MCS Control Systems
Disaster Recovery / Business Continuity Planning Policy

This document is to be used in conjunction with SF197 - Business Risk Register.

1. General

We recognise the latest revision of ISO22301, the business continuity management standard and in accordance with this standard the latest revision of ISO22313, we have developed this Disaster Recovery or Business Continuity Planning Policy.

This policy is to be utilised in accordance with our Security Measures Policy (SF260) and SWP90 Employment Human Resources Competence & Training.

Disaster Recovery (DRP) or Business Continuity Planning (BCP) is a business function that details the measures required to restore infrastructures and services following disruption or disaster.

A well-structured and rehearsed disaster recovery plan provides the peace of mind that if the worst really does occur, steps are already in place to turn what would be a major disaster into a minor inconvenience.

The key objective is to minimise the impact that such an event will have on the business.

2. Planning for Disaster

A well thought out DRP/BCP is built around the requirements and circumstances of an individual business, as well as the potential damages and degree of risk and exposure that their IT infrastructures are exposed to.

The advantages of a DRP/BCP:

- Ability to maintain, or resume, operational trading
- Safeguarding reputation, brand and image
- Reducing downtime through the mitigation of disasters
- Prevent loss of customers to competitors due to inability to trade
- Increase confidence of associates, clients, investors and business partners.

3. Developing a Disaster Recovery / Business Continuity Plan

An effective DRP/BCP can be achieved by carrying out the following five steps:

- Identify the core elements of the company
  - including finance, business processes, human resources and information technology
  - Assign monetary values for each asset or element using an Annual Loss Expectancy (ALE) calculation - multiplying the potential frequency of a disaster occurring by the expected sterling (GBP) loss per instance
- Prioritise these areas
  focusing on those directly affecting the bottom line
  Assign responsibilities for each of these areas to suitable personnel
- Define what customers, suppliers and stakeholders expect, particularly in terms of contractual obligations
  Conduct 'what if' scenario planning to determine suitable responses for various disasters or emergencies (anything that can destroy or render resources or data inoperable is a potential disaster)
- Communicate the strategy throughout the company
  ensuring the necessary resources are adequately prepared.
  Test and review the strategy at least annually or as significant internal changes occur
- Endeavour to integrate this planning and control process into every element of business planning and operation
  allowing DRP/BCP's to grow in step with the business and its changing requirements

4. Document Systems

- Define the disaster - Think of what will be the most painful event the organisation could survive.
- Get an understanding of the systems in place
  An inventory of hardware, software, business systems, and all the interactions the systems enable.
  What part of the technology is critical to operations?
- Documentation is critical
  Make a simple chart of the systems used. How they are installed, where the installation CDs are located, how they are backed up and how to get support.
- Standardise all of the desktops!
- Document the exceptions.
- Store all the data on the servers!
- Document everything!
- No exceptions.

5. Backing up Systems

Once you have defined the disaster and got an understanding of your systems, you should then ask yourself:

- Which systems are critical?
- How are the systems backed up?
- How are the systems recovered?
- Where is our data stored?
- Is all of it backed up regularly?
- How are backups documented?
- Where are the backup tapes stored?

6. Support

It is a good idea to work with a specialised disaster recovery firm for off-site assistance.
If an emergency were declared, a whole team of people would spring into action, rebuilding the infrastructure, restoring backup tapes, and restoring business operations.

7. Cross Reference

This document is to be used in conjunction with the ISO9001 requirement relating to the Context of the Organisation as referenced within the SHEQM - Integrated Management System - Safety Health Environmental & Quality Manual. Reference should also be made to IMS SHEQ Procedures SHEQP 04 - Planning - Actions to assess risk associated with threats & opportunities and SHEQP 05 - Significant Environmental Aspects & Actions, along with standard forms SF094 - Environmental Aspects Impacts & Significance and SF094 - Environmental Aspects & Impacts Register and Significance.

This policy will be kept up to date, the policy and the way in which it has operated, will be reviewed every year.

