IT Disaster Recovery Plan
for
ABC Solutions Pty Ltd

Copyright 2023

Version: 23.0

Date Modified: Aug2023

Disclaimer:

The Australian College of Business Intelligence does not invite reliance upon, nor accept responsibility for, the information it provides. The Australian College of Business Intelligence makes every effort to provide a high-quality service. However, neither the Australian College of Business Intelligence, nor the providers of data, gives any guarantees, undertakings or warranties concerning the accuracy, completeness or up-to-date nature of the information provided. Users should confirm information from another source if it is of sufficient importance for them to do so.

Contents

ABC Solutions Pty Ltd IT Disaster Recovery Plan Revision History

REVISION	DATE	NAME	DESCRIPTION
Version 1	xx/xx/20xx	John Doe	Initial document
Version 1.1	05/03/2025	Pedro Schwarz	Updated key personnel contact information to include the **Project Manager of Weather Time**. Added **COVID-19 pandemic** as a potential disaster in the **Risk Management** section. Introduced a **Work-from-Home procedure** in the **System Recovery and Restart Procedures** section.

Information Technology Statement of Intent

This document outlines policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes the recommended procedures. In the event of an actual emergency, modifications to this document may be made to ensure physical safety of the data, system, and people. ABC Solutions Pty Ltd's IT Disaster Recovery program strategically combines people, business processes and technology to ensure that a data center failover and failback can occur in production with little or no data loss and with a minimum of business disruption. IT's Disaster Recovery program leverages a combination of physical, virtual and cloud technologies to ensure that the entire operations of its data centers can automatically fail over to a geographically diverse location if needed.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan to ensure we have consistent and standard best practices to guide people in the event of a disaster, be it a natural one, an act of terrorism or cyber-attack.
- Understand and document the application and infrastructure interdependencies and business processes before we could architect, design and build a DR plan
- IT will begin the Disaster Recovery plan by setting guidelines for the maximum levels of downtime and data loss the business could tolerate in a worst-case scenario with a thorough auditing and documentation of all business processes and existing infrastructure.
- The disaster recovery plan should cover all essential and critical infrastructure, systems, and networks, in accordance with key business procedures.
- The disaster recovery plan should be periodically tested in a staged environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to consider changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites and the need for cross training of personnel in different locations.
- Disaster recovery capabilities as applicable to key customers, vendors, and others

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Pat Gelsinger, Business Analyst	Work	02 9968 5001
	Alternate	02 9742 2342
	Mobile	0423 365 753
	Home	02 9424 6424
	Email Address	pat@ABC Solutions Pty Ltd.com
	Alternate Email	patgelsinger@gmail.com
Greg Lavender, Chief Technology Officer	Work	02 9968 5002
	Alternate	02 9355 6424

	Mobile	0412 464 543
	Home	02 9125 5232
	Email Address	greg@ABC Solutions Pty Ltd.com
	Alternate Email	lavender.g@hotmail.com
Sanjay Poonen, Chief Operating Officer	Work	02 9968 5003
	Alternate	02 9243 2342
	Mobile	0423 098 124
	Home	02 9425 1233
	Email Address	sanjay@ABC Solutions Pty Ltd.com
	Alternate Email	poonen@outlook.com
Andrew Zimmer, Chief Information Officer	Work	02 9968 5004
	Alternate	02 9343 5435
	Mobile	0454 654 234
	Home	02 9654 6432
	Email Address	andrew@ABC Solutions Pty Ltd.com
	Alternate Email	a.zimmer@gmail.com
Jessica Parker,	Work	02 9968 5005

General Manager		
	Alternate	02 9798 5254
	Mobile	0409 678 567
	Home	02 9234 5678
	Email Address	jessica@ABC Solutions Pty Ltd.com
	Alternate Email	jess_park@live.com
Sarah Jane Gomez, IT Operations Head	Work	02 9968 5006
	Alternate	02 9567 0987
	Mobile	0498 567 345
	Home	02 9871 4566
	Email Address	sarah@ABC Solutions Pty Ltd.com
	Alternate Email	jane.sarah@gmail.com
Alexander Price, Director of Infrastructure and Cloud Architecture	Work	02 9968 5007
	Alternate	02 9252 7643
	Mobile	0456 534 345
	Home	02 9376 5462
	Email Address	alexander@ABC Solutions Pty Ltd.com

	Alternate Email	alextheprice@gmail.com
Pedro Schwarz, Project Manager	Work	02 9987 6543
	Alternate	02 9345 6789
	Mobile	0456 789 123
	Email	pedro@ABC Solutions Pty Ltd.com
	Alternate Email	schwarz.p@outlook.com

