*This is a sample Disaster Recovery Plan that can be used for Assessment Task 2 Organise, implement and close an Information Communications Technology (ICT) project. This policy is sourced from a template from Disaster Recovery Plan Template website and then modified and adapted for the purposes of completing this assessment task.*

# MQ Disaster Recovery Plan and Procedures

The objective of a disaster recovery plan is to ensure that you can respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. When you have prepared the information described in this topic collection, store your document in a safe, accessible location off site.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Author | Approved by | Date |
| 1 | Initial Document | Randolph Abbing | Praxis Barnes | 10 June 2018 |
| 1.1 | Minor update to include new staff | Randolph Abbing | Praxis Barnes | 25 Jan 2019 |
| 2 | Update to include change to One Drive from Google suite as file storage provider | Randolph Abbing | Praxis Barnes | 30 July 2019 |
|  |  |  |  |  |

## Section 1. Major goals of the disaster recovery plan

 Here are the major goals of this disaster recovery plan.

* To minimize interruptions to the normal operations.
* To limit the extent of disruption and damage.
* To minimize the economic impact of the interruption.
* To establish alternative means of operation in advance.
* To train personnel with emergency procedures.
* To provide for smooth and rapid restoration of service.

**Section 2. Personnel**

You can use the tables in this topic to record your data processing personnel. You can include a copy of the organization chart with your plan.

| **Personnel** | | | | |
| --- | --- | --- | --- | --- |
| **Name** | **Position** | | **Address** | **Contact Telephone** |
| Praxis Barnes | Director | | 15 Cross St, Clifton Hill, VIC | 0408123456 |
| Amanda Hilton | Office Manager | | 57 Square Road, Yarraville, VIC | 0465432109 |
| Randolph Abbing | IT Manager | | 42 Magic St, Altona, VIC | 04089876543 |
| Gisela Rosa | Administration Officer | | 68 Ships Rd, Avalon, NSW | 0456789012 |
| Nanda Danielsen | Lead Client Relationship Manager | | 90 Triangle Rd, Cronulla, NSW | 0409777543 |
| Theodora Hancock | | Client Relationship Manager | 46/350 Collins St, Melbourne, VIC | 0506765432 |
| Archie Panossian | | Lead Recruiter | 79 Main Rd, Potts Point, NSW | 0607876543 |
| Estelle Brun | | Recruiter | 34 Smith St, Summer Hill, NSW | 0509876543 |
| Aparna Aliprandi | | Recruiter | 87 Emu St, Canterbury, NSW | 0678765432 |
| Khan Sheppard | | Recruiter | 5/22 Cassell St, South Yarra, VIC | 0504901234 |
| Amar Kynaston | | Recruiter | 46/25 Martin St, South Melbourne, VIC | 0408135792 |

**Section 3. Application profile**

| **Application profile** | | | | |
| --- | --- | --- | --- | --- |
| **Application name** | **Critical Yes / No** | **Fixed asset Yes / No** | **Manufacturer** | **Comments** |
| Salesforce | Yes | No | Salesforce | Backup runs daily  Export of complete data to hard drive weekly |
| Windows 2016 Server | Yes | No | AccuWeb | Backup runs daily |
| IIS 10 Hosting | Yes | No | AccuWeb | Backup runs daily  Export of complete data to hard drive monthly |
| Microsoft One Drive for business | Yes | No | Microsoft | Backup runs daily  Export of complete data to hard drive weekly |
| Microsoft 365 | Yes | No | Microsoft | Backup runs daily |
| McAfee® Small Business Security 36 month Subscription | Yes | No | McAfee | Signature updates daily |
| Microsoft 365 Business VOIP | Yes | No | Microsoft | NA |
| Internet Service Provider | Yes | No | Telstra | NA |
| Alternative Service Provider (Wireless broadband) | No | No | Optus | NA |
| Comment legend:  1.  Runs daily 11.00pm AEST.  2.  Runs weekly on Thursday 11.00pm AEST.  3.  Runs monthly on first Friday of the month 11.00pm AEST. | | | | |

