# Next Level Protection.

## Because when challenges arise, you're ready. Or you're not.

Your Backup and Disaster Recovery e-Guide

macquarie CLOUD SERVICES

1800 004 943
macquariecloudservices.com

# A chain is only as strong as it's weakest link.

## Crisis? No drama.

**Creating a complete Backup and Disaster Recovery plan is a challenge. But securing it, future-proofing it, rigorously testing it and simplifying can be harder still. That's where we come in. Because we deliver solutions with our own Australian data centres, telco heritage and over 100 NV1 engineers, based on Australian shores, we can tailor the right fit for your needs. As Australia's most-recommended colocation, hybrid and private cloud provider, we're here to secure your data and environment and free resources for what comes next.**

Things happen. Big things like natural disasters, utility outages, cable damage or malicious actions. And smaller things like failed implementations, updates, rollbacks or malware. Power, cooling and equipment failures and simple human error. Only the right Backup and Disaster Recovery decisions, today, can prepare you for disruptions tomorrow.

No two businesses are the same, or have the same goals, so no two Disaster Avoidance, Backup and Disaster Recovery designs should be the same. This guide will take your through key selection criteria for your Backup-as-a-Service and Disaster Recovery providers, including a full outline to assist in preparing your Disaster Recovery plan.

## The best time to plant a tree is yesterday.

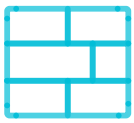
**The numbers can be stark.**

- 75% of Australian organisations are not sure their organisation's data infrastructure is resilient enough to recover data from ransomware attacks.
- 26% of Australian organisations have experienced data inaccessibility due to storage outages.
- 24% admitted to not backing up their data – at all[1].

[1] https://australiancybersecuritymagazine.com.au/75-of-australian-companies-overwhelmed-by-data-security/

### High Availability

100% uptime design-goal options such as duplicating the OS onsite.



### Disaster Avoidance

Selecting dual distributed active-active systems like our zero downtime hosting.

### Data Backup

The basics. Formerly with low-cost, low-availability and high failure tape. Now migrating to the cloud.

