Business Continuity Plan

Version 2016.2

Emergency Notification Contacts

In the advent of a disaster please immediately inform the appropriate contact from the list below.

Disaster Type	Affects	Name	Position	Mobile
Fire	Premises	Roger Ingram	Properties Mgr.	07894546123
Fire	Server/Comms room	John Prior	IT Manager	07899922759
Flooding	Premises	Roger Ingram	Properties Mgr.	07894546123
Electricity	Lights/Sockets	Roger Ingram	Properties Mgr.	07894546123
Gas	Heating	Roger Ingram	Properties Mgr.	07894546123
Water	Heating	Roger Ingram	Properties Mgr.	07894546123
Communications	Land Line Phones	John Prior	IT Manager	07899922759
Communications	IT Systems	John Prior	IT Manager	07899922759

Notification of any incident above **must** also be given to:

Ben Staff 07899922760

Tom Church 07771907592

Other Useful Contacts

Department/Company	Affects	Name	Phone
Properties	Utilities	Ian Coombs	07747694166
IT	IT Issues	IT	01249652511 (option1)
Protel	Land Line Phones	Office	01179864777
WestgateIT	Computer Systems	Office	01225636270
Smart Integrated	CCTV (Site)	Office	01249309519
Smart Integrated	Alarms (Site)	Office	01249309519
Mayhead Electrical	Electrician	Danny Mayhead	07971684524
Southern Communications	Land Line phones and Comms Lines (Not Lease Lines)	Office	01256391046
BT	Comms (Lease Lines)	Office (BT Local Business)	01454 278566

The purpose of this document is to provide procedures to follow to restore normal business operations in the event of an emergency. Extended service outages are included in this plan. In order to recover from an emergency as rapidly as possible all MJChurch employees should familiarise themselves with this plan. The procedures within apply to all MJChurch sites and operational facilities.

This plan is reviewed on a regular basis and employees are expected to regularly check for updates.

This plan is not intended as a daily problem resolution document. The scope of this document is to provide a plan for all identifiable disasters and provide procedures and resources required to assist in the recovery.

A national disaster such as a nuclear explosion is beyond the scope of this plan.

Objectives

- Provide procedures to follow to assist in recovery for MJC recovery teams
- Identify service suppliers that need notification in the event of a disaster
- Remove confusion experienced during disasters by planning and testing procedures beforehand
- Provide relocation plans for staff
- Identify the location of critical data and provide locations of backup systems

Assumptions

- Availability of key personnel in the event of a disaster
- The readiness of the appropriate key service suppliers to deal with such an emergency. Each service supplier should have its own plan to follow to deal with emergencies
- This document is available following an emergency. Accessible copies of the latest version of this document are to be kept on all sites.
- Activation and adherence to any other MJChurch policy/procedure relating to the evacuation of staff in an emergency

MJChurch Disaster Recovery Teams

- Emergency Management Team (EMT)
  Ben Staff, Tom Church, Steve Blower

- Site disaster recovery teams (DRT)
  Star Farm: Phil Jones, Nigel Hampton, Rachel Hutchins, Karl Wintle, Sam Wilson, Stewart Liddell

Saltersford: Michele Hall-Barnett, Ann Kyte
Greens: Sam Henly, Tom Nelson

- IT services team (IT)
  John Prior

Each member of the team must keep an up-to-date calling list of their fellow team members on their phones and at home. All team members must keep a copy of the latest version of this plan both at home and at work.

The teams must be aware of or have immediate use of keys for access to all areas at all appropriate sites. Each member of each site team must also be made aware of the service supply locations for each site.

Specific Roles of the EMT

- Declare a disaster
- Evaluate and activate if necessary the appropriate DRT
- Set restoration priorities based upon the damage assessment reports
- Provide senior management with ongoing status information
- Coordinate communication to department heads and major customers
- Work with the Properties department and IT to develop a coherent business restoration schedule

Instructions for use of this plan

A disaster is considered as a loss of utility service (electricity, water), connectivity or catastrophic event, however caused, that prevents the business operations from functioning at any single or multiple MJChurch site(s).

