INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) DISASTER RECOVERY POLICY AND PROCEDURES

Document Control Panel			
File Reference Number		ICT Disaster Recovery-PP-01	
File Name		ICT Disaster Recovery Policy and Procedures	
Owner		Marketing, IT & Communications Manager	
Approver		Leadership Team	
History			
Date	Author's Name	Changes	Approved by Name
01/08/2016	LE	Drafted new P&P in collaboration with IT partner	
08/11/2016		Approved	Board of Trustees
Next Review Date		08/2017	

Printed copies of this document are not version controlled.

INDEX

1 Policy Statement

1.1 PAC-UK acknowledges the importance of its ICT systems in the day-to-day running of the business.

1.2 PAC-UK recognises the need for, and value of, a comprehensive ICT Disaster Recovery (DR) Play which aims to minimise risk, disruption and the financial consequences should a disaster occur.

1.3 PAC-UK recognises that it is not possible to foresee and anticipate every eventuality, and that some are out of its control.

2 Introduction

2.1 The ICT DR procedures are to be followed in the event of a disaster concerning the main computer systems at PAC-UK offices. A disaster will be considered to be a disaster when users are unable to access the central servers and/or details are lost from the system. All PAC-UK staff is given a copy of these procedures as part of their induction. These procedures (along with every other PAC-UK Policy and Procedure) can be accessed by all PAC-UK staff via the password protected Members Area on the PAC-UK website. Hard copies are held by all Managers, including the CEO and Leadership Team.

2.2 All procedure updates, including updates to contact names and numbers, must be made to all hard copies. Additionally, PAC-UK's IT Support Service provider, Grant McGregor Ltd, must receive a copy of the revised document if changes are made.

2.3 Responsibility for ensuring that these procedures are kept up to date and tested on a regular basis rests with the Marketing, IT & Communications Manager .The procedures should be reviewed and tested at least once every 12months.

3 Roles and Responsibilities

3.1 Owner = PAC-UK Leadership Team

- Strategic owner of the Business Continuity Plan (BCP)
- Takes ownership of all threats identified and ensures the Business Impact Analysis (BIA) is current
- Participate in test and exercise planning and execution

- Ensure plans are maintained, located and secured appropriately
- Ensure staff are aware of the BCP and their role following an incident
- Liaise with Recovery Team to deliver Business Continuity education to all staff
- During Incident - Incident Management Team Leader
- Liaise with appropriate staff members

3.2 Deputy Owners = Marketing, IT & Communications Manager and IT Partner (Grant McGregor Ltd)

Marketing, IT & Communications Manager and IT Partner are responsible for:

- Maintaining plan procedures through regular review with Plan Owner
- Participating in BCP meetings, tests and exercises when required
- Assisting the Plan Owner in their day to day planning and incident management activities and
- If required, taking on the role of the Plan Owner

3.3 PAC-UK Heads of Services are responsible for:

- Ensuring they are familiar with the content of the plan
- Ensuring that contact details of key staff within their service are known
- Ensuring telephone contact lists are in place for their service
- Providing support to restoring priority services

4 Incident Recovery Team

4.1 The Recovery Team Personnel

The personnel detailed in the table below will form as soon as any of its members declare the need. On forming, those present can take decisions to apply appropriate resources to deal with an event as it occurs (ideally to prevent it becoming a crisis). It is essential for this reason that the team be made up of individuals representing core areas of the organisation.

Business Area	Key Contact Name	Contact Telephone No.
IT Partner – Grant McGregor Ltd.	Paul Sinclair or David Lawrence	0131 603 7911 (office) 07879 408 061 (mobile)
IT Partner – Grant McGregor Ltd.	Grant McGregor Main Line	0808 164 4142
PAC-UK Marketing, IT & Communications Manager	Leon Elias	020 7284 5870 (direct) 020 7284 0555 (office) 07968 944 764 (mobile)
PAC- UK CEO	Peter Sandiford	020 7284 0555 (office) 07932 220 158 (mobile)
PAC-UK Director of Service Delivery	Lyndsey Marshall	020 7284 0555 (office) 07990 573 737 (mobile)
PAC-UK Commercial Director	Adam Bell	020 7284 0555 (office) 07940 990 470 (mobile)

4.2 Meeting Locations

Location	Address
PAC-UK London Office	Torriano Mews, Torriano Avenue, Kentish Town, London, NW5 2RZ
PAC-UK Leeds Office	Hollyshaw House, 2 Hollyshaw Lane, Leeds, West Yorkshire, LS15 7BD
Grant McGregor Head Office	The Merchants' Hall, 22 Hanover Street, Edinburgh, EH2 2EP

4.3 Incident Escalation and Invocation

PAC-UK has a clear and simple method by which it can quickly recognise an ICT business continuity threat and act accordingly. The agreed escalation and invocation framework is set out in Sections 4.4 and 4.5 below.

