into the hands of any willing miscreant. Almost immediately, it was used to hijack thousands of machines on the internet. Now someone has taken that tool and strapped it to ransomware: the result is a variant of WannaCrypt, which spreads via SMB and, after landing on a computer, encrypts as many files as it can find. It charges $300 or $600 in Bitcoin to restore the documents. It is adept at bringing offices and homes to a halt by locking away their data. And it installs Doublepulsar, a backdoor that allows the machine to be remotely controlled. That's another stolen NSA tool leaked alongside Eternalblue. The malware is also controlled via the anonymizing Tor network by connecting to hidden services to receive further commands from its masters. **Lighthouse IT – What have we done to protect you?** If you are on our 24/7/365 remote server monitoring and fix premium support then your servers will have already been patched when Microsoft released the patch. We have spent the weekend manually patching customers that are not on the premium support and double checking that all servers have the latest patches from Microsoft. On Friday Microsoft released an additional patch for the ransomware this will have also been applied to your servers over the weekend.	

		What should you do? At this point in time none of our customers have been affected by the ransomware. However, on Monday your staff will be back at work. You should advise all staff not to open any emails they don't recognise. Especially things like delivery updates from DHL etc. Staff should not open any attachments they are not expecting, additionally they should not click on any links in emails. Be extra vigilant this week as new variants of the ransomware will be released which Microsoft or your Antivirus supplier may not yet be aware of. If you really need to check any email they you don't recognise do so on your mobile phone. **Backups** Backups can be encrypted by the ransomware as well, if you currently backup to external hard drives please ensure that they are disconnected from the network the following morning when the backup is complete that way if you do get hit the backups cannot be over written. **Reporting** Please report any suspicious emails or activity to the helpdesk straight away via support@lighthouseit.co.uk or 0207 915 8318.	
14th Mar 2017	11.22	Fire Alarm • In a recent Live Fire test our priority was to ensure the safety of our workforce and the general public, through co-ordination with the relevant emergency services. • Once we are satisfied that all parties were safe and the disaster / event was over we aimed to assess the damage to our business premises as soon as possible, (On this occasion it was a neighbouring property) we quickly put together specific contingency plan to put our services back on track. • If the disaster had damaged the building, we would have gone through the proper DRP channels without insurers to identify costs, and put works back on track. • We would have closely liaised with clients to inform them of revised timescales, or whether it is still possible to finish works as planned.	
11th Dec 2017		Flooding / Heavy Snow (Extreme Weather) • Due to the rapid and heavy snow accumulation in December, a number of Council / local authorities advised travel only if absolute necessary. Many roads remained impassable, and the West Midlands public transport system was incapable of transporting its usual daily commuters. For Interclass our	

		telecommuting became a vital option that allowed senior management staff to avoid a complete shutdown, by working at home, while keeping our employees off of clogged or dangerous roads. However, for telework to be successful, Interclass needed to plan ahead by identifying telecommuting strategies such as VPN and remote access, Interclass have put in place and I/T structure to support this program. We are pleased to announce it worked very well without any major issues. **A full Report can be provided if required**	

BCP

The **Interclass** Group Business Continuity Management Plan

Company Overview

Premises

Interclass Office premises – rented office space consisting of a two storey office block with parking fronting Heathmill Road, Wombourne, West Midlands, WV5 8AP

All support and back office functions are carried out from Head office.

Business Interruption Insurances are carried out from Head office

Business Interruption Insurances is in place for £100,000 increased cost of working cover with indemnity period of 12 months. Current rent cost of £37,600 p.a

Company Data and Networks

Data servers are secured in separate room within Head Office and consist of:

- MS Exchange server for network data and accounts system and data Virtual Servers are used where possible
- Data is exchange is over a SLA backed leased line
- Email are filtered externally before reaching our internal systems
- Storage of backups are taken out of the office premises to ensure they are not destroyed in the event of a fire.
- Data back-up is monitored remotely to ensure back-up information is complete and reusable.
- Regular Virus updating of all IT hardware including site based apparatus to ensure we optimise our virus protection and malware protection
- Servers are monitored 24/7/365 by our IT provided with engineers across three different time zones.
- A written IT Policy defining unacceptable misuse of IT equipment to minimise the risk of staff downloading malicious files / viruses.
- Key staff have mobile and land line telecommunications
- Back-up procedures are enforced and data copies are removed from site on a daily basis with minimum of two weeks data held on tape.
- The IT network is supported by external consultants who provide a duplicate hardware system in the event of partial or total loss within 48 hours to replacement premises

Operational staff are provided with laptop computer and smart phones to enable them to operate remotely.

Business Systems

Interclass operate ISO 9001 accredited business procedures and processes across all our projects, ensuring continuity in how information is recorded, stored and shared, both in hard and soft copy, between team members on a specific project and across all our projects. This enables easy accessibility to information and for personnel from one team to support another, should a team member be unavailable.

Assets

Plant, machinery and vehicles can be hired from the Company approved supply chain as and when required.

Supply Chain

Our supply chain provides our project teams with a selection of vetted and approved subcontractors and suppliers for all trade, material and plant requirements. In the event of a failure of a supply chain partner, we are able to substitute other suitably experienced and qualified business.

Industrial Action / Mass Resignations / Loss of Staff

The Interclass Group have assessed the risk of mass industrial action / staff walk out as extremely unlikely, especially for key management staff, given our low staff turnover and ‘open’ communication culture which encourages early resolution of any dissatisfactions or staff problems. We also recognise the importance of holding regular Personal Development Reviews to sustain employee motivation.

We recognise that any action that affects all employees, such as pay cuts or redundancies, must be carried out with appropriate consultation and recognition of their rights and relevant legislation.

Signed on behalf of **The Interclass Group**

20th December 2017

Dave Jones – Director of Health & Safety, Managing Director

The Interclass Group Wolverhampton

Review Date: **2nd January 2019**