In the advent of a disaster this plan will remain in effect until normal operations are resumed at the affected site(s).

Upon observation or notification of a potentially serious situation during working hours at a site ensure that the EMT have been notified.

The declaration of a disaster and the invocation of this plan is the responsibility of the EMT team, however should a member of the EMT not be contactable then the relevant DRT site team along with the IT team should make the decision.

Notification must be made to the EMT in the advent of the following:

- Two or more software systems (EvolutionM, Syrinx, Weighsoft5) are down concurrently for more than three hours whether planned or not.
- Any one of the above software systems is down or planned to be down for more than six hours.
- The network is down for more than three hours.

- The phone system is down for more than 4 hours.
- A planned service withdrawal has not been adequately provided for or has been extended beyond the original duration.

Alternate Locations

Should access to a building or site be denied, MJChurch staff should report to their emergency site contact for further details on where to report. The emergency site contact details are:

Site	Name	Mobile	Home
Star Farm	Derek Pullin	07786311886	
Star Farm	Rowan Adams	07876757808	
Saltersford	Jon Clarke	07799435592	
Saltersford	Michele Hall-Barnett	07469859960	
Greens	Tom Nelson	07502457476	
Greens	Sam Henly	07920752687	
Braydon	Dave Marriott	07818373936	
Braydon	Pete Ody	07827158593	
Marshgate	Jack Chaplin	07766003373	
Marshgate	Sue Jefferies	07568395175	
Warmley	Glen Whitham	07584303726	
Warmley	Chloe Buckle	07561577788	

Validating the Process

A disaster can occur at any time. Training of key personnel and validation of the processes involved is essential if resolution of normal business operations is to be restored in a timely manner. This involves regular testing of the Business Continuity plan. There are two types of tests

- Live planned scenarios
- Simulated meeting based exercises

The Live scenario, whilst providing the best learning experience for the staff involved, is likely to be the most disruptive and costly for the company. The use of planned simulated exercises can help prepare the appropriate staff for a live event.

An IT Disaster Recovery (DR) failover test can be done on a regular basis and will have minimal impact to the business, however this will only provide training for IT related issues and personnel. DR testing should be done on a regular basis and should be considered as a separate exercise.

A live planned test will enable observers to see what the staff actually do. A simulated meeting based exercise will involve staff saying what they would do without considering whether their actions would be feasible given the circumstances.

IT Systems and backup policy

The IT department provides appropriate backup solutions for all main software applications. Data is backed up regularly and off site backups are kept. All server and communication systems equipment is kept locked away to prevent loss of service through vandalism and theft and also to provide data protection for both company and individuals data.

Software backup systems

MJChurch main software systems are kept at multiple sites. Should a disaster occur in the main server room an alternate server at another location can and will be activated. Users will not need to have their individual machines reconfigured. There will however be some downtime due to the reconfiguring and commissioning of the software systems at the alternate site.

To achieve this replication backups of the main servers are made and sent to the alternate site every hour.

Data Backup Policy

Full and incremental data backups are kept. Off site backups of the main servers at Star Farm and Saltersford are kept at Greens. On site backups are also kept on site to aid in the quick restoration of data should an incident occur on site resulting in the loss of data.

The data for the main software systems is held on SQL databases. Backups of each of these databases are regularly made at least three times a day.

Department specific data is held at each of the three main sites (Star Farm, Saltersford and Greens). Each department is responsible for ensuring what records must be maintained and for how long.

Phone Systems

Although the main phone system operates across all three main sites each individual site has its own system. Therefore any loss of service at any site will not affect any other site.