4.4 Escalation

All staff has a responsibility to notify their line manager, or other appropriate manager, if they feel PAC-UK's ability to operate its ICT systems effectively may be in danger or there may be a need to invoke Business Continuity Plans. This should then be escalated until a member of the Recovery Team outlined in the table at 4.0 is informed.

4.5 Invocation

All members of the Recovery Team have a responsibility to meet as soon as is reasonable to discuss an ICT incident, or the threat of an incident, which could force Business Continuity Plans to be invoked.

4.6 Recovery Team Checklist

In the first 24 hours following a major incident there will be a number of actions that will need to be completed in the short term.

	Action required	Completed (tick to confirm))	Responsible Officer
1	The decision is taken not to invoke Business continuity Plan. Monitor situation if the issue develops.		Recovery Team Personnel
2	The decision is taken to invoke Business Continuity Plan		Recovery Team Personnel
3	Decide location of Control Centre (see table at 4.0 above)		Recovery Team Personnel
4	Is phone system and IT network operational?		Recovery Team Personnel
5	Have all members of the Recovery Team been contacted?		Recovery Team Personnel
6	Have appropriate staff and key stakeholders been identified and Informed?		Recovery Team Personnel
7	Ensure means of communication e.g. Website, telephones and post are in place.		Recovery Team Personnel
8	Ensure any costs incurred are properly recorded.		Recovery Team Personnel
9	Has a log been established to record actions taken?		Recovery Team Personnel
10	Set a target for the restoration of Affected services.		Recovery Team Personnel
11	Contact all staff (directly or indirectly) to explain if attendance is required		Recovery Team Personnel

5 Backup Procedures

5.1 Backup procedures are carried out at server level as all of PAC'-UKs data is held on one of three locations. These servers are located as follows:

Main Servers			
Server Name	**Location**	**Manufacturer**	**Model**
Alumni	Virtual Server	N/A	Virtual Server
PAC NAS001	London Office	QNAP	QNAP TS-420 NAS
PACNAS002	Leeds Office	Buffalo	Linkstation NAS Device

Backup Disaster Recovery Server			
Server Name	**Location**	**Manufacturer**	**Model**
Romy	Scolocate Edinburgh	Dell	R620

5.2 A full backup of all servers is carried out on the main server as outlined in the table below. Backups are automated and scheduled to run overnight every Monday to Friday.

Server Name	Main Role	Backup Frequency	Backup Method
Alumni Alumni is a virtual server located in a Tier 3 enterprise class data centre infrastructure located in Edinburgh	Backing up PAC-UK's Service User Database and My Office Data file system	22:30pm every day: Mon, Tues, Wed, Thurs, Fri, Sat and Sun Daily backup image copied to external hard drive – taken offsite weekly	Veeam Image to Buffalo NAS (Elmyra) Elmura is a NAS Device located in a Tier 3 Enterprise class data centre infrastructure located in Edinburgh Phase 2 part of the building which is separated away from the main server.

5.3 The previous night's backup must be checked via the backup agent to ensure successful completion. These checks are carried out by Grant McGregor as part of the contract between them and PAC-UK.

5.4 If the backup fails, the appropriate action will be taken by Grant McGregor to rectify the situation.

5.5 Any additional ad-hoc backup that may be required, e.g. prior to version upgrades etc. are made onto a CD Rom or the QNAP and following completion of the backup, are suitably labelled detailing the date and time of the backup, the person taking the backup, the reason for the backup and any additional relevant information. These backups are stored appropriately by the individual taking the backup.

