IT Business Continuity & Disaster Recovery Plan

**1. Introduction**

This IT Business Continuity & Disaster Recovery (BCDR) Plan is designed to help Small-Medium Businesses (SMBs) in Australia prepare for, respond to, and recover from IT disruptions. The goal is to ensure minimal downtime, protect critical business operations, and maintain customer trust.

**2. Objectives**

* Minimise business downtime and financial losses.
* Safeguard critical data and IT infrastructure.
* Ensure rapid recovery of IT systems and operations.
* Meet legal, regulatory, and contractual obligations.

**3. Scope**

This plan covers IT systems, infrastructure, data, telecommunications, and applications critical to the business’s operations. It applies to all employees, contractors, and service providers.

**4. Risk Assessment**

**4.1. Potential Threats**

* Natural disasters (e.g., floods, bushfires, storms)
* Cyberattacks (e.g., ransomware, data breaches)
* Hardware or software failures
* Power outages
* Human errors

**4.2. Impact Analysis** Identify and prioritise critical systems and processes based on their impact on business operations if disrupted:

* **High Priority:** Financial systems, customer databases, operational software.
* **Medium Priority:** Internal communication tools, secondary applications.
* **Low Priority:** Non-essential applications and tools.

**5. Roles and Responsibilities**

**5.1. Business Continuity Team**

* **Team Leader:** Oversees the execution of the BCDR plan.
* **IT Manager:** Manages IT recovery processes.
* **HR Representative:** Coordinates communication with staff.
* **Operations Manager:** Ensures continuity of core business functions.
* **External Vendors:** Provides specialised support (e.g., MSPs, cloud providers).

**5.2. Key Contacts** Maintain an up-to-date contact list of key personnel and external vendors.

**6. Prevention Measures**

**6.1. IT Infrastructure**

* Use redundant systems and failover mechanisms.
* Implement cloud-based backups with offsite storage.
* Regularly update and patch software.

**6.2. Cybersecurity**

* Use firewalls, antivirus software, and intrusion detection systems.
* Enforce strong password policies and multi-factor authentication.
* Conduct regular security awareness training for staff.

**6.3. Physical Security**

* Secure data centres and server rooms with access controls.
* Ensure proper environmental controls (e.g., cooling, fire suppression).

**7. Response Plan**

**7.1. Incident Identification**

* Define criteria for identifying and classifying incidents.
* Use monitoring tools to detect issues early.

**7.2. Communication**

* Notify key stakeholders, including employees, customers, and vendors.
* Use predefined templates for email, SMS, or intranet updates.

**7.3. Immediate Actions**

* Contain the incident to prevent further damage.
* Document the incident details for analysis and reporting.

**8. Recovery Plan**

**8.1. Data Restoration**

* Verify the integrity of backups.
* Prioritise recovery based on criticality.

**8.2. System Recovery**

* Follow predefined recovery procedures for each system.
* Test recovered systems before resuming full operations.

**8.3. Business Operations**

* Implement interim processes to maintain customer service and operational continuity.

**9. Testing and Maintenance**

**9.1. Regular Testing**

* Conduct annual disaster recovery drills.
* Simulate different scenarios (e.g., cyberattack, hardware failure).

**9.2. Plan Updates**

* Review and update the plan every six months or after significant changes to the business.
* Ensure contact lists and system documentation are current.

**9.3. Training**

* Provide ongoing training for all staff on their roles in the BCDR plan.
* Include BCDR topics in onboarding for new hires.

**10. Appendices**

**10.1. Critical Systems List**

* List of applications, databases, and hardware critical to operations.

**10.2. Vendor and Service Provider Contacts**

* Include names, roles, and emergency contact details.

**10.3. Incident Reporting Template**

* Provide a template to log incident details (date, time, nature of incident, actions taken).

**10.4. Recovery Procedure Checklists**

* Detailed step-by-step instructions for recovering critical systems.

**11. Conclusion**

This IT Business Continuity & Disaster Recovery Plan is a living document that evolves with your business needs and the IT landscape. Regular reviews and updates are essential to ensure its effectiveness. By implementing this plan, your business can be better prepared for disruptions, ensuring resilience and sustainability in an ever-changing environment.