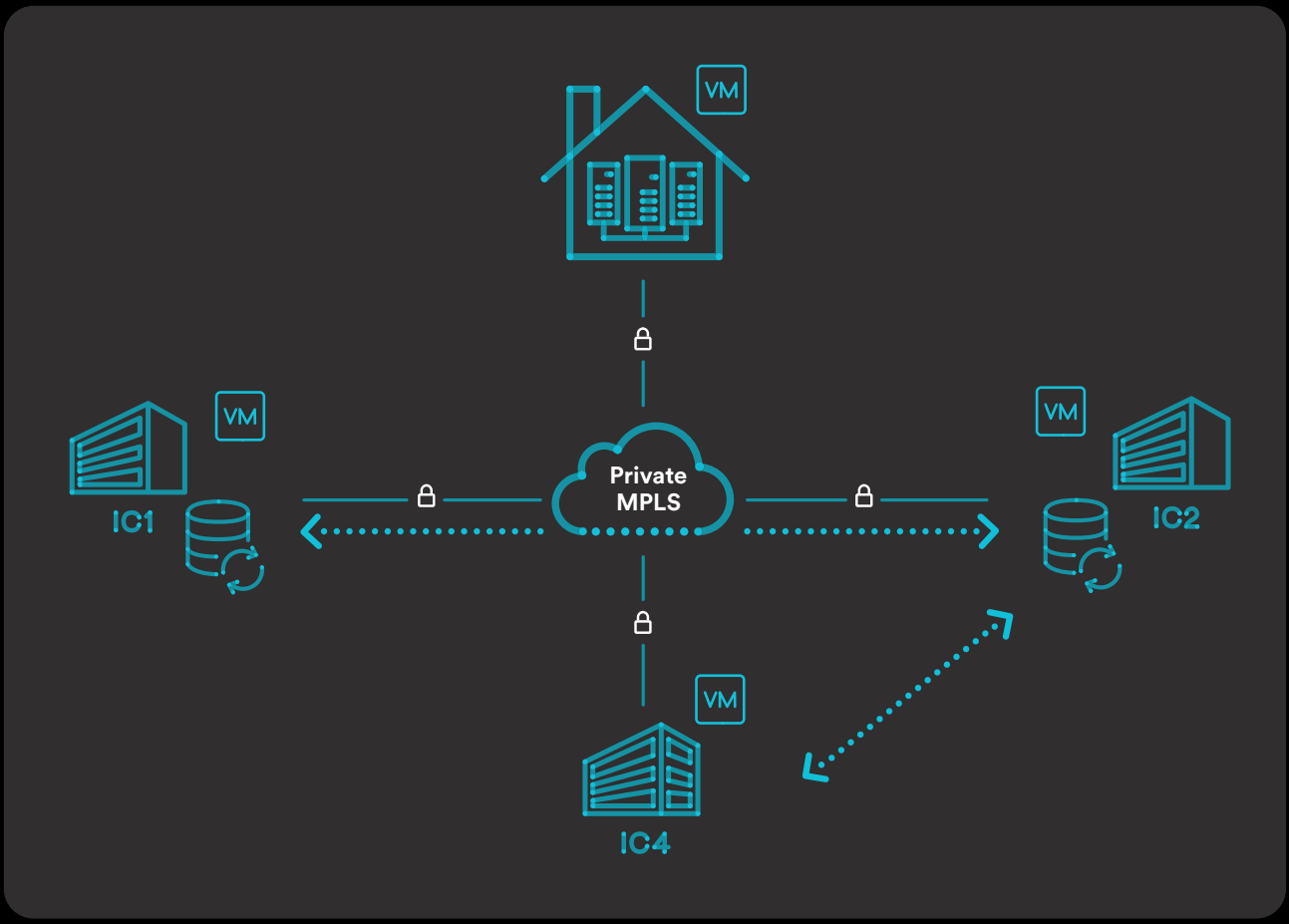
### Failover

Like a spare tyre. Provides high cost N+1 duplicates for critical IT investments.

### Disaster Recovery

Explands on all these ideas to deliver agreed RPO and RTP guarentees for when the unexpected happens.

# Backup Solutions Designed for You. Not Us.




**Operating Systems and Applications Supported**

**Data Types Supported**

# We've got your back(up) for physical and virtual servers.

## Data management is a growing challenge.

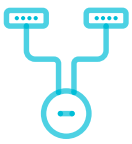
**Power, cost, and technology risks are escalating. Apps, vendors and dashboards are proliferating. DDoS attacks and ransomware are exploding.**

Training, skills and management are at a premium. It all means backup is no longer 'just an IT issue'. It goes to the heart of how you protect your business continuity, your data, your customers and your reputation.

Our secure Backup-as-a-Service (BaaS) eliminates any single point of failure, protecting assets whether they're inhouse, in Colocation or in Hybrid, Private Cloud or Public Cloud environments by leveraging our hardened infrastructure. And they do it with a single solution and interface, based on the technologies and partners you already know and trust.

## What to look for.

**Our expert team suggests the following criteria to help identify the right BaaS solution and partner for you.**



### The right layer.

Hypervisor solutions ensure compatibility is never a problem by separating the replication from apps, operating system and virtual machines.

### Tried and tested.

A proven track record, scale and strengths in testing, certification and compliance.


### Killer customer service.

Whether it's 2pm. Or 2am. When something happens, will you be searching for tickets, APIs and portals, or experiencing Australia's most-recommended customer service?

# BaaS:
# This is how we do it.

### Central visibility, reporting & control.

Get live reports online, or set up notifications. Either way, you'll retain full control of filesystem and application restoration through our online management portals – all backed by our 24×7 support teams.

### Compliance, certifications & security.

Our BaaS infrastructure is hosted in our PCI, ISM, & ISO certified data centres and uses AES256 encryption in-flight and at rest, hardened infrastructure and specialist engineers for Defence-in-Depth security.