Signed:

Name: Stephen Poole **Position:** Group Managing Director

This Policy Statement will only be signed on the original copy (available upon request)

Date Issued: 15/02/18 **Review Date:** 03/01/19

Total Loss – Catastrophic Disaster				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
All	Complete Business Destroyed	All buildings, contents, Work in Progress, Information Technology and Documentation	• We would need to source new premises for the Administration, Engineering and Production process. • Server hardware would need to be replaced, probably from a local supplier. At a pinch we could run all functions on a single server (albeit without any resilience). Operating systems & applications would need to be installed before re-installing the data from backup. Note the previous night's backup would be amongst the debris of the old server so we would lose at least a day's work, possibly more if the disaster occurred on a Sunday (i.e. we would lose Friday & Saturday). OGL would be heavily involved in this. • A number of employees could work from home if a VPN link is established. • We could purchase new PC's from a local shop (they wouldn't be Dells) and install the relevant software. • Data would be restored from backups. If any data is in hardcopy format only within project files we would have to request replacements from clients. Some hard copy data will be irretrievable. • CAD Software could be initially installed on desktops. We would probably be unable to get CAD up to full strength using this method. • Software for clients/projects is saved within the software repository on servers, which is backed up daily. This could be restored from backups, but we would also need to reorder from manufacturers. • Any work in progress would be lost. Steelwork would need to be re-ordered. Depending on the quantity and size of projects in build at the time and this will take several weeks for all deliveries. We might need to consider using additional steelwork suppliers if necessary to overcome the problem of overloading existing suppliers. • New materials would need to be sourced from suppliers. Previous purchase orders would be available from the back-ups. All would need to be re-ordered. Depending on the quantity and size of projects in build at the time deliveries will take several weeks. Consider using alternative/additional suppliers to help lead times. All consignment stock such as cable and crimps would be destroyed so would also have to be re-ordered. Additional resource would probably be required to assist with sourcing and procuring materials. Some materials are free issued by clients and would need replacing. • Production Dossiers and drawings issued to the shop floor would need to be reprinted from electronic copies stored on server unit 6. Any mark-ups on drawings will be lost. • Plant & Equipment including Power Tools & Test Instrumentation would be lost, including power supplies for the testing of the panels This could be restored quickly and we would be able to continue with battery powered drills, saws etc. • All archived materials in paper files contained in cardboard boxes would be lost. Attempt to obtain as much information as possible from electronic back-ups.	Timescales could vary, but potentially 1 -12 weeks

Engineering - Work-in-Progress, Fixtures & Fittings				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
All	Offices	Workstations	See section relating to Information Technology disaster recovery. Replacement Licences for AutoCAD and Promis-e would need to be obtained from Autodesk.	Up to 1 day
4	Offices	Project design information and project folders	Mostly stored on the server in Unit 6. If any data is in hardcopy format only within project files, we would have to request replacements from clients. Some hard copy data will be irretrievable.	Up to 1 week
All	Offices & SCADA room	Client hardware (on engineers desks)	Could be PC's, server, HMI's or PLC's. Would need to be reordered.	Timescales vary
All	Servers	Domain Controller, Mail server, main file server, CAD server	See section relating to Information Technology section.	1 day
6 & MCSN	Offices	Project design information and project folders	Data would be restored from backups. If any data is in hardcopy format only within project files we would have to request replacements from clients. Some hard copy data will be irretrievable	Up to 1 week
All	Offices	Manufacturers Technical Catalogues and data	A lot of these are stored electronically on the server in unit 6, otherwise can be downloaded, or request new catalogues from suppliers.	Timescales vary – up to 1 week
Production - Work-in-Progress, Fixtures & Fittings				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
All	Documentation	Production Dossiers and drawings issued to the shop floor	Reprinted from electronic copies stored on server unit 6. Any mark-ups on drawings will be lost.	1 day
All	Shop Floor - Material	MCC steelwork	Steelwork would need to be re-ordered. Depending on the quantity & size of projects in build, this will take several weeks for all deliveries. We might need to consider using additional steelwork suppliers if necessary to overcome the problem of overloading existing suppliers.	Timescales vary – 2 -12 weeks
All	Shop Floor - Material	Enclosures including internal components, cables, trunking etc	Due to fire, heat & smoke damage any of the components fitted in the panels would be lost. The rubber seals would be lost and much of the door mounted equipment would have melted, therefore the panels would offer no IP Rating.	Timescales vary – 2 -12 weeks
All	Shop Floor - Material	General Production Materials	Would need to be re-ordered. Depending on quantity& size of projects in build at the time, deliveries will take several weeks. Consider using alternative/additional suppliers to help lead times. All consignment stock such as cable & crimps would be destroyed and would also have to be re-ordered. Additional resource would probably be required to assist with sourcing and procuring materials. Some materials are free issued by clients and MCS would have to replace these also.	Timescales vary – 1 to 6 weeks
All	Plant & Equipment including Power Tools & Test Instrumentation	All would be lost, including power supplies for the testing of the panels.	This could be restored quickly and we would be able to continue with battery powered drills, saws etc	1 week
4	Radiant Tube Gas Heaters in roof space Gas Mains pipe runs through the middle of unit 4	Much of the structure of the building I think would remain, dependant on the material in the roof space that may be lost	Dependant on the severity and location of the fire we may be able to use some of the steelwork, maybe the frames (if they are not buckled under the heat) Some of the doors may be able to be recovered and re-painted, again dependant upon the damage caused to them.	1 – 12 Weeks, this would depend on suppliers being able to deliver the required amount of materials, this may need to be divided into a number of suppliers

