

BUSINESS CONTINUITY PLAN

Business Continuity Planning Process



Distribution List

This list provides information on who has a copy of the plan and where that copy is.

Copy Number	Version	Name	Location
001			
002			
003			



1 PURPOSE

The purpose of this Business Continuity Plan is to ensure the continuation of ACI Global as a business during and following any critical incident that results in disruption to our normal operational capability.

2 OBJECTIVES

The objectives of this plan are to ensure that ACI Global can continue its operations post a business critical function becoming non operational.

This plan will:

- define and prioritise critical business functions
- risk assess identified potential risks;
- detail immediate responses;
- details strategies and actions to continue doing business; and
- review regularly.



EVENT	CAUSE	PREVENTATIVE CONTROLS (Against Causes)	IMPACT/S	Reactive Controls (To mitigate any consequence should it happen)			
					REPUTATION	FINANCIAL	LEGAL
Data loss	Unauthorised access to system Hardware failure Viruses	Two factor authentication Personal passwords Ensure all data is regularly backup and accessible Ensure Antivirus is operational and current	Loss of data Breach of privacy	Change all passwords to 25 digits with symbols – use a password generator such as lastpass Acquire access to last backup and download to independent system or hardrive	x	x	
System Loss	Terrorists - Cybercrime Act of God	Two factor authentication Personal passwords Ensure all data is regularly backup and accessible Ensure Antivirus is operational and current	Unable to access server Unable to access information Information becomes corrupt and unusable Payments get lost	Change all passwords to 25 digits with symbols – use a password generator such as lastpass Acquire access to last backup and download to independent system or hardrive	x	x	x
Death of key personell	Natural causes Illness Deliberate act	Ensure that all key personnel are cross trained in ACI Global business continuity plan	Overall impacts to the entirety of the business	Have a strategy in place for accidental death			x
Loss of building	Fire either accident or deliberate Chemical spill Becomes an active crime scene	Enure that there is an alternative location for the operation of business to continue	Head Office untenable	Office is mobile so any alternative location will suit	x	x	



	Protests or riots prevent entry						
Loss of third party – IP provider / ACI Global platform provider / training provider	Bankruptcy	Develop a list of active providers to ACI Global and develop plans for mitigation and migration to other services should the need arise			x	x	x



3 CRISIS MANAGEMENT TEAM (CMT)

The crisis management team is in place to make decisions when the Business Continuity Plan needs to be implemented.

CMT Role	Name	Role	Mobile	Email
Crisis Coordinator	Ian Erskine	Owner	+61 4 0883 1898	ianerskine@aciglobal.com.au
IT	Myles Erskine	IT Manager	xxx	myleserskine@aciglobal.com.au

4 ROLES AND RESPONSIBILITIES

To ensure a quick and efficient response to an emergency situation, persons with responsibility for activities described in this CMP, must be aware of the procedures and their duties at all times.

4.1 Crisis Coordinator

In the event of an actual crisis the Crisis Coordinator is responsible for:

- Ensuring the CMT operates effectively;
- Determine the need for additional CMT personnel;
- Identify Crisis Control Centre location;
- Ensure a post crisis review is completed; and
- Chairing the Crisis Management Team meeting
- The provision of communication to the media relations advisor and staff during an emergency;
- Providing human resources and trauma counselling services; and
- Media Relations.

4.2 ICT

In the event of an actual crisis ICT Team is responsible for:

- Getting ICT up and running;
- Ensuring that students lose the least amount of up tie as possible.



5 ACTIVATION OF THE CMT

- The CMT will be activated immediately should one of the identified events come into being.
- When a crisis is declared, the Crisis Coordinator will contact the IT Manager and convene a meeting.
- They will determine the need for any additional personnel or roles required and have them assemble with the CMT.
- The Crisis Coordinator will advise of the location of the Crisis Control Centre and initial meeting time.
- Once assembled, the Crisis Coordinator will provide full details of the crisis in relation to threat / damage to people, assets, property and the environment.
- The CMT will ensure the Crisis Management Plan is executed appropriately, including management of key stakeholders and protection of evidence.
- Alternative locations to be determined by the Crisis Coordinator based on the location and type of event and level of risk. It may also be necessary for people to participate remotely.

Resources required upon activating the Crisis Control Centre are documented at Appendix K.

6 RETURN TO WORK

ACI GLobal will provide the necessary resources to help person/s recover as quickly and as effectively as possible in the event of a person suffering an injury.

7 EMPLOYEE ASSISTANCE PROGRAM (EAP)

EAP providers have been established to ensure suitable assistance is carried out by competent professionals in the event of a critical event occurring.

If required contact xxxxx on xxxxxxxx.

8 MEDIA RELATIONS

All media relations are to go through the Crisis Coordinator.



A.1 Crisis Coordinator Plan

NAME:			
Procedures / Checklist – DURING an Emergency			
Priority	Task	Allocated To	Status
H	Obtain full details of the event from the onsite emergency management team in terms of the threat / damage to people, assets, property and the environment.		
H	Contact the IT Manager and organise to meet and confirm the event details, status and definition of emergency or crisis		
H	Allocate the CMT roles as required		
	<ul style="list-style-type: none"> Declare the Crisis over at the appropriate time, in consultation with the CMT 		
	<ul style="list-style-type: none"> Ensure all actions arising from the Crisis review are complete and implemented 		
	<ul style="list-style-type: none"> 		

A.2 ICT Plan

NAME:			
RESPONSIBILITIES:		Assessing the impact and damage to; <ul style="list-style-type: none"> • Hardware; • Infrastructure; • Telecommunications; • Information; and • Data security. 	
Procedures / Checklist – DURING an Emergency			
Priorit y	Task	Allocated To	Status
H	Obtain full details of the event in terms of the threat / damage to people, assets, property and the environment.		
H	Organise the alert notification and initiate communication with all relevant staff.		
H	Implement the ITCP.		
H	Stand-down Systems & Telecommunication procedures when appropriate.		
Procedures / Checklist – AFTER an Emergency			
Priorit y	Task	Allocated To	Status
H	Restoration of normal operations		
H	Post emergency review of Systems & Telecommunications Plan and ITCP and implement improvements as required.		
M	Review policies, procedures and guidelines utilised by the Systems & Telecommunications Plan and the effectiveness of the Systems & Telecommunications Plan) in the light of the event / emergency and identify and make improvements.		



A.3 Post Crisis Plan Evaluation

The Post Crisis Plan Evaluation is to be completed by the Process Owner, with feedback from staff who participated in the implementation of the Plan, supporting documentation and processes within 24 hours of the Plan stand-down and are to be submitted to the Crisis Coordinator.

Plan Title:	<<Insert Plan Title: >>
Process Owner:	<<Insert Position Title>>
Evaluation Date:	<<Insert Review Date>>
Evaluation Conducted By:	<<Insert Name>>

Please consider:

- What aspects of the Plan and supporting documentation worked well?
- What aspects of the Plan and supporting documentation did not work well?
- Was the documentation adequate and up-to-date?
- Was the communication effective and informative?
- What should be done differently in the event of a future emergency?
- What lessons were learnt?
- What improvements can be made to the Plan, supporting documentation and processes?
- Identify any bottlenecks relating to the Plan, supporting documents and processes



A.4 Crisis Control Centre

Crisis Control Centre

It should be noted that ACI Global is a fully online education service provider and accordingly the crisis control centre can be located anywhere as long as access to a PC is available.

