PARTNERSHIP AGREEMENT

Between **Service NSW** (ABN 37 552 837 401) and **Murrrumbidgee Council** (the **'Council**)
(the '**Parties**')

Last Updated: 9 July 2021

1. Purpose

1.1. The purpose of this Agreement is to:

A. Provide the services of Service NSW for Business, which is a division of Service NSW with a mandate of being the one front door for businesses in NSW to access government information and services.

B. Provide the framework within which Services will be delivered
C. Document the responsibilities of Service NSW and the Council on the provision of Services
D. Provide mechanisms to manage the relationship between the Parties
E. Promote a collaborative approach to working together in a timely and effective manner and to act in good faith

This Agreement is not legally binding.

2. Background

1) Service NSW is a Division of the Government Service established under the Service Act. The functions of Service NSW include the exercise of customer service functions, within the meaning of the Service Act*;* other functions conferred by statute; and other functions relating to the delivery of Government services, as directed by the Minister responsible for Service NSW.

2) Section 7 of the Service Act makes provision for customer service functions to be delegated by other NSW Government agencies to the Chief Executive Officer ('**CEO'**).

3) The functions of the CEO are exercised by the staff of Service NSW.

4) Section 8 of the Service Act enables the CEO to enter into Agreements with local government agencies for the exercise of a non-statutory customer service function of the agency; or with respect to the exercise of a customer service function delegated to the CEO.

5) Subsection 8(4) of the Service Act provides that an Agreement with a council, a county council or a joint organisation within the meaning of the *Local Government Act 1993* must be approved by a resolution of the council, county council or joint organisation, must be approved before it is entered into.
6) SNSW partners with the Council to promote and deliver the services of SNSW for Business to businesses across NSW.

7) the purpose of this collaboration is to ensure awareness and access to Government services to all businesses in NSW.

8) the services of SNSW for Business are free for the Council and for customers.

9) The PPIP Act and the HRIP Act set out information handling principles that apply to public sector agencies (as defined in section 3 of the PPIP Act). As public sector agencies, the parties must not do anything, or engage in any practice, that contravenes a privacy principle that applies to them.

10) Section 14 of the Service Act makes provision for the disclosure and use of information, including personal information, for the purposes of the exercise of customer service functions by the CEO. Section 14 has effect despite the provisions of any other Act, including the PPIP Act and the HRIP Act.

11) Section 15 of the Service Act makes provision for the collection of personal information for the purposes of the PPIP Act and the HRIP Act, by Service NSW.

12) Section 16 of the Service Act enables an Agreement made under the Service Act, or a delegation of a customer service function by an agency to the CEO, to provide for the exercise by Service NSW of functions relating to access to information under the Government information (Public Access) Act 2009 and functions relating to the State Records Act 1998, in connection with the functions of the council concerned. The responsibilities of Agencies under the *State Records Act 1998* include making and keeping full and accurate records of their office.

13) The Parties have agreed to enter into an Agreement under section 8 of the Service Act, incorporating these Standard Terms of Engagement.

3. Guiding Principles

3.1. The Parties will:

A. Work collaboratively and in good faith in a timely and effective manner, with open communication to achieve shared objectives

B. Facilitate a partnership relationship that promotes and achieves continuous improvement and accountability

C. Ensure that each of its Personnel complies with this AGREEMENT and all applicable laws and policies relating to the Services, including the *Work Health and Safety Act 2011*

D. Comply with the agreed timelines for meeting obligations to ensure efficient and effective delivery of Services

E. Work together to identify and manage shared risks

F. Work together to prioritise initiatives and enhancements, particularly where there are limitations on time and resources; and

G. Work together to respond to the media, advise Ministers, and consult each other when developing communications that impact on Services.

4. Roles and Responsibilities

4.1. Service NSW will:

A. Provide the Services in accordance with this Agreement Standard Terms, subject to any Change Request

B. Exercise the required standard of skill, care and diligence in its performance of the Services and ensure that its Personnel have appropriate qualifications and skills to provide the Services

C. Take responsibility for the management of records it creates or holds as a result of the exercise of a customer service function, where required; and

D. Take responsibility for performing necessary maintenance of its systems and data managing the impact on customers from Service NSW system outages and working in conjunction with the Council.

4.2. The Council will:

A. Provide Service NSW with all information, inputs, resources and subject matter expertise in a timely manner as required to enable Service NSW to provide the Services as set out in the Agreement

B. Take responsibility for the management of records it receives or holds following the exercise of a customer service function by Service NSW.

4.3. The Parties undertake to maintain open channels of communication by:

A. Making available Personnel, data, reports and computer systems for the purposes of resolving customer issues

B. Appointing a Relationship Manager with responsibility for managing the contractual and operational aspects of the Services. The Relationship Manager may be varied.

5. Services

A. Service NSW will:

(i) provide the relevant information and contacts to Council to ensure its local businesses are aware and can access the SNSW for Business services

(ii) provide a single point of contact for Council to ensure it can access SNSW for Business services.

B. the Council will:

(i) refer eligible customers to the Program

(ii) provide guidance to Service NSW staff to assist in responding to inquiries

(iii) inform customers and Service NSW of the outcome of relevant applications in line with privacy requirements

(iv) provide updates on changes to local government policies, guidelines or other matters which may affect the Program

(v) identify local opportunities to inform customers of the program

(vi) provide Service NSW with feedback on the effectiveness and performance of the Program.

6. Liability

6.1. To the full extent permitted by law, neither Council or Service NSW will be liable to the customer for the customer’s actions or responsible for any liability, loss or cost suffered directly or indirectly by the business in connection with the Service NSW for Business service.

7. Data and Data Security

7.1. Each party retains ownership of its Data.

7.2. Except as required by law, neither party must ensure that its Personnel will not:

A. use the Data belonging to the other party for any purpose other than the performance of its obligations under this Agreement
B. sell, commercially exploit, let for hire, assign rights in or otherwise dispose of any Data; or

Each party must establish and maintain safeguards against the destruction, loss or alteration of either party's Data in the possession or control of that party which are is consistent with and no less rigorous than those maintained by either party to secure its own data; and comply with all applicable laws and policies.

In particular, the Parties will ensure the secure transmission and storage of data, at standards no less than those recommended by Cyber Security NSW.

8. Confidential Information

8.1. The Parties must, in respect of any Confidential Information:

A. Keep the Confidential Information confidential and not disclose that information to any person without the prior written consent of the disclosing party, other than to its Personnel, professional advisors or contractors requiring access to the Confidential Information in connection with providing the Services
B. Use the Confidential Information solely for the purpose of carrying out its obligations
C. Not permit the Confidential Information to be reproduced except to the extent reasonably required to carry out its obligations
D. Not do anything that would cause the disclosing party or its Personnel to breach their obligations under Privacy Law; and
E. Notify the other party as soon as possible upon becoming aware of any breach of this clause.

9. Privacy

9.1 Each party and its Personnel must:

A. Comply with Privacy Laws; and

B. Do all that is reasonably necessary to enable the other party to comply with Privacy Laws, including the development of documentation to demonstrate compliance with Privacy Laws, as agreed between the parties

9.2. In particular, Service NSW acknowledges that:

A. The collection of personal or health information will take place in compliance with the Privacy Laws, as modified by section 15 of the Service Act; and

B. the use, disclosure, storage and retention of such information will be in accordance with the Privacy Laws, and in accordance with applicable policies.

Schedule 3 documents the respective responsibilities of Service NSW and the Council in relation to the collection, storage, use, retention and disclosure of personal information.

9.4 Personal and health Information collected, used, disclosed or retained between the parties will be managed and retained by the parties in accordance with the *State Records Act 1998* (NSW) and all other applicable laws, including Privacy Laws.

9.5 Once either of the Parties has reasonable grounds to believe there has been unauthorised access to, unauthorised disclosure of, or a loss of Personal or Health Information, dealt with in connection with this Agreement (‘**Data Incident’**):

A. The party must immediately (but in any event, no later than 72 hours of becoming aware of the Data Incident) notify the other party of that contravention together with all relevant information relating to the contravention

B. Consult with the other party as to which party should have primary responsibility for investigating and dealing with the breach or possible breach

C. Consider, having regard to the scope of the Data Incident and the nature of the personal or health information involved, together with any other relevant factors, whether the Data Incident is serious.

D. The party with primary responsibility for the breach must notify the Privacy Commissioner as soon as practicable that a serious Data Incident has occurred; and

E. The parties must co-operate and collaborate in relation to assessment and investigation of the Data Incident, and action required to prevent future Data Incidents.

9.6 If either of the Parties receives a complaint or request for an internal review of conduct in relation to a breach or alleged breach of a Privacy Law, including under section 53 of the PPIP Act, (a ‘**Complaint’**), the following will apply:

A. It is the responsibility of the party that receives the Complaint to perform a preliminary investigation to determine the party responsible for the conduct

B. If responsibility lies wholly with the party that received the Complaint, then that party is responsible for responding to the complaint or conducting the internal review of conduct

C. If, after performing the investigation, the relevant party reasonably considers that the Complaint should be transferred to the other party, it will (after obtaining the consent of the customer) promptly transfer the Complaint and any further information obtained by the party from its preliminary investigation to the other party, no later than 20 days after receipt of the original Complaint

D. If the Complaint relates jointly to the conduct of both parties, then the party that received the Complaint will (after obtaining the consent of the Customer) notify the other party no later than 20 days after its receipt of the original Complaint and provide any further information obtained by that party from its preliminary investigation. The parties will then work together to coordinate a joint response from the parties within 60 days of receipt of the Complaint. This response may include an internal review of conduct.