### Deeply interconnected.

We're not just carrier-neutral, we're also a leading business-facing telco in our own right. We are deeply interconnected between data centres, national networks including NBN, ICON (government), AARnet (education), Megaport, PCCW and the public cloud (Azure, AWS, Google). This means we can protect resources outside of our own data centres, and you don't even need to use our WAN to make use of our services.

### Backup, recovery & retention.

Back up fully managed virtual machine images, file system and application data and a range of enterprise apps including MS Exchange, MS SQL and MS SharePoint. We enable rapid recovery of your production environment, with retention periods from 14 days to 7 years.

### Resilient storage.

Highly available, cross-site storage hosting eliminates any single point of failure and means back up images are ready for restoration 24×7 so you can bypass the lengthy RTOs of traditional media, but retain their retention capacity.

### Intelligent deduplication.

Backups need bandwidth, which can sometimes be in short supply. Our backup agents intelligently track what's changed on your virtual machines since the last backup, then package up, compress and transmit only the bare minimum.

### Easy self-service.

Get live reports online, or set up notifications. Either way, you'll retain full control of filesystem and application restoration through our online management portals – all backed by our 24×7 support teams.

# Choosing Australia's most-recommended disaster recovery provider.

## Solutions designed for you.

You've probably had enough of generic conversations about your "journey to the cloud". We'd rather we take the time to understand your current environment and goals to deliver a solution with the right tiering of performance, features and value for your requirements.

### What to look for.

Our expert team suggests the following criteria to help identify the right disaster recovery solution and partner for you.

- **Service level guarantees.** Stipulate fail-over guarantees under 30 minutes and RPOs under five minutes at a minimum, and insist on real-world definitions and consequences.
- **Distribution.** Multi-hall, multi-location and multi-cloud solutions protect you from localised risk.

## Disaster recovery: This is how we do it.

**1**

**Business Continuity**

While some applications can support Active-Active deployments by design, we can deliver this at an infrastructure level with a synchronous-write storage and distributed data centre design. This gives you the ability to achieve almost 100% uptime for all your applications.

**2**

**Disaster Recovery**

Mission-critical virtualised apps are replicated at the hypervisor level. While recovery is closer to 'crash consistency' than application-level consistency, this delivers restore points over the last five days, including an extremely aggressive 5-minute RPO, fast and simple DR activation, isolated testing and the reporting capabilities required for compliance and audit obligations.

**3**

**Backup-as-a-Service**

Managed offsite backups address non-mission critical workloads that can tolerate a data loss of 8-24 hours, and provide long-term retention to meet your compliance requirements.

## Launch™ Disaster Recovery.

**Disaster recovery is a vital solution, but a crowded market. We've drawn on 18 years of experience in colocation, hybrid and private cloud solutions to deliver an experience that stands out from the rest, featuring:**