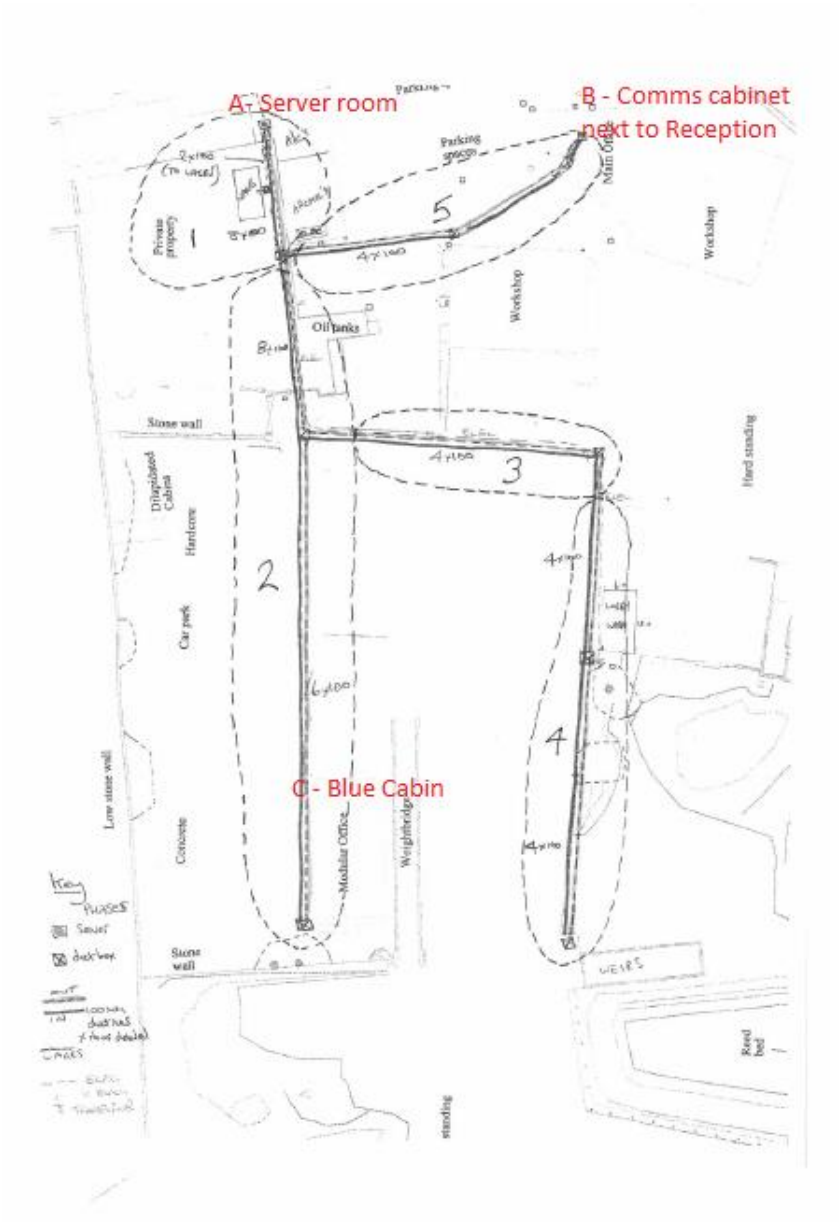
MJChurch utilise the ‘Business Continuity’ service offered by Southern Communications. Should a disaster occur this service provides for a virtual receptionist coupled with a hunt

group which will allow for any incoming calls to an affected site to be rerouted to appropriate mobile numbers or to land line numbers at another site.

Networks

All sites have alternative data lines for access to the internet which can be utilised should the main connection to the site go down. A second alternative line is also available at Star Farm which will enable the network to continue to function should there be a fire in the main server room.

Star Farm has also got multiple fibre lines installed between the buildings to allow for rerouting should it be required.



Fibre Installations:

A – B 1 x 12 core
A – C 1 x 12 core
B – C 1 x 8 core

Network cabling within the cabinets takes follows the form of Red cables for POE (mainly land line phones ports) and Blue cables for data (mainly computer ports).