10. Intellectual Property

10.1 Each party will retain the Intellectual Property Rights in its Existing Material.

10.2 Each party agrees to grant to the other party a non-exclusive and royalty free licence to use, sublicence, adapt, or reproduce:

A. Their Existing Material; and
B. All methodologies, processes, techniques, ideas, concepts and know-how embodied in their Existing Material,
C. To the extent their Existing Material is required for use by the other party, solely in connection with provision of the Services.

10.3 Each party represents and warrants to the other party that it has all required rights and consents for its Existing Material to be used for the Services.

10.4 Intellectual Property Rights in all New Contract Material will vest in the Council.

10.5 The Council grants a perpetual, worldwide, irrevocable and royalty free licence to the Intellectual Property Rights in all New Contract Material to Service NSW for the purpose of performing the Services.

10.6 Subject to clauses 10.1 and 10.4, Service NSW will own all Intellectual Property Rights in the provision of the Services, including any solution and service design.

11. Performance Management and Continuous Improvement

11.1 Service NSW for Business does not require any provisions in relation to performance management

11.2 Service NSW for Business will work collaboratively with Council to ensure continuous improvement of its services to Council

11.3 Any future extension of this Agreement by Service NSW with Council will specify the relevant performance management and continuous improvement provisions required.

12. Reporting

12.1 Service NSW for Business does not require any reporting arrangements

12.2 Any future arrangements that require reporting will be outlined in a Schedule to this Agreement.

13. Change Management

13.1 Each party will comply with the Change Management Process set out in Schedule 4.

13.2 The parties agree to complete a Change Request in the form set out in Schedule 4 to add to or vary the Services.

14. Governance

14.1 The parties agree to comply with the Governance Framework.

15. Business Continuity and Disaster Recovery

15.1 Each party will maintain Business Continuity and Disaster Recovery Plan arrangements to ensure that each party is able to continue to perform its obligations under this Agreement, or where performance is not possible, resume performance as soon as reasonably practicable in the event of a Disaster.

16. Dispute Resolution

- ***16.1*** In the event of a dispute between the parties, a party will:
- Raise the dispute with the other party's Relationship Manager and use best efforts to resolve the dispute
- If the dispute is not resolved within a reasonable period, the Chief Executive of the Council or their delegate will meet with the Chief Executive Officer of Service NSW (or their delegate) with a view to resolving the dispute.
- If the dispute is not resolved under clauses 16.1(b) within a reasonable period, attempt to resolve any dispute in accordance with the Premier's Memorandum M1997-26.
- ***16.2*** Despite the existence of a dispute, each party must continue to perform its obligations.

17. Termination

17.1 Either party may terminate this Agreement in whole or in part by giving the other party 90 days written notice or as otherwise agreed.

17.2 On notice of termination or where Service NSW is otherwise required to cease to perform some or all of the Program, the parties will work together in good faith to finalise and agree a transition out plan to facilitate smooth and orderly transition of the relevant Program to the Council or the Council's nominated third party. Where the parties cannot agree, the dispute resolution provisions in clause 16 will apply.

17.3 Upon termination, each party agrees to return all Data and property belonging to the other party within 30 days of the termination date and comply with the transition out plan agreed under clause 17.2.

18. Miscellaneous

18.1 Entire Agreement

This Agreement supersedes all previous Agreements, understandings, negotiations, representations and warranties and embodies the entire Agreement between the Parties about its subject matter.

18.2 Survival

The following clauses survive termination or expiry of the Agreement: Clauses 4, 6, 7, 8, 9, 14, 15, 16, 17, 18, 19 and any other clause which by its nature is intended to survive termination or expiry of the Agreement.

18.3 Notices

A notice under this Agreement Standard Terms must be in writing and delivered to the address or email address of the recipient party.

18.4 Variation

All variations to this Agreement and all consents, approvals and waivers made under this Agreement must be evidenced in writing and variations signed by both parties.

18.5 Waiver

If a party does not exercise (or delays in exercising) any of its rights, that failure or delay does not operate as a waiver of those rights.

10.6. Applicable law

The Agreement is governed by, and is to be construed in accordance with, the laws in force in NSW.

18.7 Counterparts

The Agreement may consist of a number of counterparts and if so, the counterparts taken together constitute one and the same instrument.

19. Execution

Murrrumbidgee Council has reviewed and accepts this Agreement

Signed for and on behalf of **Murrrumbidgee Council** by its authorised signatory	Signed for and on behalf of **Service NSW** by its authorised signatory
Name:	Name:
Title:	Title:
Date:	Date:
Signature:	Signature:
Witness:	Witness:
Signature:	Signature:

Schedules

Schedule 1 - Definitions

In these Standard Terms, except where a contrary intention appears:

Business Continuity and Disaster Recovery Plan means a business continuity and disaster recovery plan which documents the back-up and response actions each of the parties will take to continue its obligations if a Disaster occurs

Change Request means the request for a change to the scope of Services in the form set out in Schedule 2

Commencement Date means the date of start of this Agreement.

Confidential Information of a party means any written or oral information of a technical, business or financial nature disclosed to the other party, including its employees or agents, by the disclosing Party (whether orally or in writing) whether before or after the Commencement Date, that:

A. is by its nature confidential; or
B. is designated as confidential; or
C. the other party knows or ought to know is confidential,
D. but does not include information which:
    a. is or becomes public knowledge other than by breach of these Standard Terms; or
    b. is in the lawful possession of the Party without restriction in relation to disclosure before the date of receipt of the information; or
    c. is required to be disclosed by Law, government policy or legal process.

Contact Centre has the meaning set out in Schedule 1

Continuous Improvement Principles have the meaning set out in Schedule 1

Continuous Improvement Process has the meaning set out in Schedule 1

Data means the data of each party and all data and information relating to their operations, Personnel, assets, customers and systems in whatever form that may exist, including Confidential Information

Disaster means an event that causes, or is likely to cause, a material adverse effect on the provision of the Services that cannot be managed within the context of normal operating procedures including interruption, destruction or other loss of operational capacity

Existing Material means any material that is developed prior to entering into a Project Agreement or Service Agreement, or developed independently of a Project Agreement or Service Agreement, and includes any enhancements and modifications to its Existing Material created as part of a Project Agreement or Service Agreement

Governance Framework means the governance arrangements set out in the Service Agreement

HRIP Act means the *Health Records and Information Privacy Act 2002* (NSW);

Instrument of Delegation means the instruments of delegation (including its terms and conditions) made by the Council in relation to the Delegated Functions.

Intellectual Property Rights includes patent, knowhow, copyright, moral right, design, semi-conductor, or circuit layout rights, trademark, trade, business or company names or other proprietary rights and any rights to registration of such rights, whether created before or after the Commencement Date, in Australia or elsewhere

Middle Office has the meaning set out in Schedule 1

Moral Rights means the right of integrity of authorship and the right not to have authorship falsely attributed, as confined by the *Copyright Act 1968* (Cth) and the rights of similar nature anywhere in the world, whether in existence before or after the Commencement Date

New Contract Material means new data created, other than the solution or service design

Personal Information has the meaning given to it in the Privacy Laws, as amended from time to time

Personnel means the person or persons employed or otherwise contracted by either party under these Standard Terms, as the context requires

PPIP Act means the *Privacy and Personal Information Protection Act 1998* (NSW)

Privacy Law means any law that applies to either or both of the parties which affect privacy or any personal information or any health information (including its collection, storage, use or processing) including:

A. the PPIP Act; and
B. the HRIP Act.

Program means the Easy to do Business program

Quarterly Forecast has the meaning set out in Schedule 1

Relationship Manager means the nominated relationship managers of either party, as set out in the Service Agreement, or as otherwise nominated by a party from time to time

A. Service Act means the *Service NSW (One-stop Access to Government Services) Act 2013* (NSW);

Service Centre has the meaning set out in Schedule 1

Service NSW Standard Operating Conditions means the standard operating conditions met by Service NSW in the usual course of its performance of the Services set out in Schedule 1

Service Levels means the service levels, operating conditions and service levels relating to the Services as set out in the Service Agreement

Standard Terms of Engagement or **Standard Terms** means these terms and conditions and includes Schedules 1 and 2

Subcontractor means a third party to which Service NSW has subcontracted the performance or supply of any Services

Schedule 2

1. Service NSW Standard Operating Conditions

In addition to the Project Agreement, Service Agreement or Research Agreement, this section covers the standard omnichannel service inclusions.

1.1. Service Centre

Similar services as those available at Service Centres may be offered through Mobile Service Centres. The Mobile Service Centre timetable is published regularly on the Service NSW website.

Inclusion	Description
Concierge and digital assisted services	A Service NSW Concierge will greet and direct customers to the appropriate channel and dispense a ticket where applicable. If the transaction can be completed online, a Digital Service Representative will assist the customer to complete the transaction
Customer sentiment surveys	Before leaving the centre, customers will be offered the option of leaving feedback via a digital terminal

1.2. Contact Centre

Similar services (to that of phone-based) may be offered through a web chat feature accessible via the Service NSW website.

Inclusion	Description
Virtual hold call back system	During high volume periods, customers will be offered the option of leaving their details with an Interactive Voice Response (IVR) auto attendant. Customers can hang up while holding their place in the queue. Their call will be returned by the next available operator
Inbound number	Service NSW will answer all inbound enquiries on 13 77 88 as 'Service NSW'
Call coding	A Customer Service Representative will record the customer's reason for calls and the outcome
Customer sentiment surveys	Once the call is complete, customers will be offered the option of leaving feedback via an automated IVR system

1.3. Middle Office

Inclusion	Description

Enquiry triage	Service NSW will triage enquiries received to info@service.nsw.gov.au or via Service NSW website 'Contact Us' page and - Resolve these enquiries or - Refer it to the appropriate business area at the Agency
Enquiry coding	A Customer Service Representative will record the customer's reason for enquiring and the outcome

1.4. Service NSW Website and Mobile App

Inclusion	**Description**
Scheduled maintenance and planned outages	Service NSW will conduct regularly scheduled maintenance of the website and mobile app. 10 business days of notice will be provided regarding outages from planned and scheduled maintenance Maintenance activities with negligible impact or outage, such as enhancements to optimise for cybersecurity or performance, may occur without notification to the Agency

1.5. Service NSW for Business

Service NSW for Business provides a multi-channel service including digital, phone and face-to-face services for metro and regional businesses in NSW and develops relationships with councils and business associations to promote the offering to local businesses.