### Flexibility.

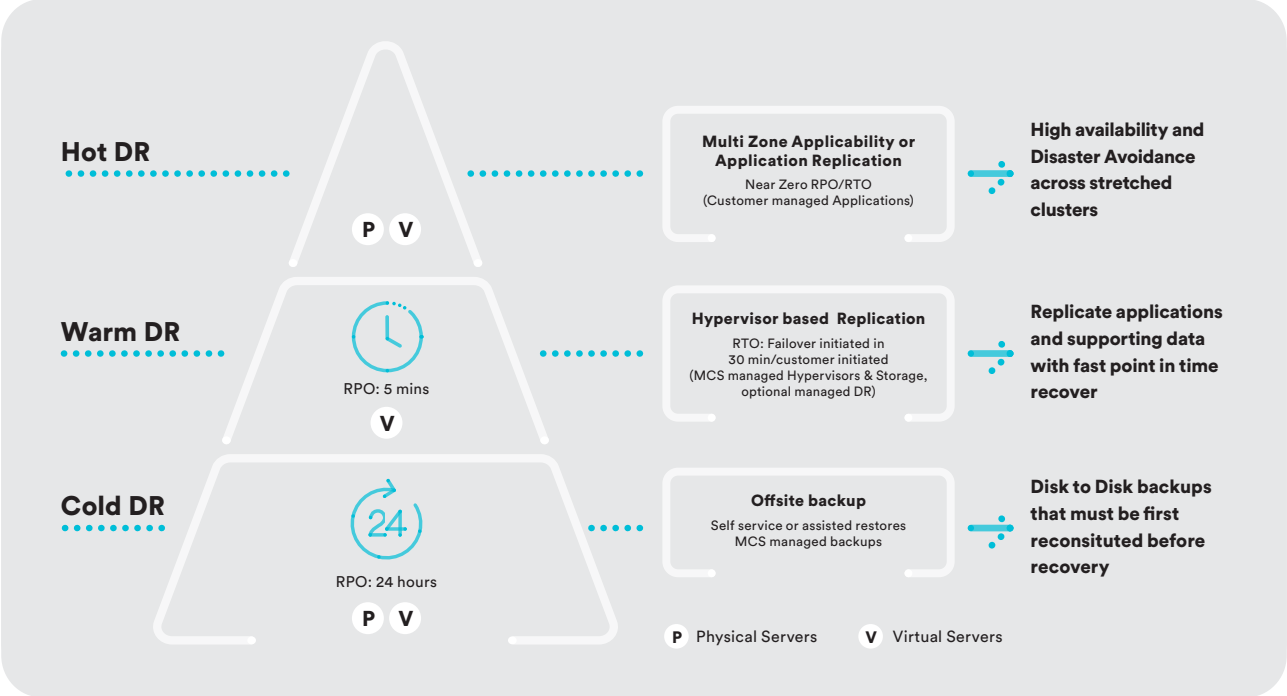
Our flexible design options can guarantee your Recovery Point Objective (RPO) and Recover Time Objective (RTO) and support you 24/7/365 with in-sourced Australian talent on-shift, not just on-call, so if something happens, we're there for you.

### Non-invasive testing.

While testing is the only way to be sure you're ready, we can help you do it without affecting your users and production workloads by enabling access to an isolated failover environment, perfect for application testing. Make scheduled outages and staff downtime for compliance testing a thing of the past.

### No need to change IP addresses.

Our solution ensure VMs will always retain their configured IP address, reducing the effort needed to make the failed-over environment and the applications within accessible to your users



# It's not about public Vs private. It's about the right workload in the right place.

**Consider each of the following to find the right fit for your Disaster Recovery requirements.**

1. **Service Level Guarantees are the key.**

   Always protect yourself with Service Level Guarantees - no excuses, no surprises. It seems intuitive, however we still hear of organisations who fail to do this, then find themselves faced with a range of nightmare scenarios such as:

   - the onus is on them to prove they were trying and failing to retrieve data
   - they're not notified when an attempted backup instance fails
   - they experience costly or highly variable data transfer fees
   - they find that breaches of Service Level Agreements have either no consequences, or are capped at a fraction of monthly charges.

   Always get it in writing and reviewed by legal eyes. That way you'll get what you pay for, with no hidden or variable fees – or there will be real-world consequences.

2. **Snapshots are not backups (and they aren't meant to be).**

   Snapshots are single-point-of-failure, moment-in-time capture of the data state in a virtual machine (VM) you can revert to, even if the VMs are off or suspended. They do not copy the full base disk, so if the VM disk volume gets damaged, your snapshots are gone as well. While this can suit some data types, it's often confined to short-term solutions for patching, updates or tests as a result.

   VM-level backups suit apps whose data doesn't change much, or that are "stateless" such as servers in a webfarm. Because they're independent of the VM, VM-level backups can protect an entire workload e.g. the virtual disks, operating system and all installed applications and data. They are easy to restore at the hyypervisor level at the expense of limited restoration granularity- it's all or nothing.

   There's a lot to it, but it can be a simple as being able to restore and move on, or not.