Stores - Materials, Fixtures & Fittings				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
4 & MCSN	Goods Inwards. Most of the components are held in cardboard packaging	Components & Materials	Re-order all materials lost	1 – 4 Weeks for Consumables and standard control gear. Delivery times would have to be obtained with regard to longer delivery items.
4 & MCSN	General Stores	The collapse of the wooden roof and the effects of a fire would result in all stock being lost.	With the result of the damage to components and the safety implications with using the materials We don't believe we would be able to recover any stock. All essential materials, components and equipment will need to be re-ordered.	Re-order of all materials, delivery schedules of 1 – 10 weeks dependant upon the equipment needed.
4	Pick / Consumables Stores	The collapse of the wooden roof and the effects of a fire would result in materials in the stores being lost,. These are all consumable items, such as cable ties, crimps, cable markers and nuts, bolts etc.	With the result of the damage to components and the safety implications with using the materials, we don't believe we would be able to recover any stock. All essential materials, components and equipment will need to be re-ordered. Many nuts, bolts and other fixings may be useable.	Timescales vary – 1 to 6 weeks
4	Cable Stores	The collapse of the wooden roof and the effects of a fire would result in all stock being lost, owing to the destruction of all outer sheathing.	With the result of the damage to components and the safety implications with using the materials, we don't believe we would be able to recover any stock. All essential materials, components and equipment will need to be re-ordered.	Timescales vary – 1 to 6 weeks
6	Bonded Stores	The majority of the components held in the Bonded Stores are plastic or the housings are plastic, therefore, due to heat we would loose most if not all of the stock.	With the result of the damage to components and the safety implications with using the materials, we don't believe we would be able to recover any stock. All essential materials, components and equipment will need to be re-ordered.	1 – 2 Weeks. This is bonded stock & does not belong to us until we use it, insurance issues may lie with the supplier.
6	Archived materials are currently kept above unit 6 in paper files contained in cardboard boxes	All paperwork would be lost.	Attempt to obtain as much information as possible from electronic back-ups.	Unknown, dependant on any electronic back-ups

Information Technology				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
All	CAD workstations	CAD Software	CAD Software could be installed on desktops in Unit 6. We would probably be unable to get CAD up to full strength using this method.	½ day
All	CAD workstations	CAD PC's	We could purchase new PC's from a local shop (they wouldn't be Dells) and install CAD software as above.	1 day
All	Other workstations	Computers	Users could either share existing workstations in other parts of MCS Coventry or MCS North, dependant on location, or we purchase some new PC's as above	Up to 1 day
All	Engineers desks & SCADA room	Client hardware	Could be PC's, server, HMI's or PLC's. Would need to be reordered.	Timescales vary
4	Reception	Switchboard	Would need to source new (or used) switchboard, help from HBT required. Incoming BT lines may also have been destroyed.	Up to 2 weeks
6	Sales & Accounts	Workstations	Users could either share existing workstations in Unit 4, or we purchase some new PC's as above	Up to 1 day
4	Hardware	SI Kits	Reorder from manufacturer (most new SI kits are now on the Archive Server)	Timescales vary
4	Software	Software cupboard (We don't know how long this would last in a fire)	Assuming contents are destroyed	Never
4	Software	Software for clients/projects	All information is saved within the software repository on servers in Unit 6, which is backed up daily and stored off site in the fire safe. We would need to reorder from manufacturer	2 hours
4 & MCSN	Software	Archive disks for old projects, SAD, MCSIS, MCSD	Some of these can be re-created from Archive Server (old projects, SAD), others (MCSD, MCSIS) will be irretrievable	Up to 1 week (or never)
Information Technology Systems				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
6 & MCSN	Servers	Domain Controller, Mail server, main file server, CAD server	Server hardware would need to be replaced, probably from a local supplier (not Dell). At a pinch we could run all functions on a single server (albeit without any resilience). Operating systems & applications would need to be installed (stored in fire safe) before re-installing the data from backup. Note the previous night's backup would be amongst the debris of the old server so we would lose at least a day's work, possibly more if the disaster occurred on a Sunday (i.e. we would lose Friday & Saturday). HBT would be heavily involved in this.	1 day
6	Servers	Accounts server	The hardware would need to be sourced from a local supplier and must be capable of running SCO Unix (Intel or compatible should work). Multisoft software is in the fire safe along with the backups. We do not seem to have SCO Unix. Note that the previous night's backup would have been destroyed along with the server, so we would lose at least a day's work. Note that Multisoft is now obsolete, we have a support contract with a company called TBSL, but they only support us on a "best can" principle (we may never be able to restore the server)	2 days (or never)
6	Servers	Archive Server	The hardware would need to be sourced from a local supplier (not Dell). Old projects can be restored from disks which are stored in the software cupboard. This server also runs the Timeware software which would need to be re-installed.	3 days
6	Servers	Off Site Back-Ups	All information is saved on servers in Unit 6, backed up daily and stored off site in the fire safe. In the unlikely event that we should we lose both buildings then there would be a problem.	Immediate solution