Inclusion	**Description**
Relationship management	Business Customer Service staff initiate and maintain relationships with councils and business associations to promote awareness and use of the service offering by such stakeholders and their local business community. It may include, but is not limited to, information sharing, regular liaison at events and stakeholder premises and issue of surveys.
Scheduled Maintenance and Planned Outages	Digital products controlled by Service NSW for Business will be regularly updated, upgraded and maintained without any outages.

1.6. Training

Service NSW will provide appropriately trained Personnel to deliver the Services.

1.7. Language

Service NSW will provide services in English and may arrange translation and interpreter services for customers from non-English speaking backgrounds if required.

1.8. Branding

Unless otherwise set out in the Project Agreement, Service Agreement or Research Agreement, Service NSW channels are singularly branded. Marketing communication is limited to Service NSW led or co-led campaigns and programs.

1.9. Contractors and Agents

Service NSW may use contractors and agents in connection with the delivery of Services. Such agents and contractors are approved persons under Part 2 Section 12 of the Service Act.

1.10. Out of Scope Services

Any item, service or deliverable that is not specified in a Project Agreement, Service Agreement or Research Agreement is deemed to be out of scope for Service NSW.

2. Operational Framework

Service NSW operational framework outlines how operations are managed on a day-to-day basis.

Operational Support	**Description**
Knowledge Management	Service NSW creates and maintains support material (knowledge articles) for serving customers. These will be sent to the Agency for endorsement of content accuracy bi-annually
Complaints Management	Service NSW will record complaints and its supporting information unless resolved at the outset. Service NSW will contact the Agency where assistance is required
Issues Management	Issues relating to existing products and services should be raised via partnerships@service.nsw.gov.au or directly with the Relationship Manager The Relationship Manager will assess the issue and facilitate a resolution within Service NSW, providing regular updates
Quality control framework/ compliance	Service NSW has a quality control framework that governs transactional activities in line with risk assessment at the time of onboarding The framework includes: - Regular review of contact centre calls, including being assessed against procedure and process used by the agent during the call - Daily quality checks of transactions undertaken by the service centre - Quarterly compliance reviews and certifications provided by all service delivery channels

2.1. IT Operations & Support

Service NSW runs a 24/7, 365 days a year service desk. Unplanned interruptions or degradations in quality of service should be raised to the Service NSW Service Desk on 1300 697 679 (option 2) or servicedesk@service.nsw.gov.au

Incident response times in our production environment are prioritised based upon urgency and impact, with associated response and resolution times.

Priority Code	Service Level Target Response/Resolution Time
P1 - Critical	Response: Immediate response, action/update within 15 minutes Resolution: 2 hours
P2 - High	Response: Immediate response, action/update within 30 minutes Resolution: 4 hours
P3 - Medium	Response: 8 hours Target Resolution: 10 working days
P4 - Low	Response: Email notification of call being logged within 2 days. Response by email or phone within 2 working days Target Resolution: 20 working days

Where vendors or other government platforms are involved, Service NSW utilises a best practice vendor governance framework for service level Agreements and for priority 1 and 2 incidents.

2.2. System and Security Maintenance

Service NSW complies with the NSW Government Cyber Security Policy and operates an information security management system that is certified against ISO 27001. These engagement Terms do not extend the certification scope to the Agency's specific activities.

3. Customer Payments

Service NSW will collect payments from customers for transactions set out in the Service Agreement. Cash, cheque, money order, credit or debit card may be accepted and merchant fees plus GST will be recovered.

Service NSW will provide remittances and reconciliation files to the Agency which include:

A. Credit T+2 value for cash, cheques* and bank card payments
B. Credit T+2 value for AMEX payments
C. Debit any cheques dishonoured
D. Debit any card payment chargebacks
E. Debit any refunds processed on behalf of the Agency

Cheque payments received over $50,000 will be remitted back to the Agency once the funds clear the Service NSW remitting bank account.

4. Business Continuity and Disaster Recovery

Service NSW will maintain an Enterprise Risk Management Framework focused on managing risks to Service NSW, including mitigation of the likelihood and impact of an adverse event occurring. As a function of risk management, business continuity management will enable Service NSW to minimise disruptive risks and restore and recover its business-critical services within acceptable predefined timeframes should an adverse event or other major business disruption occur.

Recovery and timeframes may be impacted when events or disruptions are related to dependencies on partner Agencies. The Parties will agree on Recovery Point Objectives and Recovery Time Objectives and associated charges prior to designing the system and will periodically review these objectives.

All systems and technology provided by Service NSW internally and through third-party vendors, operate through multiple data centres to achieve high availability. Service NSW systems are architectured, where practicable and possible, to ensure continuity of service in the event of a data centre disruption or outage.

Definitions

Recovery Point Objectives means the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down because of a hardware, program, or communications failure.

Recovery Time Objectives means the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity.

5. Continuous Improvement

Service NSW regularly reviews improvement ideas from employees and customers. We will provide you with any ideas relevant to your agency for consideration.

‘Continuous Improvement’ refers to identifying a process, system or policy opportunities that will deliver a benefit for our people, our customers or the NSW government. These improvements may be delivered in house where possible or by engaging our partnering agencies where further input or decisions are required under policy or legislation. A Continuous Improvement:

A. Puts the customer first
B. Makes the customer service job easier
C. Improves a step in a process
D. Changes the way a task is completed so that it doesn’t take as long
E. Reduces handling time and is cost effective
F. Allows others to benefit from best practices
G. Allows us to do things better locally, regionally or organisation-wide
H. Is a low-investment process change and not a policy change
I. Improves accountability within the various stages of the process
J. Removes steps that don’t add any value to a process

Service NSW will consider several factors such as cost to implement, cost savings, customer experience, team member experience and operational efficiency in prioritising continuous improvements.

5.1. Continuous Improvement Process

The parties will identify new continuous improvement initiatives on an annual basis, with a 6-monthly

check-in on ongoing continuous improvement initiatives.
When establishing a new continuous improvement initiative, the parties will classify the initiative based on whether it can be implemented as:

A. part of the ongoing ‘business as usual’ services (cost and resourcing to be absorbed by Service NSW; or
B. a new project initiative (cost and resourcing to be agreed by the parties).

A prioritisation process will be agreed upon between the parties to prioritise initiatives (for Service NSW, this will be performed by the Partnerships team).

The Agency may be required to effect policy, system or regulatory changes to assist in delivering the service process improvement, as agreed with Service NSW. Where a review of Agency policy, system or regulatory changes is requested by Service NSW from the Agency, these should be conducted within timeframes agreed between the respective Relationship Managers.

Schedule 3 – Privacy and Data Security

(a) General

(i) Service NSW may collect, use, disclose, store and retain personal information when exercising functions for the Council:

(iv) Where Service NSW exercises functions for the Council, Service NSW can share information it obtains with the Council without separately requesting the customer's consent. Service NSW can also share the information it obtains with any person that the Council is authorised or required to disclose the information to in accordance with the Service Act.

(c) Collection of information

(i) Service NSW will collect the following information when exercising functions for the Council:

(ii) Service NSW will take reasonable steps to ensure that the personal or health information it collects on behalf of the Council is accurate, up-to-date and complete.

(iii) Service NSW will provide a privacy collection notice to customers whenever it collects their information.

(iv) If Service NSW collects personal information for its own internal purposes, when exercising functions for the Council, it will ensure that the privacy collection notice meets the requirements of section 10 of the *PPIP Act* in light of section 15(3) of the *Service Act*.

(v) The notice will address each of the matters that a privacy collection notice is, by law, required to address. Service NSW will develop the content of the notice in consultation with Murrrumbidgee Council.

(d) Internal records maintained by Service NSW

(i) Under the *Service Act*, Service NSW is permitted to collect, maintain and use the following records for its internal administrative purposes, including for the purposes of its interactions with customers for whom functions are exercised:

- Details of transactions between customers and Service NSW
- The preferences of customers for transacting matters with Service NSW and Murrrumbidgee Council, and
- Other information about customers.

(ii) Service NSW collects, maintains and uses the following information for its internal administrative purposes:

- Details of transactions between customers and Service NSW
- The preferences of customers for transacting matters with Service NSW and Murrrumbidgee Council, and
- Other information about customers.

(e) Use of information

(i) Service NSW can use information in accordance with the *Service Act,* PPIP Act and HRIP Act.

(f) Disclosure

(i) Service NSW can disclose information in accordance with the *Service Act,* PPIP Act and HRIP Act.

(ii) Where Service NSW performs a transaction for a customer, when exercising functions for the Council, it will ask the customer for consent before sharing that information with a different agency, unless there is another legal basis for Service NSW sharing the information.

(g) Privacy Management plans

The parties agree to update and periodically review their privacy management plans or other relevant policy documents so that any person can ascertain whether Service NSW or the Council holds personal information relating to that person and if so, the nature of the information, the main purposes for which it is used and the person's entitlement to access the information, in relation to the services covered by this Agreement.

(h) Access to and amendment of

(i) Service NSW agrees that it will provide any individual who requests it with access to their own personal information without excessive delay and without any expense, in relation to information it holds as a result of exercising functions for the Council**.**

(i) Privacy Officer

The parties have nominated a Privacy Officer who is the point of contact for dealing with complaints, applications for internal reviews, data breaches, employee education and other privacy matters.