**Section 4. Inventory profile**

| **Application profile** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Manufacturer** | | **Description** | | **Model** | **Serial number** | **Own or leased** | **Cost** |
| Dell | | 10 x Precision 3550 Mobile Workstation | | Precision 3550 | DLT001 to DLT010 | own | 10 x $3,529.00 |
| Dell | | 10 x Dell Thunderbolt Dock | | WD19TB | DCK001 to DCK010 | own | 10 x $338.12 |
| Dell | | 10 x Dell UltraSharp 27 Ultrathin Monitor | | U2719DC | DUM001 to DUM010 | own | 10 x $609.50 |
| Dell | | 10 x Dell Premier Wireless Keyboard and Mouse | | KM717 | DKM001 to DKM010 | own | 10 x $196.00 |
| Dell | | 10 x Dell Pro Stereo Headset | | UC150 | DSH001 to DSH010 | own | (inclusive of Laptop cost) |
| HP | | 2 x HP LaserJet Pro Colour MFP | | M479fdw | HPP001 to HPP002 | own | 2 x $800 |
| Fellowes | | 2 x Fellowes AutoMax Micro-cut Shredder 200M | | 46565 | FSH001 to FSH02 | own | 2 x $858 |
| LaCie | | [LaCie 10TB 5big Thunderbolt2 External RAID Drive](https://www.mwave.com.au/product/lacie-10tb-5big-thunderbolt2-external-raid-drive-ac11594) | | STFC10000400 | LTD001 | own | $1684.98 |
| Notes:  1.  This list should be audited every 6 months.  2.  This list should include the following items: Processing units                        System printer Disk units                                 Tape and optical devices Models                                     Controllers Workstation controllers              I/O Processors Personal computers                   General data communication Spare workstations                    Spare displays Telephones                               Racks Air conditioner or heater            Humidifier or dehumidifier | | | | | | | |
| **Miscellaneous inventory** | | | | | | | |
| **Description** | **Quantity** | | **Comments** | | | | |
| Microsoft | | 10 x Windows 10 Pro OS Recovery Media 64bit - USB | | NA | NA | own | (inclusive of Laptop cost) |
| McAfee | | 10 x McAfee® Small Business Security 36 month Subscription | | NA | NA | subscription | 10 x $99.00 |
| Note: This list should include the following items:  Tapes                                                    CDs and DVDs PC software                                          Emulation packages File cabinet contents or documentation     Language software (such as COBOL and RPG) Tape vault contents                                Printer supplies (such as paper and forms) Optical media | | | | | | | |

**Section 5. Information services backup procedures**

Use these procedures for information services backup.

* + OneDrive cloud environment
    - Daily, a saving of changed objects in the following directories is done at 11.00pm AEST:
      * \admin\_ops
      * \client\_relationships
      * \recruitment
      * \users
    - On Thursday of every week at 11.00pm AEST a complete save of the system is done.
    - All save media is stored off-site in a safe at 42 Magic St, Altona, VIC location.
  + Salesforce environment
    - Daily, a saving of changed objects in Salesforce is done at 11.00pm AEST.
    - On Wednesday of every week at 10.00pm AEST a full sandbox is generated and completed and saved to external hard drive every Thursday before end of day.
    - All save media is stored off-site in a safe at 42 Magic St, Altona, VIC location.
  + AccuWeb hosting environment
    - Daily, a saving of changed objects in the following directories is done at 11.00pm AEST:
      * \inetpub\wwwroot
    - On Thursday of every week at 11.00pm AEST a complete save of the system is done.
    - All save media is stored off-site in a safe at 42 Magic St, Altona, VIC location.
  + Personal Computer
    - It is suggested that all personal computers be backed up. Copies of the personal computer files should be uploaded to the OneDrive cloud environment on each Thursday at 8.00pm, just before a complete save of the system is done. It is then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster can wipe out important personal computer systems.

**Section 6. Disaster recovery procedures**

For any disaster recovery plan, these three elements should be addressed.

* Emergency response procedures
  + To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.
* Backup operations procedures

To ensure that essential data processing operational tasks can be conducted after the disruption.

* Recovery actions procedures
  + To facilitate the rapid restoration of a data processing system following a disaster.

[**Disaster action checklist**](http://publib.boulder.ibm.com/infocenter/iseries/v7r1m0/topic/rzarm/rzarmdisaactionchecklist.htm)

This checklist provides initial actions that you might take following a disaster.

Contact Director, Office Manager and IT Manager (Emergency Response Team) and notify of situation

The Emergency Response Team will arrange an immediate meeting/discussion to determine:

* Nature of the disaster/emergency
* Need for an alternative physical site (mobile site)
* Need for alternative internet service provider
* Need for alternative cloud service provider

The Emergency Response Team notify relevant staff and vendors to execute the relevant disaster recovery procedures outlined below.

