SHIRE OF MUKINBUDIN

15 Maddock Street
PO Box 67
MUKINBUDIN WA 6479
Ph: (08) 9047 2100
Email: admin@mukinbudin.wa.gov.au
Web: www.mukinbudin.wa.gov.au

IN REPLY PLEASE QUOTE FILE: ADM289
Enquiries: Tanika McLennan

24 March 2025

Hon. Hannah Beazley MLA
Department of Local Government, Sport and Cultural Industries
GPO Box 8349
PERTH BUSINESS CENTRE WA 6849

Dear Minister

Report on Significant Matter – IT Governance (2023/24 Final Audit) in accordance with Section 7.12A of the Local Government Act 1995

In accordance with Section 7.12A(4)(a) of the *Local Government Act 1995*, the Shire of Mukinbudin is providing a report on the significant matter raised in its 2023/24 Final Audit regarding IT governance.

Audit Finding – IT Governance
The Auditor General identified that whilst the Shire has an ICT Use Policy, it lacks specific provisions addressing key cybersecurity controls, including password management, logical access control, backup procedures, physical access control, patch management, vulnerability assessment, and IT asset management. Additionally, the Shire does not currently have an IT Strategic Plan to guide long-term ICT priorities.

Actions Taken and Planned
The Shire acknowledges the importance of strengthening its IT governance framework and has committed to the following corrective actions:

1. **Development of a Formal ICT and Cybersecurity Policy**
    - The Shire will work with its external IT provider, Wallis Computer Solutions (WCS), to develop a comprehensive ICT and Cybersecurity Policy that incorporates all critical cybersecurity controls.
    - This policy will be completed and presented to Council for adoption by 30 June 2025.
2. **Implementation of an IT Strategic Plan**
    - The Shire will develop a long term IT Strategic Plan to guide decision-making on ICT infrastructure, cybersecurity, and technology investments.
    - This plan will be integrated with the Shire's broader risk management framework and reviewed periodically.
3. **Staff Training and Ongoing Review**
    - Cybersecurity awareness training will continue to be provided to staff to ensure compliance with the new policies.
    - The Shire will implement regular policy reviews to keep pace with evolving cybersecurity threats and best practices.

Compliance with Section 7.12A(5)
A copy of this report will be published on the Shire's website within 14 days, as required under Section 7.12A(5) of the *Local Government Act 1995*.

The Shire of Mukinbudin is committed to addressing the concerns raised in the audit and ensuring a strong and secure IT governance framework. Should you require any further information, please do not hesitate to contact me.

Yours sincerely

Tanika McLennan
ACTING CHIEF EXECUTIVE OFFICER

NAME OF ENTITY: SHIRE OF MUKINBUDIN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

2. IT Governance

Finding

The current ICT Use Policy lacks comprehensiveness, particularly in addressing crucial aspects of cybersecurity. While the existing policy touches on general ICT use, it falls short in providing specific guidelines for essential components such as password management, logical access control, backup procedures, physical access control, patch management, vulnerability assessment, and IT asset management. To address these gaps, it is recommended to either enhance the existing ICT Use Policy to include these critical elements or develop a separate, dedicated Cybersecurity Policy that encompasses all these aspects. Simultaneously, there is an absence of an IT Strategic Plan to guide the Shire's overall direction and priorities in the realm of information technology.

The issue relating to a lack of cyber security policy and plan was first reported in the 2022 management letter.

Risk: Significant *(2023: Significant)*

Implication

The inadequacy of the current policy exposes the Shire to increased risks of cybersecurity threats and vulnerabilities. Without specific guidelines and procedures in place for password management, access controls, data backup, and vulnerability assessments, the Shire may face challenges in safeguarding sensitive information, maintaining data integrity, and ensuring the overall security of its ICT infrastructure. This could lead to potential data breaches, unauthorised access, and disruptions in business operations.

Recommendation

Revise the existing ICT Use Policy by incorporating detailed sections covering password policies, logical access controls, backup procedures, physical access controls, patch management, vulnerability assessments, and IT asset management, or alternatively, develop a standalone Cybersecurity Policy that encompasses these elements.

Simultaneously, the Shire should establish a formal IT Strategic Plan that outlines the vision, goals, and priorities for information technology. This strategic plan should be integrated with cybersecurity considerations, ensuring a holistic approach to IT management. Regular reviews and updates of both policies and the IT Strategic Plan are essential to adapt to evolving cybersecurity threats and technological advancements. Training programs for employees should also be conducted to ensure awareness and compliance with the established policies and strategic objectives. This integrated approach will contribute to a resilient cybersecurity framework aligned with the Shire's broader strategic goals.

Management comment

The Shire outsources its IT management to a third party, currently Wallis Computer Solutions (WCS). WCS does have internal controls for all items mentioned above, however these are not documented in a Council policy. Management will work with WCS to develop a Council Policy.

Responsible person:	Renee Jenkin, Manager Corporate & Community Services
Completion date:	30/06/25