Privacy Officers can be contacted as follows:

Service NSW:
Privacy Officer
Service NSW
2-24 Rawson Place, Sydney NSW 2000
Phone: 13 77 88
Email: privacy@service.nsw.gov.au

Murrrumbidgee Council:

Attachment # 2 – Item # 1

Murrumbidgee
COUNCIL

Darlington Point Office
21 Carrington Street
PO Box 5
DARLINGTON POINT NSW 2706

Telephone: 02 6960 5500

Coleambally Office

39 Brolga Place
COLEAMBALLY NSW 2707

Telephone: 02 6954 4060

Jerilderie Office
35 Jerilderie Street
PO Box 96
JERILDERIE NSW 2716

Telephone 03 5886 1200

SC29

24 August 2021

2021 Regional Telecommunications Review
Department of Infrastructure, Transport, Regional Development & Communication

Email: secretariat@rtirc.gov.au

Dear Sir

Submission Regional Telecommunications Independent Review

Internet

Murrumbidgee Council has fibre to the Darlington Point Office, and yet we constantly get internet speeds which are only 20% of what we should be receiving.
It was never really noticeable when working at the office, however it was very noticeable when COVID 19 had staff working remotely. Until we received complaints from remote workers, the internet speed to the office was never tested.

It appears that in rural Australia reportable speeds and delivered speeds are not equal.

Approximately 5 km outside each of our three townships of Coleambally, Darlington Point and Jerilderie, the only connection available is Sky Muster. Sky Muster is a good option, however it is, in essence, unaffordable, and limited in up and down speeds.

Equitable access to us means a service the same in rural and remote as what is provided in urban Australia, the inequity exists in up and down speed, cost, serviceability and education.

In researching ways to provide higher speeds of internet to our Local Government Area (LGA), we tried to determined who has fibre in the ground, and who is willing to provide.

It is impossible to find out who has fibre in the ground, yet I believe 90% of it will have been installed using public funds, be it Telstra in the early days of Government ownership, NBN, Transgrid and so on.

We made great friends with Transgrid, they were very keen to work with us in providing a solution to increase speeds to our LGA. In the end we had to walk away as the costs were prohibitive. For some reason the costs with internet are disproportionately expensive, when you compare with other jurisdictions around the world. Why it that our base costs are so expensive?

As the Government contributes funds in infrastructure for internet, it should be mandated that other players have the right to utilise the infrastructure at a set fee. Our costs are high, because we are lower in population, so why do we continue to compound the problems? What I mean is, if I could see fibre mapping within Australia, I would see a Telstra fibre, beside an NBN fibre, beside an Optus fibre, beside a TPG fibre, with all heading to the same place. Just this scenario shows that we have paid 4 times the cost and, as taxpayers, consumers and customers, it does ultimately come out of our pocket. Is this not wasteful? Surely it could be mandated that everyone could utilise, for a set fee, the available infrastructure. If not, it should be Government owned. You will say that is what the NBN charter is, unfortunately NBN, like every other telco, has a profit motive, and there is no profit in rural and remote Australia, hence even our NBN is substandard.

Government silos are also killing the internet world and adding to the waste of resources. We are having a conversation with the NSW DPIE about $200M they have from the sale of the Snowy Hydro, to spend on internet and mobile coverage improvements in the bush. We went into that meeting having just heard that the NSW Education Department had given Telstra $200M to install fibre to a few schools. Why? Is this not a wasted opportunity for the towns with those schools? The NSW Government paid commercial rates for the installation, the fibre will be owned by Telstra, they (the Education Department) are paying commercial rates for the data, and the fibre is going past other local, State and Federal infrastructure, but they who own the infrastructure have not been informed, so when they seek a connection, if they have the ability, it will be 6 times the price.

Mobile

Unless you have a cellfire booster installed, forget about making a call on your mobile phone 7 km outside of any of our three towns on the Telstra network. That was the position residents and travellers of Murrumbidgee Council faced, until Council provided a 50% contribution to a new facility on a tower we already owned at Bundure on the Kidman Way. So now, when leaving Jerilderie for Darlington Point via the Newell Highway and Kidman Way, there is only a break in service for about 15 km between Jerilderie and the Bundure Tower, and a further 10km break between Bundure Tower and Coleambally, and a 5km break in service between Coleambally and Darlington Point.

Travel from Jerilderie to Narrandera on the Newell Highway, there is approximately 60km of no service area between Jerilderie and Morundah, yet there is a mobile tower at Bundure on the Newell Highway which, unfortunately for Telstra customers, is an Optus facility (I am told).

Rural Australia understands that it’s not commercially viable for the telcos to invest in rural and remote Australia, yet the need exists, and we are thankful for State and Federal Governments providing funding such as Mobile Black Spot Program.

However we need to do one of two things.

Firstly, mandate that any Government provided funds directed towards mobile coverage must allow for roaming by all carriers. Not just co-location of each other’s equipment (that should be mandated in the ities), but one set of equipment signalling all carriers. I know this statement contradicts the equitable stance, however I am sure rural and remote Australians would be happy to pay premium (say $10 a month) on top of their current plan to ensure roaming.

Why is it I can take my Telstra phone to the USA and immediately be roaming on ATT or in Canada on Rodgers, but I cannot travel along the Newell Highway, leaving Jerilderie on Telstra, roam onto Optus at Bundure, then back to Telstra past Morundah and Narrandera.

The second option would be for Government to own the infrastructure. As mentioned, rural and remote Australia are not commercially viable to the telcos. In the same way as its not commercial viable for a health company to build a private hospital in rural and remote Australia.

Government build the towers, Government owns the transition equipment, Government maintains the equipment, and Government receives an annual payment from the telcos. Look at it in the same way as the Commonwealth Bank pays Australia Post to deliver their services in Post Office across Australia, even in rural and remote Australia. ATM X, Armaguard’s Automatic Teller Machine, must have some agreement with ANZ to allow ANZ customers to use these ATM’s without paying a fee, while non-ANZ customers are charged. There are plenty of models out there. Local Government can assist you here, as we have infrastructure, towers, tall buildings and power dotted all over.

Murrumbidgee Council contributed just under $400,000 to Telstra as our 50% share of the facility at Bundure (Kidman Way), plus we already owned the tower. We know a little about equipment needed, I would hazard a guess that the total equipment cost would be less than $100,000, so in essence our contribution is to cover the cost of the next 10 or 20 years the tower will be in service.

What funding contribution under the Mobile Black Spot Program actually goes to towers and equipment, and how much goes to the operational cost and ultimately the profit of the telcos?

<u>Summary</u>

1. Where the Government provides funds under the Mobile Black spot Program, one condition must be a mandatory roaming to other mobile providers;

2. Where the Government provides funds under the National Broadband Network and/or Regional Connectivity Programme, one condition must be that any fibre installation or other capital must be made available to other providers;
3. Failing the ability to enshrine items 1 and 2 above, that the Federal Government (not via NBN) install, own and operate the backbone infrastructure of fibre, data exchanges, towers and cellular equipment, licencing telcos and providers the use of infrastructure;
4. That the Federal Government set the minimum speeds, 100MBPS up and down;
5. That the price for delivering the minimum speed be regulated;
6. These be mandatory requirements of obtaining and maintaining a telecommunications licence in Australia.

Yours faithfully

John Scarce
GENERAL MANAGER

Murrumbidgee COUNCIL

ICT Strategy

June 2021

Prepared by:

Colin Thompson

Veritech Senior Consultant

Veritech Corporation Pty Ltd

Table of Contents

Introduction

Purpose

The purpose of this document is to record the Information Communications and Technology (ICT) Strategies of Murrumbidgee Council (Council). These strategies form the governance for the management and advancement of the ICT systems in supporting the business strategies of Council.

Objectives

The objectives of Council's ICT Systems and this Strategy are:

- Deliver reliable ICT systems that underpin Councils server delivery
- Look to drive innovation through ICT
- Implement strong Governance of ICT Systems

Influences

The development of this strategy has been influenced by several sources. Some internal to Council, other external such as community or other government bodies.

Sources influencing this strategy are:

- Corporate governance requirements
- Operational Plan & Delivery Programme
- Community Strategic Plan
- Auditor (External & Internal)
- Enterprise Risk Management

Terminology

The following terms and acronyms are used throughout this document:

BCP	Business Continuity Plan, provides details on major incident management and plans for keeping the business operational during or as a result of a
CCTV	Closed Circuit Television, a private camera system that is centrally
Council	Murrumbidgee Council
Data Sovereignt	Refers to data subject to the laws of the country in which it has been
DRP	Disaster Recovery Plan, document(s) that detail the recovery steps from a disaster event. Generally, sits under the BCP providing detailed
ICT	Information, Communications and Technology
Malware	Software that installs itself onto vulnerable computers where it either extracts information or acts as a remote agent (or BOT) to execute
MFA or 2FA	Multi or Two Factor Authentication, an additional layer of security requiring people to authorise new logins by approving or entering a code from a
MSA	Managed Service Agreement Covers the requirements of the MSP when managing Council's ICT environment
MSP	Managed Service Provider
Phishing	Emails intended to extract information or funds from people, generally by
SPAM	Unsolicited emails the flood mailboxes with advertised content.
Virtual Servers	Software versions of physical servers, they operate the same as a physical server however have the benefit of sharing underlining infrastructure to improve utilisation of hardware resources. Also makes them more portable

Business Services

To effectively conduct Council operations, numerous ICT services are maintained. The following table layouts the current set of services.