UPS – Battery backup

Should MJChurch suffer a loss of power UPS supplies are installed at all sites and are sufficient for approximately one hour of supply. Battery backup is supplied to maintain the network, servers, phone systems, CCTV camera systems and weighbridges. Some desktop computers, in vital areas of the business, are also connected to UPS supplies. Many MJChurch employees work using laptops to provide continual service if power is lost and also to allow for quick relocation should the need arise.

Generator Requirement if power is lost

If power is lost a generator can be obtained from:

Power Electrics, St Ivel Way, Warmley, Bristol BS30 8TY Tel: 03708500858

For Star Farm a 200KVA Diesel Generator will provide enough power for the site providing the workshops are careful on their use of power. The generator will need to be located on the Accounts car park. The output of the generator can be wired into the main electric supply board in the building next to the car park. The electrician Danny Mayhead has knowledge and experience of doing this – his contact details are given earlier in this document.

Saltersford site has also been powered via a 200KVA generator. A generator of this size should be sufficient for Greens. Remember to provide adequate access to diesel fuel to power the generator.

In the event that a fire at Star Farm that affects the workshop with the main electrical supply three separate generators will be required. One to be situated next to reception to power the main office building. One will need to be situated next to the weighbridge to power the blue cabin. The remailing one will need to be located next to the transport workshop to power both the transport and plant workshops and also the lorry wash.

Emergency Management Procedures

There are four main types of disaster which affect:

- Premises – Fire, Natural disaster
- Utilities – Electric, Gas, Internet Connectivity (including phones)
- Technology – Software, Hardware, Network
- People – Major accident, pandemic, loss of key personnel, industrial action

The following procedures are to be followed by all EMT, DRT, IT and any other designated MJChurch personnel in the event of an emergency. Where uncertainty exists the more reactive action should be followed to enable maximum protection and personnel safety.

Subject to the type and severity of the emergency any non-essential staff may need to be asked to vacate the area.

Natural Disaster – flooding, earthquake, storm, lightening strike or similar event

Can be one of two types:

- Natural disaster with forewarning
- Sudden disaster with no forewarning

Impending natural disaster with forewarning:

Step	Action
1	Notify all EMT, DRT, IT teams
2	Identify the risks to resources and operations
3	Plan for the risks involved – to include: • Power supply provision – is a generator required? • Organise for the relocation of affected staff and IT equipment If the site to be affected is Star Farm: Bring up the backup server at Saltersford Organise for the relocation of Accounts staff to Saltersford and Waste Management to Greens. Plant and Transport staff may also need to move however backup connectivity exists at Star Farm. Some staff may be able to work from home so as to reduce the demand of valuable desk space. If the site affected is Greens: (if required) Deploy all office staff to Star Farm Organise for the redeployment of site workers appropriately If the site affected is Saltersford: (if required) Organise for the deployment of all staff to both Star and Greens sites • Dependent upon the disaster type and location move IT equipment, paper records and any other affected items away to a safe area • Remember to check stock on useful items such as: batteries, rope, flashlights, medical items, hard hats, protective clothing etc.…

	• If a team of staff is to remain on site during the disaster plan for their food and facilities • 24hrs before the disaster – verify backup generator fuel status and operation, fuel designated emergency vehicles, notify senior management. If the site to be affected is Star Farm activate the backup server at Saltersford. Check user's connectivity to this server.
4	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
5	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
6	Regularly review the situation and restore services as soon as possible
7	Conduct a damage assessment – see appendix A
8	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
9	Recovery Phase
10	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Natural Disaster with no forewarning:

Step	Action
1	Notify all EMT, DRT, IT teams
2	Plan for the situation involved – to include: • If the site affected is Star Farm activate the backup server at Saltersford • Power supply restoration (if lost) – is a generator required? • Organise for the relocation of affected staff and IT equipment If the affected site is Star Farm: Bring up the backup server at Saltersford and make changes to the DNS settings. Organise for the relocation of Accounts staff to Saltersford and Waste Management to Greens. Plant and Transport staff may also need to move however backup connectivity exists at Star Farm. Some staff may be able to work from home so as to reduce the demand of valuable desk space. If the site affected is Greens: (if required) Deploy all office staff to Star Farm Organise for the redeployment of site workers appropriately If the site affected is Saltersford: (if required) Organise for the deployment of all staff to both Star and Greens sites • Dependent upon the disaster type and location move IT equipment, paper records and any other affected items away to a safe area • Check stock on useful items such as: batteries, rope, flashlights, medical items etc.… • If a team of staff is to remain on site during the disaster plan for their food and facilities