6 Threat Assessment

6.1 Threats to PAC-UK's Critical ICT Activities have been assessed against the likelihood and impact of the identified threats occurring

Likelihood						
	A					
	B					**2**
	C			**1**	**4**	
	D			**3**		
	E					
	F					
		5	**4**	**3**	**2**	**1**
		Impact				

Likelihood	Impact
A = Very High	**1** = Catastrophic
B= High	**2** = Critical
C= Significant	**3** = Significant
D= Low	**4** = Marginal
E= Very Low	**5** = Negligible
F= Negligible	

6.2 CT Business Continuity threats are listed below:

	Threat Scenarios	Score	See Continuity Plan Tables
1	Unable to access buildings e.g. fire, flood, severe weather immediately but will be accessible in the next 48 hours	C3	8.1 to 8.9
2	Unable to access buildings e.g. fire, flood, severe weather immediately and will not be accessible in the next 48 hours	B1	9.0 to 9.2
3	Equipment or systems failure (internal power failure)	D3	10.0
4	Serious information security incidents	C2	11.0 to 11.2

6.3 Risk Assessment

The risks outlined in 6.4 have been identified and categorised as follows:

Probability	1 – Low 2 – Medium 3 – High	
Impact	1 – Low 2 – Medium 3 – High	Business can function without item for 2 months Business can function without item for 1 month Business Cannot function
Total	Probability x Impact	
Category	1-3 Low 4-6 Medium 7-9 High	

6.4 ICT Risks

PAC-UK has identified the following ICT risks:

Risk	Probability	Impact	Total	Category
Complete Loss	1	3	3	Low
Server Failure	2	3	6	Medium
Phone System Failure	1	3	3	Low
Website Failure	1	1	1	Low

6.5 Software and Data Risks

The software and data risks outlined in 6.6 have been identified and categorised as follows:

Impact	1 – Low 2 – Medium 3 – High	Business can function without item for 2 weeks Business can function without item for 3 days Business cannot function without item
System Rating	1 – Low 2 – Medium 3 – High	Business can function with minimal disruption System holds valuable but not essential data Essential business system
Total	Impact x System Rating	
Category	1-3 Low 4-6 Medium 7-9 High	

6.6 PAC-UK has identified the following software and data risks:

System	Impact	System rating	Total	Category
Service User Database	3	3	9	High
Payroll/Sage Software	3	3	9	High
Email Server (Microsoft)	2	2	4	Medium
Internet Access	2	1	2	Low
MyOfficeData (File server)	3	3	9	High

7 Disaster Recovery Procedures

7.1 Disaster Recovery Procedures must be implemented if the following occurs-

PAC-UK staff are unable to access the office building immediately (e.g. fire, flood, severe weather) <u>but expect the office building to be accessible within the next 48 hours</u>

7.2 The following procedures detailed from 7.3 onwards should be followed in conjunction with the Disaster Recovery Checklist (Appendix A).

7.3 Immediately on the discovery of the disaster the Incident Recovery Team (see table 4.1) must be notified initially using the appropriate contact numbers.

7.4 In the event of one of these people being unavailable, then an appropriate alternative from the contact list should be contacted. Having assessed the seriousness of the disaster, the most senior person present will contact other personnel as appropriate.

7.5 Responsibility for ensuring that the disaster recovery procedures are followed rests with the Leadership Team or in his/her absence, the Marketing, IT & Communications Manager.

7.6 If the situation is such that police and/or fire personnel are on site, then permission must be obtained from the appropriate authority before entering the site or touching any of the equipment.

7.7 Once on site, all equipment within the office must be checked against the Asset Register held by Grant McGregor's ConnectWise System and PAC-UK's internal Asset Register saved on MyOfficeData. Any missing equipment must be listed.

7.8 **If the Network <u>is</u> intact and <u>is</u> operational**

- Then connections to all terminals and printers should be checked. Once this has been completed the servers should be switched on (if this is not already the case) and a check of the functionality of programs and data should be made. A fuller, more detailed check must be carried out at the earliest opportunity by all users.
- No further updating of information is allowed until all users have confirmed that the data within PAC-UK's MyOfficeData file system and other relevant systems is up to date.
- A list of passwords required for reloading systems and for setting up users on the system should be obtained from Grant McGregor. The list of passwords is held in Grant McGregor ConnectWise system.
- Once the replacement hardware and relevant software have been set up, all users must be notified of the point to which the backup relates, e.g. date and time of the last entries on the system, at the earliest possible opportunity.
- Users will also be requested to confirm that the system is as expected, in particular reports such as trial balances, etc. and that they have access to the same programs and data that they had access to prior to the disaster.
- No processing will be allowed until all such confirmations are completed.

