GREATER SHEPPARTON CITY COUNCIL

CYBER SECURITY POLICY

Effective: Day Month Year

CYBER SECURITY OPERATIONAL POLICY

Version:	1
Business Unit:	Technology & Digital Transformation
Responsible Officer:	Manager Technology & Digital Transformation
Adopted By:	Day Month Year
Next Review:	Day Month Year

1. PURPOSE

The purpose of this Cyber Security Policy is to establish a consistent, risk-based framework for protecting the confidentiality, integrity, and availability of Council information, information systems, and technology assets.

This policy establishes the minimum cyber security governance and control requirements to manage cyber risk across Council operations, ICT systems, cloud services, third parties and information assets to reduce the likelihood and impact of cyber security incidents, safeguard public sector information, and support the secure and resilient delivery of Council services.

The policy aligns with the Victorian Protective Data Security Standards (VPDSS) and applicable whole-of-government cyber security guidance, and mandates the implementation and ongoing maintenance of the Australian Cyber Security Centre (ACSC) Essential Eight mitigation strategies at a minimum of Maturity Level Two (ML2), using a risk-based approach with formally approved exceptions where required.

2. OBJECTIVE

The objectives of this policy are to:

- Meet legislative and regulatory obligations
  Ensure Council meets its obligations under the Privacy and Data Protection Act 2014 (Vic) and complies with the Victorian Protective Data Security Framework and Standards (VPDSF and VPDSS) for information security governance, risk management, and control implementation.

- Establish clear cyber security governance and accountability
  Define responsibilities for cyber security risk ownership, management, and oversight across Council, including executive, operational, and user responsibilities.

- Protect information and systems from cyber threats
  Reduce the likelihood and impact of cyber incidents such as unauthorised access, data breaches, ransomware, and service disruption through the implementation of preventive, detective, and corrective controls.

- Align with recognised cyber security frameworks
  Mandate the implementation and ongoing maintenance of the Australian Cyber Security Centre (ACSC) Essential Eight mitigation strategies at a minimum of Maturity Level Two, using a risk-based approach and formally approved exceptions where required.

- Manage third-party cyber security risk
  Ensure that suppliers, service providers, and external parties do not introduce unmanaged cyber security risks to Council systems or data through structured assessment, contractual controls, and ongoing monitoring, consistent with VPDSS requirements for external party oversight.

- Support continuous improvement and assurance
  Provide a foundation for ongoing monitoring, assessment, and improvement of Council's cyber security maturity, including internal reviews, audits, and reporting to executive management.

3. SCOPE

This Cyber Security Policy applies to all activities, people, and technologies that could affect the cyber security posture of Council systems and environments.

The policy applies to:

- All Council personnel, including:
  - Employees
  - Contractors, consultants, and temporary staff
  - Councillors and committee members

- All third parties and service providers that:
  - Access Council networks or systems
  - Manage, host, support, or monitor Council technology
  - Provide cloud, SaaS, managed, or outsourced ICT services

- All cyber-relevant technology assets, including:
  - Servers, virtual machines, and operating systems
  - End-user devices such as workstations, laptops, mobile and remote devices
  - Network infrastructure, firewalls, and security appliances
  - Applications, databases, and middleware
  - Endpoint protection, logging, monitoring, and detection platforms
  - Backup, recovery, and disaster recovery systems

- All technology environments, regardless of location or hosting model:
  - On-premises infrastructure and data centres
  - Remote and hybrid working environments
  - Cloud-hosted and third-party managed platforms

This policy governs controls and practices intended to prevent, detect, respond to, and recover from cyber security threats, including unauthorised access, malware, ransomware, denial-of-service attacks, data exfiltration, and compromise of accounts or systems.

While this policy supports the protection of information, its primary focus is on cyber security risk management, system resilience, and technological safeguards, in alignment with the Victorian Protective Data Security Standards (VPDSS) and the ACSC Essential Eight at Maturity Level Two.

4. DEFINITIONS

Reference term	Definition
Cloud Service	A computing service delivered over the internet, including Software as a service (SaaS), Platform as a service (PaaS) or Infrastructure as a service (IaaS)
Compensating control	An alternative control implemented where a standard control cannot be met, providing equivalent risk reduction
Cyber security incident	An event that threatens the confidentiality, integrity or availability of Council information systems or data
Endpoint	Any device that connects to Council systems or network, including desktops, laptops and mobile devices
Immutable backup	Backup data that cannot be altered or deleted for a defined retention period
Information asset	Data, systems, applications or infrastructure that store, process or transmit Council information
Least Privilege	Granting only the minimum level of access required for an individual or system to perform authorised tasks
Logging	The recording of system, security and user activities for monitoring, investigation and audit purposes
Multi-Factor Authentication (MFA)	An authentication method requiring two or more independent factors to verify identity
Privileged account	An account with elevated permissions capable of modifying system

	configurations, security controls or user access
Risk-based approach	The application of security controls proportionate to assessed risk, considering likelihood and impact
Third party	Any external organisation or individual that accesses Council systems, data or networks
Vendor security assessment	A formal evaluation of a supplier's cyber security controls relative to Council risk requirements

5. CYBER SECURITY GOVERNANCE

5.1 Accountability

a. The Chief Executive Officer retains overall accountability for cyber security risk.
b. The Manager Technology & Digital Transformation (TDT) is responsible for the implementation and oversight of cyber security controls.
c. Directors, Managers and Team Leaders are responsible for cyber risk within their business systems and processes.
d. All users are responsible for complying with Council's cyber security requirements.

