8.1 DISASTER RECOVERY PLAN UPDATE

Contact Person: Dale Welsh

Why is this matter confidential?

Subject to an order pursuant to Section 90 (3) (e) of the Local Government Act 1999, this matter is confidential because the Disaster Recovery Plan contains detailed information relevant to security of Council's ICT environment..

A. COMMITTEE TO MOVE MOTION TO GO INTO CONFIDENCE

No action – this motion passed in the open section.

B. THE BUSINESS MATTER

8.1 DISASTER RECOVERY PLAN UPDATE

Responsible Executive Manager : Dale Welsh

Report Author : Elena Casciano

Delegated Authority : Matters for Information

Attachments : 1⇩. City of Playford - Disaster Recovery Plan - March 2023

Purpose

The purpose of this report is to provide the Corporate Governance Committee ('the Committee') with an update on Councils Disaster Recovery Plan.

STAFF RECOMMENDATION

The Corporate Governance Committee receives the report.

Relevance to Strategic Plan

The disaster recovery plan (DRP) is a documented and systematic approach that Council implements to recover critical systems, data, and infrastructure in the event of a significant disruptive incident or disaster. The primary goal of Councils DRP is to minimise downtime, mitigate the impact of the disaster, and restore normal operations as quickly and efficiently as possible. An effective DRP ensures that Council can meet its strategic objectives.

Relevance to Community Engagement Policy

There is no requirement to undertake public consultation as part of this report.

Background

Council maintains a robust DRP and its role is to assist ICT staff by detailing a set of scenarios and steps that need to be taken to recover Information, Communication and Technology infrastructure to resume normal business operations. The DRP plan addresses:

- Potential risks and threats that could disrupt business operations, such as natural disasters, power outages, cyber-attacks, or equipment failures
- Critical functions, systems, and data required to support key business processes
- Establish regular data backup procedures, including off-site or cloud storage options
- System architecture, backup schedules, retention periods, and data restoration processes to ensure data availability and integrity
- Recovery strategies for each critical system or process including redundant systems, alternative infrastructure, or third-party service providers
- Priority order of recovery and recovery procedures
- Documentation of the entire disaster recovery plan, including all procedures, contact information, and necessary resources
- Clear communication channels to inform staff, stakeholders, customers, and relevant authorities during a disaster.

In July 2022 an internal audit of the City of Playford Business Continuity and Disaster Recovery Plans (DRP) was completed by KPMG. This audit identified several areas where the DRP and testing could be improved.

Current Situation

Following the 2022 internal audit, Council focused on two areas of improvement to address the audit findings:

1. Reviewing the DRP documentation to include a contemporary and complex disaster scenario including cyber security.
2. Testing the disaster recovery capability of the ICT architecture to ensure that they are effective.

In March 2023 the DRP was reviewed and updated (Attachment 1) incorporating the recommendations provided by internal audit. In addition to this, the ICT team have developed a rolling two-year testing schedule to regularly test the DRP to identify weaknesses, validate recovery procedures, and train personnel on their roles and responsibilities. Upon the first test, the ICT team have identified several improvements to the Disaster Recovery capability of its infrastructure and architecture and have included these improvements into the forward work plan. One of the main improvements identified relates to automatic switching from primary to secondary sites. Once implemented, within a 60 second window of the primary site not responding, the secondary site will activate automatically without human intervention and without interruption to any user.

Future Action

The DRP testing cycle will provide the opportunity to continuously evaluate the effectiveness of the DRP and make necessary improvements based on lessons learned from actual incidents, changing business requirements, changing ICT landscape or emerging threats. Each time a learning is had, the DRP will be updated to include relevant information ensuring that it is always up to date.

In addition to this, the ICT team will commence efforts to define recovery time objectives (RTOs - acceptable downtime) and recovery point objectives (RPOs - maximum acceptable data loss) to provide more clarity and precision to recovery efforts.