Business Service	System(s)	Requirement Source	Delivery
Finance	Civica Authority	Internal	On-premise
Purchasing	Civica Authority	Internal	On-premise
Payroll	Civica Authority	Internal	On-premise
Payment (inc Rates)	Civica Authority	Internal	On-premise
Work Order	Civica Authority	Internal	On-premise
Fleet	Civica Authority		
Document Management	Content Manager	Legislation	On-premise
Mapping	IntraMaps	Internal	On-premise
Mapping (Corporate)	Mapinfo	Internal	On-premise
DR Management	Recover		
RMS Roads and other Council assets (Operational)	Reflect	RMS	On-premise
Email	Exchange 2016	Internal	On-premise
Webcast	Blue Jeans	Legislation	Cloud/On-premise
Inter-site networking	ATI Australia long range wireless links	Internal	On-premise
Phones	Alcatel-Lucent	Internal	On-premise
Internet	Telstra NBN	Internal	On-premise
Internet	Fibre NBN DP		
Email Security Scanning	Trend Hosted Email Security	Internal	Cloud
Work, Health & Safety	Safeplan	RMS	On-premise

Cloud Services

Cloud Services as a generalisation, involve a company hosting their own solution and providing this to many businesses as a service. As opposed to the traditional method of requiring each business to obtain hardware, the software and implementing/maintaining this themselves. The benefit of the cloud services path is smaller business can now access solutions that were previously only available to enterprises that could afford to implement and maintain solutions themselves. Often the service is available in a fraction of the time required to implement on-premise.

Cloud services do come with a number of factors that Council needs review when considering the adoption of a cloud service. These include:

- Data Sovereignty, best practise involves keeping customer and financial data onshore.
- Security of information in transit and while stored, encryption and access methods are big considerations.
- Cost, sometimes it’s more cost effective to self-host.
- Reliability of local internet services to access the cloud solution

Council will be developing a Cyber-Security policy that will build on these points and detail what needs to be done when considering a Cloud based platform or tool.

Current Plans

The environment around the current services is reasonably stable with no plans for dramatic changes, there are however several activities in progress at present, or in the short term.

Development of IT Maturity

Several activities are planned across the ICT landscape to improve the maturity of IT operations at Council. Some of these include:

- Revision and development of policies
- Revision of BCP documentation and testing
- Further development of staff awareness on ICT and Cyber Security risks
- Development of financial plans for ICT hardware changeovers

Work Health and Safety Management System

Council are currently in the process of implementing a full Work Health and Safety Management (WHSM) system across all areas of council. The system is called “Safeplan” and will work off the current Intranet.

Timing: In Progress

Future Initiatives

Asset Management Systems Review

Currently Council is using the “Reflect” asset management system and has plans for developing operational procedures with the Roads Maintenance area based on Roads and Maritime Services (RMS) guidelines. Once completed, it’s expected that these procedures could be used across other asset classes also maintained in “Reflect”.

Council will be looking to do a review of its Asset Management System requirements and capabilities in the future.

Other factors:

- New staff within the asset management space are looking at alternate asset management platform options.
- “Reflect” has recently been purchased by Civica (supplier of “Authority”) with plans to integrate this into the “Authority” system. This will be a space to watch to determine whether this will address Council’s Asset Management requirements.

Timing: Beyond FY22

Customer Relationship Management

Since the implementation of Civica Authority, there has been plans for implementing Customer Relationship Management (CRM) within Authority. This was held off until other core services were bedded down, with the expectation that this be reviewed sometime after Q3 FY21.

Timing: On hold

Time and Attendance

Now that the Council has completed the consolidation of employee data into Authority, its starting to look at timesheet processes across the sites.

The decision has been made to leverage the Time Sheet solution within Authority for online time sheets. This implementation is schedule to commence late in FY22.

Timing: Q3 – 4 FY22

Online Learning Management and Training system

Council has started doing some background research into options for Online Learning Management and training systems.

It is proposed to conduct a review of requirements and systems in the new

financial year. Timing: Q1/2 FY22

Future Initiatives

Online Requisitioning

Council is looking to move to online requisitioning, leveraging the existing functionality with Authority. This project will be implemented late in FY22, inline with the online time sheets.

Timing: Q3 – 4 FY22

Governance

Governance within an ICT environment covers a number of areas or functions. In this section the following items are addressed:

- Risk
- Business Continuity Planning
- Data Protection
- Cybersecurity
- System Access

Risk

While an essential business tool, ICT systems introduce some unique business risks (negative and positive) that need to be managed effectively.

As Council has a developing Corporate Risk Management process, ICT will endeavour to integrated into this process as it develops. An ICT Risk Register has been developed under the MSA and will be maintained by the MSP.

Business Continuity Planning

Council's Business Continuity Plan (BCP) needs considerable updating to reflect the updated operations across all areas. This includes the ICT components of the BCP.

BCP Approach

During FY21, work has been completed on the development of an ICT Subplan with recovery instructions. This plan will is based on the recovery requirements of the different business units and aims to address a number of potential scenarios that could be reasonably foreseen as potential incident events.

BCP Resources

Council has some replication of information between sites at present for Disaster Recovery (DR) purposes and access to a cloud-based recovery environment via its subscription to Datto backups.

BCP Improvements

During FY21 the implementation of the Datto backup solution has greatly improved Council's coverage and ability to manage disaster situations involving IT Infrastructure. At this stage these improvements need to be tested.

BCP Testing

Until proven, a BCP cannot be relied upon to successfully deliver restored services. Therefore, Council in conjunction with its MSP will conduct annual testing of the IT Sub plan, and corresponding revision to address areas requiring improvement.

Timing: Q2 FY22

Governance

Data Protection

Having access to reliable data sources is critical to the operations of Council, therefore several layers of protection have been applied to data.

- Protection of unauthorised access
    - "Cyber Security" is a threat faced by all businesses connected to the Internet. Several protection methods are currently in place at Council, the details of which are expanded in the Cybersecurity section.
    - Internally systems access will be restricted to that required to complete an employee's duties. System Access section below provides further detail on this.
- Hardware Redundancy
    - The use of servers with hardware redundancy on storage and power helps to ensure data integrity in the event of component failures. All servers in use and to be purchased will continue to leverage hardware redundancy.
- Backups
    - Backups are intended for retrieval of lost or legacy data. Further details are available the Backups section below.
- Disaster Recovery
    - In the event of a major failure or disaster, the Datto data-centre has backups of key systems that can be brought online to restore services. Further details are available the Business Continuity Planning section.

Backups

During FY21, Council moved to a new cloud-based backup solution from Datto. Using this solution, backups are conducted at the Virtual Server level to a local device, then synchronised to the Datto data centre after hours. This solution provides:

- Backup checks via automated starting of backup images to verify they start correctly.
- Ransomware detection built-in
- Offsite storage and recovery

capabilities Schedules are:

- Hourly backups of regularly changing servers (databases, email, etc) between 9am and 6pm weekdays. Last backup of the day is written to the Datto cloud.
- Nightly backups on other servers each day, which are also written to the cloud.

Data Retention

Council has subscribed to the "infinite" retention on backups, which covers:

- Onsite:
    - All hourly backups kept for 7 days
    - Then the final daily is kept for 1 week
    - Then a weekly kept for 1 month
- Offsite:
    - All hourly backups kept for 7 days
    - Then the final daily is kept for 1 week
    - Then a weekly kept for 1 month
    - A monthly backup is then kept forever

Governance

Cybersecurity

Threats to Internet-connected businesses come with an ever-changing array of techniques, requiring a multi-pronged approach to Cyber-Security. This is an area that Council in conjunction with its MSP will continuously review looking for opportunities to safeguard resources from being compromised.

Council is currently managing Cybersecurity via:

- Awareness training
- Security Infrastructure
- Anti-virus and Malware protection
- Email SPAM, Phishing and Malware protection.
- Patch Management

Awareness

Many of the current threats target people rather than systems to gain access to information allowing them access via the “front door”. Therefore, increasing employee awareness of these tactics is crucial to maintaining the integrity of Council’s systems.

Council will use combination annual security awareness training and staged phishing emails to aid in the development of staff awareness of cybersecurity. Council’s MSP will responsible for the delivery of these education services.

Infrastructure

Firewalls are an essential layer of protection sittings between the Internet and Council’s resources. These devices manage connections to and from internal systems which natively are not designed to directly interface with the Internet. Additional modern Firewalls also scan incoming traffic for threats and drop traffic that could reduce performance.

For perimeter security, Council leverages Endian Firewalls, configured, and maintained under the MSA.

Even though a perimeter Firewall is in place, it is also necessary to add protection at the desktop/server levels against threats that may enter the network via other paths (Eg. USB device, Foreign computer, Email). To secure these internal devices, Council is leveraging the “Trend Micro Worry-Free Business” solution which also includes a desktop Firewall.

Anti-virus, Malware

Desktop level protection of devices is a must; therefore, Council has implemented the “Trend Micro Worry-Free Business” solution to provide Anti-Virus, Malware and Firewall protection on all internal computers.

Email

Email is such an available method of transferring information that it has become a preferred vector for gaining unauthorised access to other systems.

Council’s uses an in-house hosted email system (Microsoft Exchange 2016) with the addition to a third-party security scanning tool called “Trend Micro Hosted Email Security” scanning incoming email for threats.

Governance

Future considerations will include reviewing the requirement for Multi-factor Authentication (MFA) on remote access including emails, or migration to hosted Office 365 platform which would include MFA.

Patch Management

Patch Management is the process of applying security fixes and updates to computers and networking equipment.

Under Council's MSA, Patch Management is the responsibility of the MSP and is focused on Microsoft products, Anti-virus products and Firewall devices. Patch management checks are conducted as part of the monthly "Server Check" functionality.

System Access

Computer and financial systems

All requests for computer access are forward to Vicki Sutton or Sue Mitchell, if approved are forwarded to Council's MSP for action.