5.2 Risk Management

Cyber risks must be:

a. Identified, assessed and treated in accordance with Council's risk management framework
b. Considered as part of TDT projects, system changes, procurement and vendor onboarding
c. Reviewed following incidents, audits, control failures or significant environmental change

6. INFORMATION SECURITY PRINCIPALS

6.1 Least Privilege Access

a. People, systems and services are only given the minimum level of access required to perform their approved tasks. Access must be role-based, authorised, and regularly reviewed to ensure it remains appropriate. Elevated or privileged access must be restricted, time-bound where possible, and promptly removed when no longer required. This principle reduces the likelihood and impact of unauthorised access, misuse, or compromise of systems and information.

6.2 Defense in Depth

a. Security controls are implemented in multiple, overlapping layers so that the failure of a single control does not result in a security breach. Council applies technical, administrative, and procedural controls across networks, systems, applications, identities and data. These layers work together to prevent, detect, and respond to cyber threats, increasing resilience against both deliberate attacks and accidental failures.

6.3 Security by Design

a. Cyber security is considered from the initial design and planning stages of systems, services, and processes, rather than being added after implementation. Security requirements must be integrated into system procurement, development, configuration and change processes. This ensures risks are identified early, controls are proportionate to risk, and security gaps are not introduced through poor design or late remediation.

6.4 Shared responsibility for cyber security

a. Cyber security is the responsibility of all Councillors, employees, contractors and third parties, not solely the ICT function. While the Technology & Digital Transformation function provides secure systems and oversight, individuals are responsible for using

systems appropriately, protecting credentials, handling information securely, and reporting suspicious activity. Effective cyber security relies on consistent and informed behaviour across the organisation.

6.5 Risk based decision making

a. Security controls are applied based on the level of risk, rather than treating all systems and information equally. Council prioritises controls according to the sensitivity of information, the criticality of systems, and the potential impact of a compromise. Resources and effort are focused where they reduce the greatest risk, supporting informed, proportionate and sustainable cyber security decisions.

7. ESSENTIAL EIGHT – MATURITY LEVEL 2 CONTROLS

Council will implement and maintain the following controls at a minimum. Any exceptions need to be assessed for risk, have compensating controls in place and be reviewed regularly.

7.1 Application Control

a. Council-approved applications only
b. Blocking of unapproved executables, scripts and installers
c. Controlled installation via managed deployment platforms

7.2 Patch Applications

a. Security patches applied within vendor-recommended timeframes
b. Internet-facing applications prioritized
c. Patch status monitored and reported

7.3 Configure Microsoft Office Macro Settings

a. Macros disabled by default
b. Internet-sourced macros blocked
c. Trusted locations controlled

7.4 User Application Hardening

a. Block untrusted content
b. Secure browser configuration enforced via policy

7.5 Restrict Administrative Privileges

a. Administrative access limited to approved roles
b. Separate privileged and standard user accounts
c. Privileged activity logged and monitored
d. Privileged accounts reviewed 6 monthly

7.6 Patch Operating Systems

a. Operating System security patches applied within defined service level agreements
b. Unsupported operating systems are not permitted

7.7 Multi-Factor Authentication (MFA)

MFA enforced for:

a. Remote Access
b. Privileged accounts
c. Cloud and SaaS services
d. Email and identity platforms

7.8 Regular Backups

a. Backups performed daily
b. Offline, offsite or immutable backups maintained
c. Backup restoration tested regularly
d. Backup and Recovery arrangements must meet documented business defined RTO and RPO requirements.

8. IDENTITY AND ACCESS MANAGEMENT

a. Access must be role-based and aligned to the user's position or approved duties
b. All access must be formally approved prior to provisioning
c. Shared accounts are prohibited unless explicitly approved

d. Accounts must be disabled promptly when access is no longer required

9. NETWORK SECURITY

a. Perimeter and internal network protection must be maintained
b. Firewall rules must be documented, approved by Team Leader Infrastructure & Cyber Security and reviewed periodically
c. Logging and monitoring must be enabled across critical systems
d. Security devices must be patched and managed centrally where practicable
e. Network segmentation must be implemented where feasible
f. No unauthorised devices are to be connected to the network

10. INFRASTRUCTURE AND PHYSICAL SECURITY

a. Servers must be hosted in approved facilities
b. Physical access must be restricted via access controls
c. Hosting location (on-premises, cloud, region) must be documented
d. Critical infrastructure must use redundant power supplies and utility power supply systems.
e. Data cabling must be physically secured and clearly labelled

11. SERVERS AND OPERATING SYSTEMS

a. Servers must use secure baseline configurations
b. Unnecessary services and ports must be disabled
c. Security patches must be applied within defined timeframes
d. Admin access must be role-based and restricted to authorised personnel