3. **What else do you need to do to be up and running?**

   People, not just portals and APIs, so you can secure a solution for your specific Recovery Point Objective (RPO) and Recovery Time Objective (RTO) needs. This can include how you propagate updates, set workloads up with an IP address, configure other workloads to access services offered by DNS, configuring the rest of the network infrastructure to automatically and rapidly update DNS, firewalling, intrusion detection, threat protection and other services to accommodate the shifted workload. It's something our stretched networks and firewalls handle by design. And why we're Australia's most-recommended provider.

4. **Tools Matter.**

   Our commitment to industry standards, our exclusive Australia's VMware Showcase Partner status and our MacquarieView tools mean you can benefit from our DR solutions without a challenging learning curve. Tools matter e.g. unlike public cloud hyper-scalers we support Keyboard Video Mouse (KVM) console for Virtual Machines (VMs) so in a lights-out situation, you're not left troubleshooting windows with a text-only serial console.

# Disaster Recovery Plan Template.

**A Disaster Recovery Plan (DRP) establishes guidelines for returning IT operations to normalcy following a natural or man-made disaster. This template was created to serve as a starting point for your company's DRP.**

Disasters covered in this plan can include extreme weather events, malicious acts, infrastructure damage like cables being severed, human error or countless possible failures, rollbacks and updates that can seriously compromise the functioning of a company's IT operations. When creating your DRP, it's important to carefully evaluate which factors represent the greatest risk to your team - and tailor the plan accordingly.

An effective DRP can greatly reduce the negative effects of a disaster by reducing downtime, minimising equipment damage, reducing data loss, and improving employee response. This guide can serve as a starting point for your own plan, but in order to optimise its effectiveness, it must be adapted to your company's unique needs.

After you have completed the document and trained your employees on it, distribute it to key personnel with both hard soft copies and hard copies (including duplicates kept offsite). Only having digital copies on your at-risk network is a classic gotcha.

**Use this plan as a guideline for your own DRP, modifying and adding content as necessary.**

**For more information:**
**Call 1800 004 943**
**+61 2 8221 7003 or visit**
**macquariecloudservices.com**

# Disaster Recovery Plan Template.

## 1. Objectives of this Template

**This section states the goals of your disaster recovery plan. This helps focus the plan on the mission critical objectives and also provides a reference point by which the success of the plan can be measured. Below is an example:**

This set of guidelines contains all of the information necessary to respond to an IT disaster. Remember to always follow proper safety procedures during times of emergency and don't engage in any activity that might put you or other employees at risk.

- Minimise downtime of mission critical operations.
- Reduce damage to critical hardware.
- Train staff on proper disaster response procedure.
- Ensure key data is not lost.
- Mitigate financial losses from incident.
- Deliver on customer and partner expectation.

## 2. What is a disaster?

**This section defines a disaster and provides guidelines for when the DRP should be activated. Use a definition that fits your likely disaster scenario, making it broad enough to account for unforeseen possibilities, but not so broad that it causes unnecessary action.**

With respect to this plan, a disaster is defined as an incident that causes one or more vital systems to stop functioning, causes the building to become unusable in any way, or any combination of the above.

**Possible disasters include:**

- Fire.
- Extreme weather or naturals events.
- Malicious actions.
- Infrastructure damage.
- Human error.
- Mission-critical inputs fail e.g. power, cooling etc.

**There might be a disaster if:**

- You personally observe one of the above mentioned possible disasters.
- System alarms have been activated.
- One or more systems have become non-functional.
- Security has informed you that there is a disaster.

## 3. When should this plan be used?

**This section defines the scope of your DRP, letting staff know when the guidelines set forth should be put into action. Generally speaking, the DRP should be designated for resuming IT operations only. For broader instructions on resuming general business operations, create a separate business continuity plan.**

This plan takes into account malfunctions, damage and anything negatively affecting the following:

- Network connectivity.
- IT staff.
- The building in which IT infrastructure is housed.
- Server room environment control.
- Power source etc.

For issues relating to departments outside of IT, please consult the above mentioned Business Continuity Plan.

