Administration 8 - ICT BUSINESS CONTINUITY

1. Overview

The ability for the Shire of Christmas Island to in-house facilitate its back up/restoration processes is business critical in remote Australia. The Shire notes that destruction or otherwise loss of ICT equipment will take weeks to months to replace with shipping, hence the AD7 policy will require the Shire to follow procedures suited to remoteness to ensure the best ICT Business Continuity possible.

ICT Business Continuity is defined as ability to continue to access Outlook, Synergy, MEX and other platforms the Shire may be subscribed to or have acquired from time to time. It also covers the ability to access stored electronic archives.

2. Policy Statement:

2.1 To provide optimal back up/restoration facilities and procedures to ensure ICT business continuity for the Shire of Christmas Island

3. Server Data Back Up Procedures:

3.1 Definition

A Server Data Back Up ensures a snapshot capture of all data on the servers including data in Synergy, MEX and Outlook.

It enables the IT section to revert to the back-up date all the files and other data captured at that specific time. It cannot 'undo' individual instances of data loss, rather it is a point of reset for the entire data store of the network to a specific time.

It is the primary line of defence against disaster.

3.2 The Director for IT shall ensure a supply of daily back-up tapes suited to the present server technology is available to the Shire at all times.

3.3 The Director for IT shall ensure back-up of the servers daily at the same set-time. Director is to make network users aware of the set-time for this planned action.

3.4 The Director for IT shall transport the back-up tapes to place of residence where they will be stored in a fire-proof box the Shire shall install and provide.

3.5 The back-up tapes shall be utilised on a rotating weekly basis.

4. UPS Back-Up Procedures

4.1 The Director of IT shall ensure sufficient Uninterruptible Power Supply (UPS) units are available for all terminals and other ICT assets that require protection.

4.2 The IT section will manually install and inspect the UPS units across the

network and ensure users have their devices connected correctly.

4.3 The IT section to conduct annual inspection of UPS units across the network to ensure their condition is acceptable. In the event of a major power failure or local electrical surge or similar, the IT section will carry out an inspection and report back to the Director of IT their findings.

5.0 Outlook Data Back-Up Procedures

5.1 As per the AD7 Shire ICT Policy, users are to keep their Outlook inboxes and sent boxes backed up regularly.

The IT section is to assist network users once a year to ensure their Outlook mail is backed up onto their staff drive on the common server.

6.0 Restoration Procedures:

6.1 Restoration is required when data loss occurs on the servers or network. The Director of IT will be responsible for restoring data loss through use of back-up tapes or other archive technology that the Shire may engage in from time to time.

The procedure to keep the back-up tapes secure are in AD 7 – SOCI ICT Policy.

7.0 Cold Stand-by Facilities:

7.1 There are several hardware facilities essential to the operation of the ICT systems in the present 2023 network design.

a) Storage Area Network (SAN) unit
b) Physical server

7.2 Additional backups of these facilities are kept at the George Fam Centre new in boxes. In the event of a physical failure of the operational units, the IT section is to install the backup units after verifying the operational units are beyond salvaging.

7.3 The Director of IT will then replace the backup units with a new backorder of the same unit at the nearest possible time.

The Director of IT is to inform the CEO and Director of Finance of the timeline of expected replacement

7.4 The IT section is to make recommendations to the Director of IT for the acquisition of spares necessary to maintain the cold stand-by facilities needed for the network design in effect.

8.0 Emergency Temporary Access – 'Break Glass password'

8.1 In recognition of the need to grant emergency temporary access in the event the IT section is unable to provide, the following procedures will guide the emergency temporary access process.

a) The IT Officer is to handwrite the passwords for all network management systems and seal in an envelope. The envelope will be signed by the CEO, IT Officer and Director of IT across the seal

and dated.

b) The CEO will affix the Shire seal and record the affixation of the seal in the Shire seal ledger with date.

c) The envelope will be placed in the Shire's safe.

d) In the event that the CEO, or Acting CEO, cannot reach the Director of IT or the IT Officer and have no foreseeable way of doing so, the CEO and one other Director level staff member may open the signed envelope and report as such at the next Council Meeting.

Both CEO and the Director accompanying the CEO in the opening of the seal must take all care that the passwords do not leak to non-authorised parties.

e) When the IT section is back on duty, they will change the passwords for the necessary network management systems. Repeat from Step

Document Control Box

Version	Approved, Amended, Rescinded	Date	Officer	Resolution number	Key changes/ notes	Next Review date	File Ref No.
1	Approved	21/3/2023	Chirs Su	15/23			