- Authority Access via i_al110 User Administration – iservices System/Web Platform

Remote Access

Council provides remote access to contractors and selected staff to enable work from outside the office. There are two access methods available:

- RDPlus, which is a secure connection using a web browser to gain remote control of a dedicated computer within the office.
  Normal use is by employees on their home computer, controlling the work computer.
- OpenVPN, which provides a secure tunnel from the persons computer back to the office network.
  Normally used by employees with laptops, or contractors.

Reviews

In order to ensure that the correct people have the appropriate and approved access, regular reviews will be conducted to confirm appropriate access is in place.

This process will be initiated with a general security review to be managed Council's MSP. This
review will also cover Authority and Content Manager systems.

Following on from this review, systems Access reviews will be reviewed annual basis, conducted by the MSP.

Timing: Q1 -2 FY22

Governance

Software Licensing and Versioning

Council utilise a variety of software packages in completing its required duties, each of these packages have their own set of licensing rules that Council must comply with to legally use them. Additionally, as software vendors enhance their products, they release new versions, which if left unmanaged can lead to mismatched product versions spread throughout the business, resulting in compatibility issues.

Council is seeking to stay in control of licensing requirements and maintain a standard set of applications across the business. As part of the merger, Council developed a register of software applications and licenses. This register will be supplied to the MSP, refreshed and used to assist with planning and budgeting of upgrades and software maintenance.

System Documentation

Accurate systems documentation is key to effectively maintaining ICT systems. This documentation is consulted regularly when troubleshooting and considering design changes. It's also the most effective way to share knowledge between people that may not be in the same location.

Council relies on its MSP to develop and maintain this information.

Presently this information is maintained in the MSP's Wiki.

Resourcing

Council has a wide range of responsibilities that are supported by ICT services, maintaining all the required ICT skillsets inhouse is not practical for in regional locations. Therefore, Council will use a combination of in-house and outsourced resourcing to cover off its ICT resourcing requirements.

Inhouse

Council does not have any dedicated inhouse resources for the delivery of IT Services, however, to keep MSP costs under control, Council has taken onboard some minor ICT administrative tasks (e.g. Password resets, Email signature changes)

This has been achieved by delegating permission to two security groups that people can be added to in order to reset passwords or update account details.

Outsourced

There are several areas of Council's ICT landscape that has been outsourced to specialist providers. The major areas would include:

- ICT Management, Computer systems and Network management
  Covers off working with Council on the management planning to meet business requirements and objectives, as well as the day to day operational management of in-place systems.
- Phone Systems Management
  Covers off the ongoing support and changes on the phone system used across Council's
  sites.
- Building Access Systems
  Covers off the maintenance and any changes required within the building management system.

Some of the minor or more targeted areas include:

- Civica Authority consulting.
- Document management

Hardware life cycles

Over time computer systems age and become more prone to failure, and generally, the demands of the systems hosted on them increase beyond the original design specifications. Therefore, computer systems need to be rolled over at regular intervals to ensure they can effectively meet business requirements.

Assisting with the planning of these rollovers on an annual basis will form part of the MSP’s responsibilities. The following guidelines will be used in developing the plans for budgeting and implementation.

Servers and storage

Generally, a server operating within the original design specifications should be considered to have a useful life of four years. Storage systems with solid-state storage could be extended to five or six years with suitable capacity.

At the time of writing Council had 3 physical servers and 2 legacy servers. A review of the age and capacity of these systems will be conducted for the development of budget plans with Council.

Workstations

The aim of providing workstations to staff is to aid in the delivery of work, therefore Council intends to make sure workstations are aiding and not hindering staff functions by regularly rolling over workstations at the end of their useful life. The useful life of a well-provisioned workstation would be considered as four years. This expectation may be reduced on laptops due to wear and tear of being moved around, battery life and generally lessor specifications to achieve mobility.

The annual rollover plans will include provisions of a quarter of the fleet each financial year. This provides a healthy basis of computers whilst spreading the expense over this period.

Networking Equipment

The demands on networking equipment are generally reasonably static, and as long as they have suitable throughput capacity should achieve a useful life of five to six years. Examples of networking equipment include Routers, Switches, Firewalls, Wireless Access Points, and controllers.

Plans for rollover of networking equipment will be incorporated with the annual rollover plans.

Printers/Copiers

Council has found that printers/copiers typically have a useful life of around three years for large capacity units and 5 years for smaller units. With a lot of moving parts, they do tend to require more parts and maintenance as they age.

Summary of Actions

The following tablet summarises the actions discussed throughout this document.

Section Referenced	Tasks	Assigned	Timeframe
Current Plans	Revision and development of policies	Veritech	Current – Q4
Current Plans, Business Continuity	Revision of BCP Documentation and testing	Veritech	Current - Q2 FY22
Current Plans	Develop staff awareness on ICT and Cyber Security	Veritech	Q2 FY22
Current Plans	Development of financial plans for ICT Hardware	Veritech	Q2 FY22
Current	Work Health and Safety Management system	Council	In Progress
Future Initiatives	Asset Management system review	Council	In Progress
Future Initiatives	Develop an Internal Audit Program	Council	Complete
Future Initiatives	Customer Relationship Management	Council	On-hold
Future Initiatives	Time and Attendance system review	Council	Q3 – 4 FY22
Future Initiatives	Online Learning Management and Training system	Council	Q1 – 2 FY22
Future Initiatives	Online Requisitioning	Council	Q3 – 4 FY22
BCP	Testing	Council/Veritech	Q2 FY22
Cyber Security Awareness	Phishing Simulation	Veritech	Annual
Cyber Security Awareness	Phishing Training	Veritech	Annual
System Access	System Access Reviews	Veritech	Q2 FY22
System Access	Software register update	Veritech	Q1 FY22
Resourcing	IT tasks for inhouse resources	Veritech	Complete
Hardware	Hardware capital plan	Veritech	Q2 FY22

Version Control

Version	Author	Descriptions	Date
Draft	Col Thompson	Draft document created for review.	
Draft 1	Col Thompson	Draft updated following workshop	29.5.2020
Draft 2	Col Thompson	Updated following meeting with Sue	21.6.2021

Appendix A – IT Contracts Register

Contract	Short Description	Provider	Document	Contract Start	Renewal or Review
IT Managed Services Agreement	IT Management and Support	Veritech Corporation		1/8/2017	1/8/2020
Phone System	Phone System Management and	Advanced Communications			
Building Access Systems	Access controls across Councils sites	EACOM			
Authority Maintenance	Authority support and consulting	Civica			

Murrumbidgee COUNCIL

BCP IT Sub plan

June 2021

Prepared by:

Colin Thompson
Veritech Senior Consultant

Veritech Corporation Pty Ltd

Table of Contents

1 Introduction

1.1 Purpose

This sub plan is intended to sit under Council’s master Business Continuity Plan (BCP) and provide additional details specific to Information Communications and Technology (ICT) related services, and provide recovery instructions.

1.2 Objectives

The objectives of the sub plan are:

- Identify current ICT services that may be required during or following an incident
- Document agreed recovery targets
- High recovery provisions
- Develop potential scenarios and checklists recovery
- Document recovery procedures
- Provide communications templates

1.3 Use of BCP

This BCP has been designed to be used by personnel with ICT knowledge to response the incidents that have triggered the initiation of BCP processes.

Murrumbidgee Council’s contracted Managed Service Provider is Veritech Corporate Pty Ltd.

1.4 Assumptions

No assumptions recorded.

2 Services

2.1 Existing Services

Council's maintains numerous ICT systems to support business activities, the following table is intended to identify these business services and the supporting systems.

Underlying infrastructure systems (E.g. Active Directory, SQL) will not be list here but will be factored into the recovery requirements and are listed in the ICT Dependency Matrix within Veritech's documentation.

Service	System	Hosting
Payment Processing, Rates processing, Applications (Development, Cemetery), Purchasing, Inventory Management, Payroll, Fleet	Civica Authority	On-premise
Business Intelligence System	Civica BIS	On-premise
Credit Card Payments	Banking Terminals	On-premise
Email	Exchange	On-premise
Mapping	Intramaps	On-premise
Mapping (Corporate)	Mapinfo	On-premise
Document Management	Content Manager	On-premise
RMS Asset Management	Reflect	On-premise
Phones	Alcatel-Lucent PBX	On-premise
File Storage	Fileserver	On-premise
DR Management	Recover	
Webcasting	BlueJeans	On-premise/Cloud
Inter-site networking	ATI Wireless	On-Premise
Internet	Telstra NBN	On-premise
Internet	Fibre NBN (DP)	On-Premise
Remote Desktop	Terminal Services	On-premise
Work from home	RDPlus	On-premise

2.2 Service Recovery Targets

Recovery targets are driven by the:

- Recovery Time Objective (RTO) – measure of how quickly services need to be restored before they cause major impact on business activities. Keeping in mind that this is a disaster not just a business interruption, the shorter this target is, the more expensive the recovery provisions will be.
- Recovery Point Objective (RPO) – is the maximum tolerable data loss, measured in time (E.g. hours, days). This typically refers to the period of time between the last successful backup and the occurrence of a disaster event. Again, the shorter this period is, the more expensive the backup costs.

Together these measures help determine the levels of redundancy and backups that need to in place for business to continue functioning following an incident.

2.2.1 Recovery Time Objective

The recovery time objectives in the following table have been established following discussions with Vicki Sutton and Sue Mitchell.

RTO refers to the period following a disaster that Council can survive without a service before in starts to cause major business interruption.