Notification calling tree

- Greg Lavender
- Chief Technology Officer

- Andrew Zimmer
- Chief Information Officer
- Jessica Parker
- General Manager

- Sarah Jane Gomez
- IT Operations Head

- Pat Gelsinger
- Business Analyst

- Alexander Price
- Director of Infrastructure and Cloud Architecture

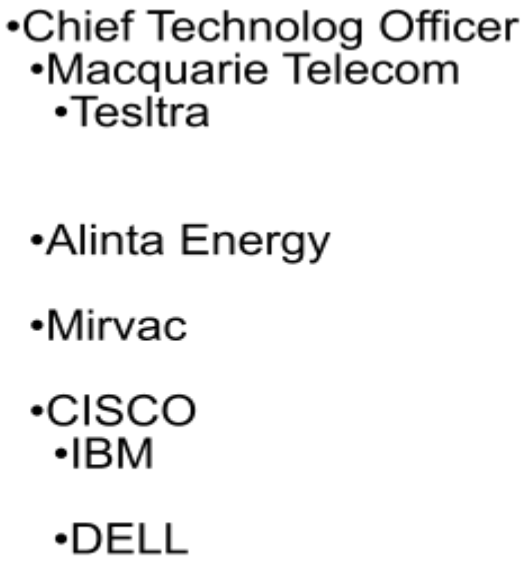
External contacts

Name, Title	Contact Option	Contact Number
Mirvac Property Manager		
Account Number 15242		
	Work	02 8754 1111
	Mobile	0427 333 645
	Home	02 8224 6432
	Email Address	admin@mirva.com
Alinta Energy		
Account Number 986756	Work	02 9525 6542
	Mobile	0498 623 542
	Home	02 8534 7654
	Email Address	admin@alintaenergy.com
Macquarie Telecom		
Account Number 09876	Work	02 8767 6232
	Mobile	0423 756 765
	Fax	02 9875 5324
	Home	02 8765 0987
	Email Address	admin@macquarie.com

Telstra		
Account Number 745987	Work	02 9868 4568
	Mobile	0491 543 325
	Home	02 9345 7659
	Email Address	admin@telstra.com
IBM		
Account Number 457875	Work	02 9257 6876
	Mobile	0487 748 786
	Emergency Reporting	02 5769 8987
	Email Address	admin@ibm.com
CISCO		
Account Number 243567	Work	02 9653 2265
	Mobile	0441 566 578
	Fax	02 9352 5323
	Email Address	admin@cisco.com
DELL		
Account Number 897409	Work	02 9242 2563
	Mobile	0498 575 232

	Home	02 9243 5234
	Email Address	admin@dell.com

External contacts calling tree



Plan overview

Plan Updating

This will involve the use of formalized change control procedures under the control of the Director of Infrastructure and Cloud Architecture. It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials.

Plan documentation storage

Copies of this plan, soft copies and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a soft copies and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a soft copies and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

Backup strategy

This strategy entails the maintenance of a fully mirrored duplicate site and off-site data storage which will enable instantaneous switching between the live site (headquarters) and the backup site.

KEY BUSINESS PROCESS	**BACKUP STRATEGY**
IT Operations	Fully mirrored recovery site
Customer Operations	Fully mirrored recovery site
Product Services and Sales	Fully mirrored recovery site
Cloud Sales	Fully mirrored recovery site
Cloud Management	Fully mirrored recovery site
Multi- Cloud Operations	Fully mirrored recovery site
Tech Support- Hardware	Fully mirrored recovery site
Tech Support- Software	Fully mirrored recovery site
Finance	Off-site data storage facility

Call Centre	Off-site data storage facility
Website	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Intrinsic Security	Fully mirrored recovery site
Cross training of personnel in different locations	Off-site data storage facility
Business Continuity Program	Fully mirrored recovery site
Training and Certification Program	Off-site data storage facility
Account Management Service	Fully mirrored recovery site
Partner Connect Program	Fully mirrored recovery site
Merchandising	Off-site data storage facility

Risk management

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Risk	Brief Description of Potential Consequences & Remedial Actions	Cost
Tornado	1	10000	10000	Damaged power lines and electrical systems causing fire and explosion so data cannot be accessed from anywhere. Have backup power and ensure only battery powered devices are operating to avoid electrocution and explosion	$500

Electrical storms	1	10000	10000	Damaged power lines and electrical systems causing fire and explosion. Have backup power and ensure only battery powered devices are operating to avoid electrocution and explosion	$5,000
Flood	100	10	1000	All critical equipment is located on first floor. Drainage system around the site should be covered to prevent litter from getting into them preventing the area from being flooded	$5,000
Fire	100	10	1000	FM200 suppression system installed in main computer center. Fire and smoke detectors on all floors.	$400
Electrical Power Failure	100	10	1000	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.	$14,000
Act of terrorism	1	1000	1000	Cyber terrorism can cause electrical blackouts, failure of equipment and breach of security. Using full-service internet security suite, using strong passwords, keeping software updates, keeping strong network.	$15,000
Loss of communications network services	10	10	100	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience.	$10,000