3	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore services as soon as possible
6	Conduct a damage assessment – see appendix A
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Fire in Offices

Step	Action
1	Evacuate the affected site if the fire still active
2	Contact Fire brigade if not already done
3	Notify all EMT, DRT, IT teams
4	Plan for the situation involved – to include: • Complete a safety check of the site • Power supply restoration (if lost) – is a generator required? • Organise for the relocation of affected staff and IT equipment appropriately • If a team of staff is to remain on site during the disaster plan for their food and facilities
5	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
6	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
7	Regularly review the situation and restore services as soon as possible
8	Conduct a damage assessment – see appendix A
9	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
10	Recovery Phase
11	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Fire in Server/Comms Room

Step	Action
1	Evacuate the affected site if the fire still active
2	Contact Fire brigade if not already done
3	Notify all EMT, DRT, IT teams
4	Plan for the situation involved – to include: • Complete a safety check of the site • Power supply restoration (if lost) – is a generator required? If the affected site is Star Farm: Bring up the backup server at Saltersford and make changes to the DNS settings. If the fire has affected the Accounts offices organise for the relocation of Accounts staff to Saltersford • Organise for the relocation of any affected staff and IT equipment appropriately • If a team of staff is to remain on site during the disaster for security plan for their food and facilities
5	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
6	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
7	Regularly review the situation and restore services as soon as possible
8	Conduct a damage assessment – see appendix A
9	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
10	Recovery Phase
11	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Water Supply

Step	Action
1	Contact Water Supply company if not already done
2	Notify all EMT, DRT, IT teams
3	Plan for the situation involved – to include: • Complete a safety check of the site • Organise for temporary replacement heaters if required • Organise for temporary toilet facilities to be installed on site • Organise for the relocation of any affected staff, vehicles and IT equipment appropriately if required

	• If a team of staff is to remain on site during the disaster for security plan for their food and facilities
4	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
5	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
6	Regularly review the situation and restore services as soon as possible
7	Conduct a damage assessment if required – see appendix A
8	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
9	Recovery Phase
10	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Power

Step	Action
1	Contact the Power Supply company if not already done
2	Notify all EMT, DRT, IT teams
3	Plan for the situation involved – to include: • Complete a safety check of the site • Organise for the installation of a generator If the affected site is Star Farm: Bring up the backup server at Saltersford and make changes to the DNS settings. • Organise for temporary replacement propane heaters if required • Organise for the relocation of any affected staff, vehicles and IT equipment appropriately if required • If a team of staff is to remain on site during the disaster for security plan for their food and facilities
4	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
5	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
6	Regularly review the situation and restore services as soon as possible
7	Conduct a damage assessment if required – see appendix A
8	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
9	Recovery Phase

11	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Connectivity to the Internet

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Contact the Internet Service Provider (ISP) company if not already done
3	Plan for the situation involved – to include: • Complete a safety check of the site • Organise for the installation of a generator If the affected site is Star Farm: Bring up the backup server at Saltersford and make changes to the DNS settings. It might also be necessary to organise for Accounts users to be relocated to Saltersford site. • Organise for the relocation of any affected staff, vehicles and IT equipment appropriately if required • If a team of staff is to remain on site during the disaster for security plan for their food and facilities
4	Contact relevant service suppliers and get any affected services restored as quickly as possible. Inform senior management of the likely timescales
5	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
6	Regularly review the situation and restore services as soon as possible
7	Conduct a damage assessment if required – see appendix A
8	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves the restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
9	Recovery Phase
10	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Internal Network Connectivity – including partial loss