Service	Requested RTO	ievable RTO	Comments
Authority – Payment Processing	2 Days	1 Day	Manual receipting option available
Authority – Payroll / Fleet	2 Days	1 Day	Have the option to replay the last banking if required
Purchasing	2 Days	1 Day	
Rates	2 Days	1 Day	
Applications	2 Days	1 Day	Now more dependant on the State Government portal
BIS	1 Week	1 Day	
Credit Card process	2 days		Banks to provide, all credit card facilities are in Council Offices only.
Email	1 Day	1 Day	
Mapping (Intramaps)	1 Week	1 Day	
Mapping (Mapinfo)	1 Week	1 Day	
Content Manager	1 Day	1 Day	
Reflect	1 Day	1 Day	Software and data is synced to the cloud.
Phones	1 Day	1 Day	
File Systems	1 Day	1 Day	
DR Management (Recover Software)			Able to access as required
Web Casting (Blue Jeans)	1 Week		Alternate site available (E.g. Jerilderie or Darlington Point)
Inter-site Wireless	2 Days		Alternate options required
Internet Access	2 Days		
Remote Desktop	1 Week	1 Day	

RDPlus	2 Days	1 Day
Sewer Alarms		
Building Security	1 Week	

2.2.2 Recovery Point Objective

The recovery point objectives in the following table have been established following discussions with personnel within Council.

The RPO refers to the “acceptable” data loss following a disaster event, measured in time.

Service	Requested RPO	Achievable RPO
Authority – Payment Processing	2 Days	1 Day
Authority – Payroll / Fleet	1 Day	1 Day
Purchasing	2 Days	1 Day
Rates	2 Days	1 Day
Applications	2 Days	1 Day
BIS	N/A	N/A
Credit Card process	N/A	N/A
Email	1 Day	1 Day
Mapping (Intramaps)	2 Days	1 Day
Mapping (Mapinfo)	2 Days	1 Day
Content Manager	1 Day	1 Day
Reflect	N/A	
Phones	N/A	
File Systems	1 Day	1 Day
DR Management (Recover Software)		
Web Casting (Blue Jeans)	N/A	
Inter-site Wireless	N/A	
Internet Access	N/A	
Remote Desktop	N/A	
RDPlus	N/A	
Sewer Alarms	N/A	
Building Security	N/A	

3 Recovery Provisions

At present, Darlington Point is allocated as the primary IT services hub with Jerilderie as a fail over or recovery location.

The following provisions are currently in place:

- Replication for Email services to Jerilderie with automated fail over
- Datto backups are stored within the Datto Cloud. Limited capacity local recovery exists on the appliance if its available following an event.
  Large scale event will require recovery within the Datto Cloud.

Other provisions

- Phone System – Advanced Communications have offsite backups of the phone system and spare equipment to reconstruct it.

3.1 BCP Document Storage

Electronic copies of this plan will be made available to Murrumbidgee Council, with the master copy stored with Veritech's site documentation for Council.

Hard Copies are to be distributed to key recovery team members. A record of these is to be kept in the table below so new copies can be arranged once updates are made.

3.2 BCP Hard Copy Register

The following register is to be used in tracking hard copies of this BCP Sub Plan.

Current Version:

Published Date:

Name	Position

4 DR Checklists

The nature and extent of a disaster event means that a recovery is not necessarily a matter of just restoring systems, which in some cases could be destructive.

To aid with determining which systems need to be restored following a declared disaster event, a series of DR Checklists have been created to highlight what needs to be recovered.

The detailed checklists are located at the rear of this document as Appendices.

Checklists

- Appendix A – DR Checklist – Loss of computer room (Darlington Point)
- Appendix B – DR Checklist – Internet Feed Loss
- Appendix C – DR Checklist – Virtual Server Host Failure
- Appendix D – DR Checklist – Prolonged power loss at main council building
- Appendix E – DR Checklist – Pandemic Outbreak
- Appendix F – DR Checklist – Loss of inter-site wireless links

5 Recovery Instructions

The following section is intended to provide the recovery instructions as referenced within the DR checklists; therefore, recovery is not intended to be completed by just moving from top to down within the follow list.

5.1 Internet Access

Various options existing for restoring Internet access. Most likely scenario is that an outage will only impact one site. Therefore the following procedure focuses on diverting Internet access via the other primary site.

Do the following in the Endian of the site with failed internet:

- For Darlington Point; In the Endian under routing, create a new routing entry for 0.0.0.0 to go via 172.20.1.1.
- For Jerilderie; In the Endian under routing, create a new routing entry for 0.0.0.0 to go via 172.16.1.1.

5.2 Restore Phone Services

Advanced Communications carry the parts required and backups to restore the phone system.

- Notify Advanced Communications that restoration is required using the Communication Appendix A. Location for the phone system to be installed will need to be provided.

Estimate time to complete: 6 hours

5.3 Datto Cloud Restoration

Restoration during a disaster event is best coordinated through Datto support.

Details:

Phone: 02 8015 6826

Email: support@datto.com

Model: S4P10

Serial: D05099D93759

5.3.1 Recovery Concept:

The “data centre” previously located in the Darlington Point office will restored within the Datto Cloud virtualisation environment, this includes restoration of in/outbound internet services. The Datto cloud will become the central site for all IT services, until the Chambers building (or alternative site) resumes in normal operations.

Recovery Process:

- Restore virtual machines within Datto Cloud
- Implement site to site OpenVPN connections from each location into the Datto Cloud network. (Datto assistance is required to complete this step).
- Map incoming Internet Services.

Note: Veritech server documentation contains the CPU and RAM details that will be required when recovering each Virtual Server.

5.3.2 Services to be recovered

This table lists the services and corresponding systems that need to be recovered. These are listed in preference order, don't move to the next group until the previous one is finished due to dependencies.

		Systems To recover	Business Group to verify	Signed Off (Date, Time, Person)
1	Domain Services	Newell	IT	
2	SQL Services & Civica	Bascule, Sturt	IT	
2	Email Services**	Billabong	IT, Information Services Officer	
3	Content Manager	Bucyrus	Information Services Officer	
4	Mapping	Waddi	GIS Officer	
4	File Storage	Levee	Information Services Officer	
5	Remote Desktop and	Dragline, Goanna	Information Services Office	
6	BIS	Bonna	Finance Manager	

** Email Services will be internal only until the incoming services are remapped.

5.3.3 Site to Site VPN

Site to site VPN is used to reconstruct the missing network infrastructure between sites. The linked article below contains the Datto instructions for establishing site to site VPN.

https://help.datto.com/s/article/KB360032324171

Note: In the scenario with loss of either Darlington Point or Jerilderie offices, Coleambally should still have access via the other office as they sit in the middle with the point to point links.

5.3.4 Map internet services

Incoming and some outgoing internet services need to be mapped to the required VM's, then the public DNS records updated.

5.3.4.1 Incoming Services

For each service complete the following:

- From the Datto "LaunchPad", press "Port Forwarding".
- Enter the internal IP address and port number of be forwarded.
- Record the public address that is displayed once the "Apply" button is pressed.
- Update and publish the DNS record on Veritech's NS1.

Known services to the updated:

Service	DNS Name	Internal IP	Port(s)	Public IP from LaunchPad
Email	Mail.murrumbidge.nsw.gov.au	172.16.2.20	25, 80, 443	<only available once recovery is initiated>
RDPlus	dp.murrumbidgee.nsw.gov.au	172.16.2.130	446	

5.3.4.2 Outgoing Services

The following updates are required for outgoing internet services:

- Trend Micro HES. Add the outgoing public IP address to the "User-defined mail servers" listing under the HES Domain configuration.
- Civica SecureLink. Connection from Bascule to 124.47.169.51 port 22.

5.3.5 User VPN updates

Once the infrastructure has been recovered, staff will be looking for VPN to enable work from home or alternate locations outside work ones.

Configuration is completed via the Datto launch using the following instructions: https://help.datto.com/s/article/KB204736574

5.4 Datto Local Restoration

The following instructions cover restoration of virtual servers to the local Datto device.

Key servers to recover:

1. Newell – Domain Controller
2. Billabong – Exchange
3. Bascule – Authority (includes SQL databases) If

capacity exists:

4. Bucyrus – Content manager
5. Levee – File Server (not critical as everything is replicated to Felix in Jerilderie.

Recovery steps to be performed for each of the above servers:

- Access your Datto portal: https://portal.dattobackup.com/
- Open “BCDR Status”
- Open the “Device Web” on “PaddleSteamer”
- Click “Restore”
- Select the system to restore
- Select “Local Virtualisation”
- Select the recovery point, then “Start Restore”
- Update the VM resources based on the original guest resources
    - specifications on Veritech’s Wiki: http://wiki.vcorp.local/Clients/BlandShireCouncil/BscServers
- Set the Network Option to “Bridge to eth0, 172.16.0.0/16”
- Press “Apply”, then “Start VMs”
- Test the VM

6 Communications Templates

6.1 Phone System – Advanced Communications

Hi Support,

Murrumbidgee Council has suffered a disaster event which includes the loss of the phone system within the Council office building.

As a matter of urgency, can we arrange for a recovery system to be installed at:

- Recovery Crisis Centre location: ______________________________
- Address:

IT Recovery Contact: ______________________ Mobile:

Regards

<Name>

<Position>

6.2 Computer Purchases – Veritech

Hi Veritech,

Following the disaster event, <Event name>, Murrumbidgee Council is need of urgent replacement systems.

Please arrange the supply, build and installation of the suitable hardware for the following:

- <Number of> x Servers, <minimum specification>
- <Number of> x Laptops, <minimum specification>
- <Number of> x Desktop Computers, <minimum specification>
- <Number of> x Firewalls
- <Number of> x Switches, <minimum ports>

The installation location for this equipment should be confirmed with the IT Recovery Contact.

IT Recovery Contact: ______________________ Mobile: ________________

Regards

<Name>

<Position>

6.3 Telstra – Re-directions

Managed within the Corporate plan.

6.4 ATI Wireless

Hi ATI,

Following the disaster event, <Event name>, Murrumbidgee Council is need of urgent restoration of wireless infrastructure at ______________________

Please coordinate the recovery with our IT Recovery Contact.