- As soon as the system is available for processing of data **all** passwords must be changed and the system will prompt all users for a new password.
- As soon as the above procedures are completed and processing recommences, an insurance form must be completed by the Leadership Team and/or the Marketing, IT & Communications Manager, if appropriate, and submitted to PAC-UK's insurance brokers.
- At this point the relevant check lists should be double checked to ensure that all procedures have been completed. Once all procedures have been completed the checklist must be signed and dated by the senior manager in attendance. A brief report should then be completed and addressed to the Leadership Team detailing the problem and the procedures followed to recover from the problem.

7.9 **If the Network <u>is not</u> intact and <u>is not</u> operational**

- Grant McGregor Ltd will be notified by the Leadership Team and/or the Marketing, IT & Communications Manager and instructed to be onsite within 8 hours.
- Once the replacement hardware and relevant software have been set up, all users must be notified of the point to which the backup relates, e.g. date and time of the last entries on the system, at the earliest possible opportunity.
- Users will also be requested to confirm that the system is as expected, in particular reports such as trial balances, etc. and that they have access to the same programs and data that they had access to prior to the disaster.
- **No processing will be allowed until all such confirmations are completed.**
- As soon as the system is available for processing of data **all** passwords must be changed and the system will prompt all users for a new password.
- As soon as the above procedures are completed and processing recommences, an insurance form must be completed by the Leadership Team and/or Marketing, IT & Communications Manager, if appropriate, and submitted to PAC-UK's insurance brokers.
- At this point the relevant check lists should be double checked to ensure that all procedures have been completed. Once all procedures have been completed the checklist must be signed and dated by the senior manager in attendance. A brief report should then be completed and addressed to the Leadership Team detailing the problem and the procedures followed to recover from the problem.

8 Power Failure Procedures

8.1 In the event of a power failure, the Leadership Team will-

- Establish how long the disruption to supply will last
- Establish what priority functions are affected
- Is the disruption confined to PAC-UK office/s or is it wider?
- If only PAC-UK offices are affected see the procedure to follow in Section 7
- Ensure phone line providers are contacted to transfer telephone line to appropriate mobile phone number to allow telephone network to remain operational

Note: Whilst the above deals with the immediate response to the threat, The Recovery Team must take into account how PAC-UK will recover priority services to full operation. Other non-priority services will also need to be recovered. Progress on these services will also need to be monitored.

9 Serious Virus Infection or Serious Information Security Incident Procedures

9.1 In the event of a serious virus infection or serious information security incident **any member of PAC-UK staff** will contact Grant McGregor Ltd immediately and advise of the situation.

9.2 Grant McGregor Ltd will ask all users to log out of all systems immediately and will then proceed to clean and disinfect all PCs and File Servers. A restore will be carried out from the most recent back-up if data is corrupt in any way.

10 Checklist

10.1 A checklist to ensure all procedures have been followed is attached (Appendix A).

11 Monitoring and Review

Monitoring of the ICT Disaster Recovery Plan (and recording and reporting of any relevant incidents to PAC-UK's Leadership Team) will be undertaken by PAC-UK's Marketing, IT & Communications Manager in collaboration with PAC-UK's IT Partner (Grant McGregor Ltd).

The IT Disaster Recovery Policy and Plan will be reviewed annually and updated as necessary.

12 Appendix A – Disaster Recovery Checklist

To be completed by PAC-UK's Leadership Team and/or Marketing, IT & Communications Manager.

	Procedure	Y/N	Action Required
1	Have the Incident Recovery Team been contacted? (see Section 4.0)	Y/N	
2	In the event of structural damage or police investigations permission must be granted to enter the building. Has permission been granted? Yes – Permission granted by:	Y/N	
3	If main office inaccessible decide which procedures are to be carried out (see Section7.1 to 7.9)	Y/N	
4	Check equipment against asset list (Grant McGregor and Marketing, IT & Communications Manager lists)	Y/N	
5	Any missing or damaged equipment? (If Yes, please attach detailed list)	Y/N	
6	Check if File Server operational? If YES carry out procedures at 7.8 If NO carry out procedures at 7.9.	Y/N	
7	Restore completed and checked	Y/N	
8	Notify all users of the points that the system has been restored to i.e. date, time of last entries etc.	Y/N	
9	Confirmation from all users that access levels and date is as it was before the disaster	Y/N	
10	All passwords changed	Y/N	
11	Double check the relevant check lists to ensure procedures completed		
12	Complete insurance form and submit to insurance brokers		
13.	Write brief report detailing the disaster		
Report to Leadership Team Name: Date: Signed:			