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Plan for the situation involved – to include: • Cooperate with IT and any external agency involved to check internal connectivity issues as required • Install backup network equipment if required

	• If loss due to fibre core being severed appropriate rerouting of network connectivity is required. If more than one core severed contact Protel immediately for relaying of fibre core • Organise for the relocation of any affected staff and IT equipment appropriately as required
3	Inform senior management of the likely timescales for resolution
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore services as soon as possible
6	Conduct a damage assessment if required – see appendix A
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase. This involves to restoration of damage equipment and furniture. The relocation of IT services to the site and finally the relocation of affected staff.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Data

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Plan for the situation involved – to include: • Cooperate with IT and any external agency involved to identify the extent of the data lost • IT to organise for restoration of data from backups
3	Inform senior management of the likely timescales for resolution
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore data as soon as possible
6	Conduct a damage assessment if required – see appendix A. Probably not as a result of any damage but the reason for the data loss should be established
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Major Software Application

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Plan for the situation involved – to include: • Cooperate with IT and any external agency involved to identify the extent of the application loss • IT to organise for restoration of the application via contact with the relevant software supplier • Backups may need to be used to restore to the last known good installation (may include data restoration)
3	Inform senior management of the likely timescales for resolution
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore the application as soon as possible
6	Conduct a damage assessment if required – see appendix A. Probably not as a result of any damage but the reason for the loss of the application should be established
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Data/Service through Cyberterrorism Attack (external and internal)

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Plan for the situation involved – to include: • Cooperate with IT and any external expert agency involved to identify the extent of the cyber attack • IT to organise for restoration of any application or service via contact with the relevant software supplier • Backups may need to be used to restore to the last known good installation (may include data restoration)
3	Inform senior management of the likely timescales for resolution. Consult with senior management regarding the notification required to investigative authorities, the police, customers, suppliers and staff
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore the application as soon as possible
6	Conduct a damage assessment – see appendix A. Probably not as a result of any physical damage but the reason for the loss application, service or data must be

	established and any security flaw must be identified and preventative measures taken.
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Data/Service through Deliberate Internal Misuse

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	Plan for the situation involved – to include: • Cooperate with IT and any external expert agency involved to identify the extent of the attack • IT to organise for restoration of any application or service via contact with the relevant software supplier • Backups may need to be used to restore to the last known good installation (may include data restoration)
3	Inform senior management of the likely timescales for resolution. Consult with senior management regarding the notification required to the police and any notification to customers, suppliers and staff depending upon whether a breach of security has occurred
4	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
5	Regularly review the situation and restore the data/service as soon as possible
6	Conduct a damage assessment – see appendix A.
7	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase.
8	Recovery Phase
9	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Loss of Staff due to disease, accident or pandemic

Step	Action
1	Notify all EMT, DRT, IT teams – particularly IT
2	If disaster due to disease or pandemic consult authorities regarding the extent and measures required to prevent contagion to other staff or sites
3	Plan for the situation involved – to include:

	• Full cooperation with any external experts involved to identify the extent of the problem and the recommended measures to be taken • IT services, staff, operations and equipment may need to be relocated if it is deemed necessary and if access to the original site is permitted • Splitting of departmental staff across multiple sites might be required to ensure operational activity • Use of home working may be required to reduce the risk of contagion • Site or operational closure might be required
4	Inform senior management of the likely timescales for resolution. Consult with senior management regarding the notification required to customers, suppliers and staff following acceptance of medical expert's opinion. It should be noted that senior management may not be available in this situation
5	Inform all affected MJChurch staff of the actions taken and keep the emergency site contacts regularly informed
6	Regularly review the situation and restore the application as soon as possible
7	Conduct a damage assessment – see appendix A.
8	Dependent upon the results of the damage assessment senior management decide whether to continue to the business recovery phase.
9	Recovery Phase
10	Following the disaster, review and make changes to this plan accordingly based upon the knowledge gained

