CYBER SECURITY POLICY
NO.: CPOL/CORP219

Responsible Officer: Information Technology Manager

Adopted:	May 2007	**Reviewed:**	July 2026
Next Review:	July 2030	**Type:**	Council Policy

1. PURPOSE

Management of cyber security risk requires a concerted effort across all of Council and cannot be considered just an aspect of information technology. This Policy establishes Council's cyber security risk management approach and is based on the principle that '*Cyber security is everyone's business!'.*

Cyber security enables confidentiality, integrity and availability of information by providing protection against malicious and accidental threats. Cyber security threats take advantage of weaknesses in technology, people and processes to harm information. Council manages cyber security risk to safeguard its mission and protect the interests of the people whose personal information it holds.

2. SCOPE

This Policy applies to all Users of Council ICT Resources and any person who has access to Council information.

Users using Council ICT Resources must comply with this Policy, irrespective of location or device ownership (e.g. personally owned devices). Exceptions to this Policy must be approved by the Director Corporate Services, Chair of IMAC.

3. DEFINITIONS

Term	Definition
Act	Local Government Act 2020 (Vic)
CEO	Chief Executive Officer
Council or SHRCC	Swan Hill Rural City Council
ICT Resources	Covers all ICT facilities including all computers, mobile devices including smart phones, resources located in meeting and conference rooms throughout Council, together with use of the Network and all associated items such as internet access, email, hardware, remote access, data storage, computer accounts, software (both proprietary and those developed by the Council), telephony services, and voicemail.
IMAC	Information Management Advisory Committee, a Council internal committee set up to oversee and control the end-to-end information management tools and processes.
Policy	This Cyber Security Policy
Procedure	The associated Cyber Security Procedure
User	Any person who has been duly authorised to access any ICT Resource including but not limited to:

Term	Definition
	• Employees, • Councillors, • Contractors, • Guests/visitors of the Council, and • Companies or other organisations

Terms defined in the above table will appear with a Capital first letter when used in the body of the document.

4. POLICY

4.1. Principles

a) Council's Information Security Management Systems (ISMS) supports its Cyber Security Strategy, which seeks to mitigate risk and protect Council's critical information against increasingly aggressive and sophisticated cyber threats whilst continually adapting to Council's evolving needs.
b) The key components of the Cyber Security Framework Plans shall be information management, cyber security risk management and cyber security incident management.
c) Information management is critical to robust cyber security. Underpinning the cyber security framework, Council's Information Management Framework shall facilitate identification, management and governance of information assets. It mandates the security classification of information assets which provides the basis for consistent, risk-based protection.
d) Cyber security controls will seek to reduce cyber security risk by either reducing the likelihood and/or impact of an incident.
e) Cyber security incidents shall be managed as per the Cyber Security Incident Management Procedure.

4.2. Roles and Responsibilities

The roles and responsibilities of implementing cyber security and responding to any cyber security incidents shall be as specified in the Procedure, Cyber Security Incident Response Procedure and the Cyber Security Exceptions Procedure.

4.3. Monitoring, Review and Assurance

This Policy shall be reviewed once per year to ensure it aligns with Council's Cyber Security Strategy, legislative or regulatory changes and industry best practice.

This Policy along with other related documents shall also be reviewed as part of the post incident audit and debrief after any significant cyber security incident.

The internal audit process shall provide independent oversight, review and assurance on the effectiveness of cyber security controls to manage risk and meet compliance requirements.

4.4. Recording and Reporting

Council shall ensure that all metric related to cyber security is recorded and reported as per the Procedure.

Council shall also ensure that any cyber security incidents are reported as required by legislation and regulations.

5. RELEVANT POLICIES, PROCEDURES AND DOCUMENTS

Records Management Policy
Cyber Security Procedure
Cyber Security Incident Response Procedure
Cyber Security Framework Plan
Risk Management Procedure
Cyber Security Exceptions Procedure.
State Emergency Management Plan - Cyber Security Sub-Plan, Dec 2025
Victorian Protective Data Security Standards (VPDSS) Version 2.0
Australian Signals Directorate (ASD) Essential Eight Maturity Model

6. APPLICABLE LEGISLATION

Emergency Management Act 2013
Local Government Act 2020
Privacy and Data Protection Act 2014

7. DOCUMENT HISTORY

Ver. No.	Issue Date	Description of Change
1.0	May 2007	Initial Release
1.1	September 2012	Review
1.2	February 2014	Review
1.3	September 2021	Review
1.4	August 2024	Review and Alignment to Essential 8
2.0	July 2026	Major Review including change of title.

Signed:	DocuSigned by: Stuart King FB7439FE09B2493...	**MAYOR**	**Date:**	**18 August 2026**