
Policy: Cyber Security

Responsible Officer: Group Manager Organisational Services (Helen McNeil)

Recommendation

That Council:

1. Revoke the policy titled 'Cyber Security' dated 20 October 2021 attached to this report (**Attachment 1**); and
2. Adopt the revised policy of the same name attached to this report (**Attachment 2**).

Background

Council's 'Cyber Security' policy was adopted on 20 October 2021 and is due for review as part of Council's regular policy review program.

This policy was informed by the [NSW Cyber Security Policy](#), which is mandatory for all NSW State Government agencies to adopt, and is designed to:

- (a) provide a set of security controls to regulate the use, passage, and storage of cyber within Council in addition to applicable legislative requirements,
- (b) help protect Council and to minimise the risk that might result from inappropriate use of Council cyber,
- (c) establish a consistent policy position for cyber security,
- (d) have a current cyber incident response plan that integrates with the Council incident management process,
- a) support the development of a cyber security strategy, architecture, and risk management process and incorporate these into the agency's current risk framework and processes.

The review found that if re-adopted, with the minor administrative improvements outlined below, this policy will continue to support Council to identify and respond to cyber incidents.

Review outcome

Through the review process no changes to the NSW Government Cyber Security Policy were identified, and the requirements in that policy continue to be recommended as a foundation of good practice for local government. The review also made reference to the ['Cyber Security Guidelines – Local Government'](#) (2022) published by Cyber Security NSW.

A minor amendment to the review frequency of Council's current policy has been made to achieve administrative efficiencies by aligning the review frequency of the policy with most of Council's policies, being a four (4) yearly cycle rather than an annual cycle. The amendment to the review frequency of this policy was also identified in the internal audit on records management completed in 2024.¹

Other minor amendments include the addition of cross-references to additional procedures developed to support enhanced information access and security processes at Council.

All amendments to the revised policy at [Attachment 2](#) to this report have been made as a 'tracked change' for ease of reference.

¹ Recommendation no. 8 'Internal Audit Report – Records Management' (InConsult, 2024)

Governance

- **Finance**

Not applicable.

- **Legal**

It is not mandatory for Council to adopt the provisions of the NSW Government's Cyber Security Policy. However, adapting and adopting these provisions within Council's own policy is consistent with recommendations put forward by the Audit Office of NSW.

Consultation

The revised policy has been updated in consultation with the ICT Manager.

Conclusion

The Cyber Security policy has been reviewed and remains current subject to a minor amendment to its review frequency. It is therefore recommended to Council for re-adoption with a review frequency of four (4) years.

Attachments

1. Cyber Security policy dated 20 October 2021 (for **revocation**)
2. Cyber Security policy (**for adoption**)