## 4. Relevant Personnel

**Key staff should be listed here. This provides an index of necessary contacts that responders can use during a disaster.**

### Disaster Recovery Team

The Disaster Recovery Team is responsible for ensuring the success of the disaster recovery process. They should be contacted promptly after the discovery of a disaster to initiate the DRP.

| Name | Position | Email | Phone |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

### Management

Management should be notified immediately upon discovery of a disaster.

| Name | Position | Email | Phone |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

### Mata Processing Staff

These are the relevant staff in the IT department that can provide support in the disaster recovery process.

| Name | Position | Email | Phone |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## 5. Notification Tree

The notification tree provides a guideline for whom to notify and when in the event of a disaster. In the event of a disaster, contact the necessary personnel as directed by the following notification tree:

| Track 1 | Track 2 | Track 3 |
|---|---|---|
| | Disaster Recovery | |
| | ↓ | |
| | Disaster Recovery Team | |
| ↓ | | ↓ |
| Disaster Recovery Team | | Management |
| ↓ | | ↓ |
| | Data Processing Team | |

## 6. Inventory and Systems Audit

This area provides a step-by-step checklist for all inventory and systems. This will serve as an assessment of the current state of operations and help determine what steps need to be taken to resume normal operations. Use this form to take inventory of the relevant inventory and systems. Make note of any damage and what steps need to be taken to either restore or replace critical items. This list should be updated every ____ months.

**Inventory:**

| Model | Manufacturer | Description | Current condition | Required Action | Mission Critical |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

**Systems:**

| Model | Manufacturer | Description | Current condition | Required Action | Mission Critical |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

## 7. Backup Facility

This section includes information about the backup site where operations can continue while the main site is being repaired. Include instructions for transportation, location and operation. If the backup site is in a distant location, it may also be necessary to include information about accommodations and the local area.

To continue normal operations in the event of a disaster, it may be necessary to move operations to a backup site. Use the information below for procedures on initialising the backup facility. The backup facility contains a copy of the DRP, redundant servers, enough workstations to continue operations and data backups. These should be key criteria in your Colocation Data Centre provider also.

**Location: [Address and Map]**

**Transportation Instructions:**
Transport data processing staff to the backup site via rental car, as per company policy. Ensure that the route is safe and everyone is accounted for before departing the main facility.

**Rental Car Company 1:**
Hertz
(XXX) XXX-XXXX
Keith Smith Ave, Mascot NSW, 2020 Australia

**Rental Car Company 2:**
Ace Rent a Car
(XXX) XXX-XXXX
4/221-223 O'Riordan St, Mascot NSW, 2020 Australia

# 8. Disaster Recovery Procedures

This is where the full instructions for disaster recovery are located. They should include instructions for mobilising the backup site, repairing systems and resuming normal operations. The following lists should be edited to match the needs of your organisation. Also, it is recommended that multiple sets of instructions be included for a variety of possible disaster scenarios. Make instructions concise while still including enough information to ensure clarity.

These procedures should be followed in the event of a disaster. Use caution when dealing with potentially dangerous situations and never follow any step that might put you or a fellow employee at risk.

## Disaster Discovery

If a state of disaster as described in Section 2 has been declared, initiate the following steps:

- Notify the Disaster Recovery Leader of the situation. If the Disaster Recovery Leader is not available, notify the Standby Disaster Recovery Leader.
- Inform senior management a state of disaster has been declared.
- Notify relevant authorities of the situation.
- Gather the disaster recovery response team.
- Make a thorough investigation of the building and systems to determine the scope of damage (using the Inventory and Systems Audit forms in Section 6).
- If possible, initiate data backup of unsecured data.
- Notify clients or customers of expected downtime.
- Notify media of expected downtime.
- Take steps to prevent further damage to systems.
- Restore systems operations, if possible.
- If systems cannot be immediately restored, move on to the next section, “Continuing Operations”.

## Continuing Operations

If the disaster is severe enough that operations at the main site cannot be restored immediately, it might be necessary to relocate operations to the backup facility. Use the following instructions to initialise the backup site:

- Assess designated backup site and determine if it will be adequate to resume critical operations.
- Make arrangements for added workstations or equipment if backup site hardware isn’t sufficient.
- Coordinate transportation to backup site using instructions in Section 7.
- Move operations to backup site as expediently and safely as possible.
- Restore data from systems backup.
- Create new work schedule and tasks for staff.
- Determine estimated time until staff can return to main site.
- Proceed on to next section, “Return to Normalcy”.