Information Technology Systems (continued)				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
6	Servers	Email server	If we have no e-mail server, ADSL line or router then it should be possible to redirect e-mail to another location (possibly HBT) where it could be picked up remotely (if have an Internet connection), or by someone based at HBT's offices.	Immediate solution
4	Infrastructure	Network Infrastructure	It is possible that the ADSL lines come into unit 4 and these may have been destroyed. Will require BT to move lines to Unit 6. The telephone system is all stored on the computers and all key employees have mobile phones, therefore the communication links would not be lost.	Immediate solution for computer back up and mobile phones. Up to 2 weeks for BT.
6	Infrastructure	Network infrastructure	It is possible that the ADSL lines come into unit 6 and these may have been destroyed. Will require BT to move lines to Unit 4. E-mail & Internet routers will need to be replaced. Should be able to source locally or from HBT.	Up to 2 weeks
MCSN	Infrastructure	Network Infrastructure	ADSL router will have been destroyed and will need to be replaced. Should be able to source locally or from HBT.	1 day
MCSN	Infrastructure	ADSL lines may also have been destroyed	If office is to be relocated then this is not a problem, otherwise in the hands of BT.	Up to 2 weeks (or NA)
4	Firesafe (guaranteed for 2 hours in the flames)	All contents, if total destruction	Irretrievable	Never
All	Back up	Nightly backup tapes for fileserver, CADserver & e-mail	All information is saved on servers in Unit 6, which is backed up daily and stored off site. Recreated during the following night's backup	2 hours
All	Back up	Nightly backup tapes for accounts server	All information is saved on servers in Unit 6, which is backed up daily and stored off site. Recreated during the following night's backup	2 hours
All	Back up	Backups going back 6 months for fileserver, CADserver & e-mail	All information is saved on servers in Unit 6, which is backed up daily and stored off site. Recreated during the following night's backup	2 hours
General Business Continuity				
Unit	**Area**	**What we would lose**	**How we would recover**	**Estimated recovery time**
All	Human Resource Changes mid-project	Continuity of work, leading to customer dissatisfaction and ultimately losing out on future business with the client	Refer to the Integrated Management Procedure SHEQP 10 - People Competence & Awareness, under the section Human Resources Changes	Up to 1 day
All	Employee Fatality	Continuity of work, leading to customer dissatisfaction and ultimately losing out on future business with the client. This would be due to the HSE shutting us down for a time period.	We would need to inform our customers of the issue, see if we can continue to build in other areas of the business or rent premises to continue the process. When up and running, we will need to accelerate the process and maybe work additional overtime, or employ agency labour, to see us through the shutdown period.	
All	Suppliers	Continuity of work, leading to customer dissatisfaction and ultimately losing out on future business with the client	We have considerable experience in the industry and have developed a database of the standard products used in the production of control panels and systems integration, which is included within our bespoke ERP system. This is updated at regular intervals to ensure that we are constantly abreast with the latest products, providing the latest technologies at the best value for money for our clients. The ERP product database, utilised on all projects, provides continuity throughout all processes. Unless in exceptional circumstances, we will always endeavour to have more than one supplier of essential products, to ensure that if a product is not available from a particular supplier, we will always have a back-up, ensuring continuity of the project. This is reflected within our supplier base on the ERP.	Up to 1 day

Notes & Assumptions

- **NB.** Water damage caused by the Fire Service in tackling the fire, has not been included in the assessments.
- It is assumed that anyone who has a laptop will have it with them when disaster strikes and they would therefore not need to be replaced.
- The versions of Microsoft Windows and Microsoft Office installed on our machines are OEM versions, which means the licenses are not transferable to another machine. If we purchase new machines we will also need to purchase Windows and Office.
- Timescales assume we could get any hardware from a local supplier straight away and that 1 day = 24 hours (not an 8.5 hour working day)
- We currently have support contracts with the following companies:
    a. HB Telecomm
    b. OGL Computers
    c. Wisegrove (Timeware)
    d. TBSL (Multisoft)