12. SOFTWARE AND APPLICATIONS

a. Software inventories must be maintained
b. Application control must be implemented

13. NAMING CONVENTIONS

a. IP address allocation and naming must follow documented standards
b. File and folder structure must follow defined conventions and have least privilege access controls

14. WEB FILTERING

a. Web filtering must block:
    - Known malicious sites
    - High risk categories
b. Exceptions must be justified and approved by Team Leader Infrastructure & Cyber Security

15. PASSWORD AND AUTHENTICATION POLICIES

a. Strong password requirements must be enforced
b. Password reuse must be restricted
c. MFA must be enabled wherever technically feasible

16. LOGGING AND MONITORING

a. Security events must be logged and retained
b. Logs must be reviewed for suspicious activity
c. Centralised logging systems should be used wherever possible

17. VULNERABILITY MANAGEMENT

a. Routine vulnerability scanning must be performed
b. Critical vulnerabilities must be risk assessed and remediated
c. Exceptions must be documented and approved
d. Results must be reported to Manager TDT

18. DOCUMENTATION

a. All systems must have documented:
    - Architecture
    - Configurations

- Procedures
- Ownership

b. Documentation must be reviewed and updated regularly
c. All assets must be documented and audited regularly

19. PURCHASING AND PROCUREMENT

a. All purchasing of software and hardware related to information technology must go through the TDT team utilizing the Technology Review Framework
b. Cyber security review for new systems is mandatory

20. CLOUD, SAAS AND HOSTED SERVICES

a. All cloud and SaaS systems must be approved by Manager TDT
b. Where possible, Single Sign On (SSO) or MFA must be enabled
c. Vendor security posture must be assessed
d. Non-network accounts must be disabled promptly when access is no longer required
e. Contracts must include:
    - Incident notification obligations
    - Data location and ownership
    - Exit and data return requirements
    - Security responsibilities
f. Where a system is mandated by an external authority, all required security and risk assessments must still be completed. Any residual risks must be documented and formally accepted through Council's governance processes.

21. THIRD PARTY ACCESS TO NETWORK AND SYSTEMS

a. Third party access accounts are only made available on request
b. Cyber security risk assessments are mandatory prior to onboarding
c. All third party access must be approved by an authorised internal owner (system owner, manager or TDT representative)
d. All third party access must be centrally logged

e. Third party accounts are time limited
f. Access is granted using the principle of least privilege
g. Password must not be shared via bitwarden and tied to third parties email address
h. Third party accounts much be disabled immediately once access is no longer required
i. Third party accounts are reviewed regularly to ensure no unused accounts remain enabled

22. ARTIFICIAL INTELLIGENCE AND AUTOMATION TECHNOLGIES

a. AI Services must be approved by the TDT team
b. AI tools must meet security, privacy and data protection requirements
c. Sensitive or protected information must not be entered into unapproved AI systems
d. AI systems must integrate with identity, access control and logging where possible

23. ENDPOINT AND DEVICE SECURITY

a. All council devices must be centrally managed and use a standard System Operating Environment (SOE)
b. Enforce security baselines
c. Endpoint protection must be installed and monitored
d. Mobile devices must comply with MDM requirements
e. Firewalls must be enabled

24. CHANGE MANAGEMENT

All system and application changes must:

a. Be formally assessed
b. Be approved prior to implementation
c. Follow documented change procedures

25. INCIDENT MANAGEMENT

a. All suspected cyber incidents must be reported immediately to the Manager TDT
b. Incidents are managed in accordance with Council's Incident Response Plan
c. Incidents must be recorded, classified and reviewed
d. Mandatory reporting obligations under VPDSS will be met

26. AWARENESS AND TRAINING

a. Cyber security awareness training is mandatory
b. Staff must understand their cyber security responsibilities

27. BREACH OF OPERATIONAL POLICY

Any breach to this Operational Policy will be addressed in accordance with Council's Managing Workplace Performance and Behaviours Policy

28. RELATED DOCUMENTS

- Incident Response Plan
- ICT Systems Standards and Conventions

29. RELATED POLICIES

- Information Security Management Framework Operational Policy (M24/16509)
- Acceptable Use Operational Policy (M25/90271)
- Risk Management Operational Policy (M23/53909)
- Business Continuity Plan Operational Policy (M24/95994)
- Employee Code of Conduct (M21/113784)
- Managing Workplace Performance and Behaviours Policy (M23/44451)

30. RELATED LEGISLATION

- Information Privacy Act 2000 (Vic)
- Privacy and Data Protection Act 2014 (Vic)

- Victorian Protective Data Security Framework (VPDSF)
- Victoria Protective Data Security Standards (CPDSS)
- Essential Eight (Maturity Level 2)

31. REVIEW

This Operational Policy will be formally reviewed every three years by the Manager, Technology & Digital Transformation. However, an earlier review may be initiated if directed by the Executive Leadership Team or in response to significant legislative or regulatory changes.

DOCUMENT REVISIONS

Version #	Date Adopted	Date Effective