## Return to Normalcy

After the backup site has been initialised, the disaster recovery team must begin restoring the main site to functioning condition. Use the following steps to return to normalcy:

- Determine state of systems and operations.
- Create plan for system repair or replacement.
- Notify insurance company of damages.
- Restore data from backups.
- Execute plan to repair or replace damaged systems or equipment.
- If necessary, repair or find alternate main site building.
- Test systems to ensure they are functioning as normal.
- If possible, return employees to main site.
- Notify management of return to normalcy.
- Notify clients and media of return to normalcy.

## 9. Evaluation

In this section, the Disaster Recovery Team will evaluate the effectiveness of the DRP after a disaster. This will help the team create more effective DRPs in the future. Use the following form to evaluate the DRP after a disaster has occurred and the disaster recovery plan has been executed:

**1. Briefly describe the disaster that occured:**

**2. Which systems were affected by the disaster?**

**3. How effective was the DRP in meeting the objectives laid out in Section 1?**

**4. Did the DRP successfully meet its RTO?**

**5. Was the data backup plan sufficient to meet the RPO?**

**6. How could the plan be improved to better meet its goals?**

**7. Are there any goals that should be added to the plan?**

**8. Should the RTO be adjusted?**

**9. Should the RPO be adjusted?**

**10. How much did the disaster recovery process cost?**

**11. Are there any ways the plan could be made more cost effective?**

## 10. Testing Procedures

**This section provides the procedures for testing the DRP to ensure that it is effective and up-to-date. It is recommended that multiple tests be included. Create more detailed tests to be conducted annually and shorter tests to be conducted monthly. Use a combination of simulation testing, parallel testing and walk through testing. Be sure to test for the effectiveness of each component of the plan.**

It is necessary to test the procedures outlined in this document regularly to ensure that they are up-to-date and effective. Below are several test guidelines to be conducted at the designated intervals.

### Disaster Simulation Test

**Test objectives:** Determine the effectiveness of the DRP in a simulated disaster scenario without interrupting normal operations.

**Disaster to be simulated:** Fire caused by malfunctioning temperature control system in server room.

**Disaster effects:** The fire was controlled quickly but damaged the temperature control system, causing it to malfunction.

**Interval of test:** Yearly, no prior notice given before drill.

### Test Procedures:

- Announce that the drill has been initialised and primary temperature controls have failed.
- Run through the DRP.
- Test notification tree for disaster scenario.
- Initialise temperature control failovers.
- Assess the status of temperature control failovers.
- Assess response time of staff.
- Assess DRP effectiveness.

## 11. Plan Maintenance

**This section provides guidelines for updating the plan as systems and procedures change. It should also include a regularly scheduled DRP review session to update and revise the plan.**

In order to maintain its effectiveness, the DRP must be updated every ____, after the addition of any critical system or any significant system update.

**Review sessions are scheduled for the second Friday of December each year and must:**

- Update contact info for key personnel.
- Update backup site information.
- Update core objectives.
- Review effectiveness of plan directives.
- Review the plan's compliance with governmental regulations.
- Review testing procedures.
- Add any new procedures as required by changes in systems etc.

# Choosing Australia's most recommended Backup-as-a-Service and Disaster Recovery provider.

## It's about technology. And people.

At Macquarie Cloud Services, we're different. We're hundreds of people with thousands of solutions. We take the time to understand your starting point, where you want to go and how you want to get there. And we make it happen with Australia's most-recommended team.

## Every journey is different.

Every journey is different. No two starting points are the same. So no two solutions should be the same either. We specialise in a human cloud experience, connecting our named engineers and architects with your specific requirements to deliver a flexible future-proof design with everything you need and nothing you don't.

**It can all start with a single coffee. Lets' talk.**