IT Recovery Contact: ____________________________ Mobile: ______________________

Regards

<Name>

<Position>

7 Contacts

Resources	Company	Contact	Number(s)	Email
Phones	Advanced Communications		02 6922 2222	service@advancedcomms.com.au
		Andrew Baggio	0427 165 558	andrew@advancedcomms.com.au
		Joel Moller	0400 165 554	joel@advancedcomms.com.au
Building Access	EACOM		02 6964 2033	sales@eacom.com.au
Telstra Services	Telstra – Account Executive			
Telstra Faults	Telstra		132 999	Account Number: 477 9856 000
IT and Communications	Veritech	Livio Mazzon	02 6964 5377 0408 527 251 0428 235 871	livio@veritechcorp.com.au Livio.mazzon@gmail.com
Inter-site Wireless Links	ATI Australia	Brent Dennis	Office 02 9901 8400 Direct 02 9901 8414 Mobile 0409 399 735	Brent.Dennis@ati.com.au

Appendix A – DR Checklist – Loss of computer room (Darlington Point)

Scenario: Incident involving the loss of the main computer room in Darlington Point.

Potential Impacts:

- All servers and data lost
- Phone system lost
- Primary internet feed lost
- Inter-site network traffic routing lost

Assessment:

Yes	No	Item Assessment
		Are there any of the key servers available? Key Servers: Billabong, Bascule
		Is the firewall accessible? DP: 172.16.1.1, Jer: 172.20.1.1, Coly: 172.17.1.1
		Is the computer room physically accessible with the possibility to retrieve any equipment?
		Is the Internet accessible?
		Is networking to other site working? Ping: 172.16.1.1 (DP), 172.20.1.1 (Jer), 172.17.1.1 (Coly)
		Are the phones working?

Nominated IT Recovery location: ______________________________

Nominated Crisis Recovery location:

IT Recovery Team:
Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
  - Responsible for defining recovery steps required
  - Responsible for coordinating ICT recovery operations
  - Reporting Director of Corporate & Community Services every 2 hours
- **IT Team members:**
  - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
  - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery:

Day 1:

- **Servers Option 1: Relocate servers to recovery location (if they are accessible)**
  - Only an option if they are physically accessible
  - Assigned to: ______________________________
- **Servers Option 2: Initiate Datto disaster recovery**
  - Section 5.3 Datto Cloud Restoration
  - Assigned to: ______________________________
- **Restore Phone Services**
  - Notify Telstra and redirect (managed within the corporate plan).
  - Notify Advanced Communications of event and requirement to recover phone system to the “Crisis Recovery Location”
    - Communications template: 6.1 Phone System – Advanced Communications
  - Assigned to:
- **Establish site to site VPN to Datto Cloud**
  - Site to Site VPN. Section 5.3.3 Site to Site VPN
  - Assigned to: ______________________________

Day 2 – 5:

- Place orders for replacement server hardware/racking

Appendix B – DR Checklist – Internet Feed Loss

Scenario: Incident involving the loss of the main internet feed to council office in Darlington Point or Jerilderie.

E.g. Backhoe digs through fibre or Telstra network failure

Potential Impacts:

- Incoming servers from the internet will stop working (Email, Remote Access)

Assessment:

Yes	No	Item Assessment
		Is Internet access from PCs in the Jerilderie office working?
		Is Internet access from PCs in the Darlington Point office working?
		Is the Internet working via 4G? (Potential alternate route)
		Is the network between Darlington Point and Jerilderie working? Do ping test to each end. DP: 172.16.1.1 Jer: 172.20.1.1

Nominated IT Recovery location: ______________________________

Nominated Crisis Recovery location:

IT Recovery Team:
Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
  - Responsible for defining recovery steps required
  - Responsible for coordinating ICT recovery operations
  - Reporting Director of Corporate & Community Services every 2 hours
- **IT Team members:**
  - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
  - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery:
Depending on the responses above apply one of these options, which are listed in preference order.

Internet is still working in the other office

- Route traffic via the other office: 5.1 Internet Access

No Internet is either office. An assessment will be required to determine what other options are available, then integrate these into the solution.

Appendix C – DR Checklist – Virtual Server Host Failure

Scenario: A server hosting virtual servers has catastrophically failed.
E.g. Component failure leading to damage to other critical components.

Potential Impacts:

- Guest servers will not be accessible, could stop people processing business transactions via Civica Authority or other systems.

Assessment:

Yes	No	Item Assessment
		Is the outage restricted to just the one physical host?
		Are there other issues that may be causing issues? E.g. Power fail, switch failure.
		Has the fault impacted the storage systems? E.g. Is the file system of the server still functional?
		Is it likely the guest VM's are operational if the hardware was restored?
		Is it likely the issue could be recovered within 4 hours on the failed host?
		Is there capacity else where to restore critical guests providing critical services? Eg. Alternate host or on Datto appliance.

Nominated IT Recovery location: ______________________________

Nominated Crisis Recovery location:

IT Recovery Team:
Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
  - Responsible for defining recovery steps required
  - Responsible for coordinating ICT recovery operations
  - Reporting Director of Corporate & Community Services every 2 hours

- **IT Team members:**
  - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
  - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery:

Depending on the responses above apply one of these options, which are listed in preference order.

Recovery can be achieved within 4 hours on the existing host:

- Continue with hardware restoration.

Failed host impacted storage systems, or recovery will take longer than 3 hours to achieve:

- Is there capacity on the local Datto to recover critical guests?
    - Yes, restore guest to local device (Section: 5.4 Datto Local Restoration)
    - No, restore to Datto Cloud via targeted recovery (Section: 5.3 Datto Cloud Restoration)
- Post physical server restoration, replicate guest VM's back to physical host.

Appendix D – DR Checklist – Prolonged power loss at main council building

Scenario: Incident involving the loss of power to the council building for a prolonged period.

E.g. Power outage of a few days, either through failure or maintenance work.

Potential Impacts:

- All servers would be offline, impacting business transactions from processing.

Assessment:

Yes	No	Item Assessment
		Is the power outage expected to last longer than
		Is there a generator option? Either for building or critical services.

Nominated IT Recovery location: ______________________________

Nominated Crisis Recovery location:

IT Recovery Team:

Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
  - Responsible for defining recovery steps required
  - Responsible for coordinating ICT recovery operations
  - Reporting Director of Corporate & Community Services every 2 hours

- **IT Team members:**
  - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
  - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery:

Depending on the responses above apply one of these options, which are listed in preference order.

- Option 1: Restore power via generator.
  No current provision exists for this option, however, Council's engineering and electrical staff may be able to provide a solution.

- Option 2: Physically relocate Infrastructure from the computer to another location.
  Investigation would be required to identify suitable locations.

  Estimate 8 hours to complete and troubleshoot once a location suitable is identified.

- Option 3: Recover services to Datto Cloud.
  Recovery achievable within 1 day, however steps must to taken to ensure onsite services don’t come back online to cause conflicts and potential data loss.
  - Disconnect power leads to all cabinets with the Council computer room.
  - Initiate Datto disaster recovery (Section 5.3 Datto Cloud Restoration)
  - Initiate site to site VPN (5.3.3 Site to Site VPN)

    Warning: Once power is restored servers will need to be replicated back to site in a controlled fashion to avoid conflicts or data loss.

Appendix E – DR Checklist – Pandemic Outbreak

Scenario: Pandemic outbreak requires employees to work from home or alternate locations.

Potential Impacts:

- Most employees don’t have company laptops to connect to systems at Council.
- Inability to continue processing transactions effectively.

Assessment:

Yes	No	Item Assessment
		Staff member has a company laptop
		Staff member has access to a personal computer
		Staff member has no computer or internet access

Nominated IT Recovery location: ______________________________

Nominated Crisis Recovery location:

IT Recovery Team:
Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
    - Responsible for defining recovery steps required
    - Responsible for coordinating ICT recovery operations
    - Reporting Director of Corporate & Community Services every 2 hours

- **IT Team members:**
    - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
    - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery:
Depending on the responses above apply one of these options, which are listed in preference order.

Staff member has a company laptop:

- Provide OpenVPN access

Staff member has access to a personal computer:

- Provide RDPlus access to control workstations within the office

Staff member has no computer or internet access:

- Source computer suitable of running RDPlus
- Arrange internet access, either 4G modem or mobile hot-spot.

Appendix F – DR Checklist – Loss of inter-site wireless links

Scenario: An event causes the loss of the links that join all sites together.
(E.g. Sever storm breaks the mast on wireless tower)

Potential Impacts:

- Site(s) will become isolated from the network, unable to access resources in the other Council Offices.

Assessment:

Yes	No	Item Assessment
		Is the Darlington Point to Coleambally link working?
		Is the Coleambally to Jerilderie link working?

Nominated IT Recovery location: ____________________

Nominated Crisis Recovery location: IT ____________________

Recovery Team:
Typically the IT Recovery team would be assigned by Livio Mazzon or the Veritech Jobs Controller following escalation of the event to Veritech.

- **IT Recovery Coordinator:**
  - Responsible for defining recovery steps required
  - Responsible for coordinating ICT recovery operations
  - Reporting Director of Corporate & Community Services every 2 hours

- **IT Team members:**
  - Responsible for completing recovery activities as directed by the IT Recovery Coordinator.
  - Reporting to the IT Recovery Coordinator every 30 minutes.

Recovery
Depending on the details of the event, rectifying the issue could take days to weeks based on equipment deliveries. Therefore, the work around to be implemented will be to restore enable site to site VPN to connect Darlington Point and Jerilderie.

The Endian Firewalls in both sites are pre-configured and just need the services enabled.

Full instructions with screen-shots are available in Veritech’s documentation:
http://wiki.vcorp.local/Clients/MurrumbidgeeCouncil/MurFailoverVPN