Appendix A

Damage Assessment

Providing access to the site is possible:

- Complete a safety and security check of the site
- Assess the damage to the affected areas and assets to include paper records (files, contracts, documentation etc.…), IT equipment, network infrastructure, power cabling, physical building structure, furniture and fittings.
- Contact suppliers of affected electrical or electronic equipment to ensure its safe working order.
- Contact Insurers accordingly
- Complete a critical equipment status form – Appendix B
- Order replacement equipment accordingly
- Develop a priority list for the restoration of services, facilities and operations
- Based upon the priority list and the lead times involved place orders for replacement items

Appendix B

Critical Equipment Status Form

Site:

Date:

Assessors:

Page:

Status Key:

OK –	Undamaged
U -	Usable
R -	Requires repair
D -	Destroyed

Equipment	Status	Comments

Appendix C

Disaster Form

Disaster Date & Time:

Type of Disaster:

Site:

Building(s) Affected:

Any Access Issues:

Business Operations Affected:

Page:

Disaster Event Log (on going)

Date / Time	Event

Appendix D

Major IT Equipment per site and supplier

Greens

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	2	HP 1920-48G JG927A	Qual	
Network Switch	1	HP 1920-24G POE JG925A	Qual	
Network Switch	1	HP V1910-24G JE006A	Qual	
Network Switch	1	HP V1910-24G POE JE008A	Qual	
Phone System	1	Samsung Office Serv 7100	Protel	
Server	1	Dell Power Edge R210	Westgate/ Dell	
NAS Enclosure	1	QNAP	Westgate/ Ebuyer	
Fibre Router	1	Cisco 2921	BT	
Fibre Interface	1	ADVA FSP150CP Circuit No: ONEA521427 FBT-ORNT-11-B	BT	
Firewall	2	Sonic wall TZ215	Westgate/ Dell	

Star Farm

Server Room:

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	1	Netgear ProSafe GS748T (only used for CCTV on the old fire network)	Westgate/ Ebuyer	
Network Switch	2	HP 1920-48G JG927A	Qual	
Network Switch	1	Netgear ProSafe M4100-26G-POE	Qual	
Phone System	1	Samsung Office Serv 7200	Protel	
Server	1	Dell Power Edge R310 (MJC-VMControl)	Westgate/ Dell	
Server	1	Dell Power Edge R520 (MJC-Host)	Westgate/ Dell	
Fibre Router	1	Cisco 2921 FTIP003383476	BT	
Fibre Interface	1	ADVA FSP150CP Circuit No: ONEA423380 SNEID: 2064 0451 FBT-ORNT-11-B	BT	
Firewall	2	Sonic wall TZ300	Westgate/ Dell	

Reception:

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	2	HP 1920-48G JG927A	Qual	
Network Switch	1	Netgear ProSafe M4100-50G-POE+	Qual	

Blue Cabin (Skips):

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	2	HP 1920-48G JG927A	Qual	
Network Switch	2	Netgear ProSafe M4100-50G-POE+ (one spare but racked)	Qual	

Saltersford

Main Building:

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	2	Netgear ProSafe FS728TP (24G POE switch)	Westgate/ Qual	
Network Switch	1	Netgear ProSafe GS748T	Westgate/ Qual	
Server	1	Dell Power Edge R520 (MJC-Host02)	Westgate/ Dell	
Server	1	Fujitsu (Xeon(R) E5620@2.40Ghz 12GB) (Windows Server 2008R2 Std)	Westgate/ Dell	
Fibre Router	1	Cisco 2921	BT	
Fibre Interface	1	ADVA FSP150CP Circuit No:ONEA420711 FBT-ORNT-11-B	BT	
Firewall	2	Sonic wall TZ300	Westgate/ Dell	

Middle building:

Item	Qty	Product Code/Description	Supplier	Phone
Network Switch	1	Netgear GS728TP (24G POE switch)	Westgate/ Qual	

Appendix E

Staff able to work from home

Department	Position	Name	Mobile