[**Recovery startup procedures for use after actual disaster**](http://publib.boulder.ibm.com/infocenter/iseries/v7r1m0/topic/rzarm/rzarmrecstrtupprocuseactudisa.htm)  
Consider these recovery startup procedures for use after actual disaster.

**Section 7. Recovery plan for work from home**

This topic provides information about how to plan your recovery task at a mobile site.

* 1. Notify administration, client relationship and recruitment staff (see above) of the nature of the disaster and the need to work from home.
  2. Confirm in writing the substance of the telephone notification to administration, client relationship and recruitment staff (see above) within 48 hours of the telephone notification.
  3. Confirm all needed backup media are available to load into alternative cloud or virtual sites.
  4. Prepare a purchase order to cover the use of alternative virtual or hosting sites.
  5. Depending on communication needs, notify staff of alternative changes to access the Internet (i.e. From Telstra to Optus wireless broadband).
  6. Begin loading system from backups if required:
     1. **Vendors Support Contact**

|  |  |
| --- | --- |
| **Vendor** | **Support Contact** |
| Telstra | Concierge Tech Support 132 999 |
| Optus | Call 1300 213 984  Monday to Friday 8:30 AM - 7:00 PM  Optus Loop Support  Call 135 667  Monday to Friday 9:00 AM - 7:00 PM |
| Salesforce | Australia (Sydney)  Main: +612 9394 7300  Technical Support: 1800 667 638  Australia (Melbourne)  Main: +61 3 9010 2100  Technical Support: 1800 667 638 |
| AccuWeb | [support@accuwebhosting.com](mailto:support@accuwebhosting.com)  <https://manage.accuwebhosting.com/login> |
| Microsoft | https://support.serviceshub.microsoft.com/supportforbusiness |

* 1. Begin setting up power and communications at everyone’s home or remote site.
  2. Individuals test access to Microsoft 365 Outlook email, Microsoft 365 Business VOIP, OneDrive files, Salesforce, the communications lines and do necessary checks.
  3. Begin normal operations as soon as possible:
     1. Daily saves
     2. Weekly saves
     3. Monthly saves
  4. Plan a schedule to back up the system in order to restore on a home-base computer when a site is available. (Use regular system backup procedures).

**Section 7. Testing the disaster recovery plan**

In successful contingency planning, it is important to test and evaluate the plan regularly.

Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document.

[Table 1](http://publib.boulder.ibm.com/infocenter/iseries/v7r1m0/topic/rzarm/rzarmtestdisarecplan.htm#rzarmtestdisarecplan__tstpln) should be helpful for conducting a recovery test.

| Table 1. Checklist for testing the disaster recovery plan | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Yes** | **No** | **Applicable** | **Not applicable** | **Comments** | |
| *Conducting a Recovery Test* |  |  |  |  |  | |
| * 1. Select the purpose of the test. What aspects of the plan are being evaluated?   2. Describe the objectives of the test. How will you measure successful achievement of the objectives?   3. Meet with management and explain the test and objectives. Gain their agreement and support.   4. Have management announce the test and the expected completion time.   5. Collect test results at the end of the test period.   6. Evaluate results. Was recovery successful? Why or why not?   7. Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?   8. Make suggestions for changes. Call for responses by a given date.   9. Notify other areas of results. Include users and auditors.   10. Change the disaster recovery plan manual as necessary. |  |  |  |  |  | |
| *Areas to be tested* |  |  |  |  |  | |
| * 1. Recovery of individual application systems by using files and documentation stored off-site.   2. Reloading of system save media and performing an initial program load (IPL) by using files and documentation stored off-site.   3. Ability to process on a different computer.   4. Ability of management to determine priority of systems with limited processing.   5. Ability to recover and process successfully without key people.   6. Ability of the plan to clarify areas of responsibility and the chain of command.   7. Effectiveness of security measures and security bypass procedures during the recovery period.   8. Ability to accomplish emergency evacuation and basic first-aid responses.   9. Ability of users of real time systems to cope with a temporary loss of online information.   10. Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.   11. Ability to contact the key people or their designated alternates quickly.   12. Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.   13. Availability of peripheral equipment and processing, such as printers and scanners.   14. Availability of support equipment, such as air conditioners and dehumidifiers.   15. Availability of support: supplies, transportation, communication.   16. Distribution of output produced at the recovery site.   17. Availability of important forms and paper stock.   18. Ability to adapt plan to lesser disasters. |  |  |  |  |  | |

**Section 8. Record of plan changes**

Keep your plan current, and keep records of changes to your configuration, your applications, and your backup schedules and procedures.