Earthquakes	10	10000	100000	Damages and destruction of power lines and collapse of building. Use of cloud services to store data so that the business operation isn't affected even with destruction of physical devices	$15,000 per month
Prolonged Rain	100	1000	100000	Prolonged rain increases the chance of flooding. Drainage system around the site should be covered to prevent litter from getting into them preventing the area from being flooded	$5,000
Act of sabotage	1	100	100	Causes obstruction, disruption and destruction. The best practice to ensure business is not affected by act of sabotage is to have intrinsic security in place.	$10,000
COVID-19 Pandemic	100	1000	10000	The COVID-19 pandemic and potential future pandemics pose a risk to normal business operations by forcing employees to work remotely and limiting access to physical office locations. This disruption can impact productivity and the availability of key personnel.	$20,000 annually

Probability: 1 = Rare, 10 = Infrequent, 100 = Possible, 1000 = Likely, Very Likely = 10000

Impact: 1 = Lowest, 10 = Low, 100 = Medium, 1000 = High, 10000 = Highest

Emergency Response

Disaster Recovery Team

The team will be contacted and assembled by the Emergency Response Team. The responsibilities of the Disaster Recovery Team include:

• Establish facilities for an emergency level of service within 1.5 business hours;

• Restore key services within 4.0 business hours of the incident;

• Recover to business as usual within 10.0 to 24.0 hours after the incident;

• Coordinate activities with Disaster Recovery Team, first responders, senior managers, CIO, Business Analyst and IT Operations Head

• Report to the emergency response team

Alert, escalation and DRP activation

This policy and procedure have been established to ensure that in the event of a disaster or crisis, the team members will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery.

Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- IT Operations Head
- Business Analyst
- Director of Infrastructure and Cloud Architecture
- General Manager
- Chief Information Officer

If not available, try:

- Chief Technology Officer

- Chief Operating Officer

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior managers from the main business departments. The BRT Leader will be a senior manager and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

Plan triggering events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Electrical storms and fire
- Act of terrorism and sabotage

Assembly points

Where the premises need to be evacuated, the Disaster Recovery Plan invocation plan identifies two evacuation assembly points:

- Primary – Lewis Berger Park;
- Alternate – The end of the parking lot towards Shoreline Drive

Activation of emergency response team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Emergency Reference card containing ERT contact details to be used in the event of a disaster.

Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services immediately;
- Assess the extent of the disaster and its impact on the business, data center and employees within the premises;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

DRP Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes if the headquarter building is inaccessible, unusable, or destroyed.

Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact (extension 5000) to relay information on the disaster.

Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member and staff members across different company sites will perform notification duties.

Recorded Messages/Updates

For the latest information on the disaster and the organization's response, staff members can call extension 5000. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

Alternate Recovery Facilities

If necessary, the hot site will be activated, and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site, as necessary.

Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

System recovery and restart procedures

The system recovery and restart procedures for business continuity after a disaster includes (Bernstein & Newcomer, 2009):

- If the checkpointing frequency can be adjusted by the system administrator, then increasing it will reduce the amount of work needed at restart.
- Running a benchmark with different checkpointing frequencies will help determine the expense of using frequent checkpoints to improve recovery time
- Spreading the database over more disks increases the effective disk bandwidth and can reduce restart time
- Increase the system resources available to the restart program. After the operating system recovers from a failure, it runs recovery scripts that include calling the database restart algorithm, tuning it can help reduce restart time.
- Verify the system works as it did before the interruption.

Work-from-Home Procedure

In the event of a disaster requiring remote work, the following steps will be followed:

- Secure Remote Access: Employees must use company-provided VPN and follow secure access protocols to connect to internal systems.
- IT Support Assistance: The IT team will ensure all employees have the necessary software, hardware, and connectivity to perform their duties remotely.
- Virtual Check-Ins: Regular video meetings and progress reports will be conducted to maintain communication and monitor productivity.
- Cloud-Based Solutions: Secure cloud storage and collaboration tools (e.g., Google Drive, Microsoft Teams) will be utilized to ensure seamless workflow.
- Cybersecurity Compliance: Employees must follow strict cybersecurity guidelines, including the use of strong passwords, two-factor authentication, and encrypted communications to prevent data breaches.

Transition to normal operations

The transition of business operations to normal after a disaster or disruption includes:

- If applications running in recovery site are a little unstable, consult the personnel maintaining the applications to determine the best time to transition back to the main processing site
- Transition back to the main processing site at a time when workload if low, so any users or related systems will better tolerate the actual cutover.
- Have sufficient staff at both the recovery site and the main processing site to switch processing back to the main site.
- Additional costs associated with operating the recovery site may bring pressure to transition back to the main processing site as soon as possible.

Operating and support critical IT applications at the main processing site must meet some minimum criteria so the applications can function properly after you transition them back to the main site.