POSITION DESCRIPTION

POSITION TITLE:	Senior Cybersecurity Specialist				
POSITION NO:	100734	**CLASSIFICATION:**	Band 8		
DIVISION:	Corporate Services				
BRANCH:	Digital and Technology				
UNIT:	Technology Services				
REPORTS TO:	Senior Cybersecurity Lead				
POLICE CHECK REQUIRED:	Yes	**WORKING WITH CHILDREN CHECK REQUIRED:**	Yes	**PRE-EMPLOYMENT MEDICAL REQUIRED:**	No

Yarra City Council committed to being a child safe organisation and supports flexible and accessible working arrangements for all.

This includes people with a disability, Aboriginal and Torres Strait Islanders, culturally, religiously and linguistically diverse people, young people, older people, women, and people who identify as gay, lesbian, bisexual, transgender, intersex or queer.

We draw pride and strength from our diversity, remain open to new approaches and actively foster an inclusive workplace that celebrates the contribution made by all our people.

POSITION OBJECTIVES

This is an exciting role to collaborate with the entire City of Yarra (CoY) Council D&T teams to maintain a high-level cybersecurity against security threats by designing, implementing, monitoring, and maintaining robust security systems and measures. Also, the role fosters cybersecurity awareness, leads security vulnerability patch deployment, implements mitigation security strategies, and ensure CoY IT systems compliance including overseeing cybersecurity operations such as threat intelligence, incident response and recovery.

ORGANISATIONAL CONTEXT

The Municipality is committed to efficiently and effectively servicing the community to the highest standards, protecting, enhancing, and developing the City's physical and social environment and building the population and business base. A major imperative of the Organisation is the introduction of a best value framework with an emphasis on customer service and continuous improvement.

The D&T Branch contributes directly to the achievement of the organisational goals. As a member of the Corporate Services Division, the incumbent is required to pursue Branch goals through effective teamwork within the Branch and with colleagues in other branches and divisions developing sound working relationships with a range of internal and external parties.

ORGANISATIONAL RELATIONSHIP

Position reports to:	Senior Cybersecurity Lead
Relationships:	Closely liaise with staff in the Digital and Technology Branch and with Technology Services Unit. Supervision of contract staff and suppliers/vendors engaged for project-based activities. Liaise with council's suppliers as necessary to evaluate, install and maintain systems as required; and Liaise with staff at all levels across the organisation on IT security support issues.

KEY RESPONSIBILITY AREAS AND DUTIES

- Oversee the development, implementation, and maintenance of cybersecurity strategy, policies, standards, and procedures with Victorian Government and CoY Council standards.

- Administer cybersecurity operations encompassing threat intelligence, vulnerability management, incident response to mitigate breach impacts.

- Evaluate and implement emerging cybersecurity technologies and best practices, and ensure compliance with relevant laws, regulations, and legislation.

- Evaluate, implement, and track adherence with the ACSC Essential 8, Victorian Protective Data Security Standards (VPDSS) and NIST.

- Conduct comprehensive security risk evaluations and assessments for new and prospective applications, applying objective measures and established frameworks to ensure adherence to security standards.

- Responsible for security configuration upgrades and provision of advice regarding potential improvements to security.

- Responsible for security configuration upgrades and provision of advice regarding potential improvements to security

- Responsible for ensuring the organisation meets security standards, for example the ACSC Essential 8, Victorian Protective Data Security Standards (VPDSS) and NIST CSF.

- Responsible for responding to and fixing security items raised by Yarra City Councils Audit Committee.

- Should advise the Technology Services Lead of relevant security issues or actions above at the earliest practical opportunity.

- Responsible for the supervision and development of cybersecurity staff and contractors.

- Responsible for overseeing and managing external security services providers

- Responsible for leading incident response.

ACCOUNTABILITY AND EXTENT OF AUTHORITY

- Accountable for the cybersecurity performance and outcomes of Yarra City Council, and the management of cybersecurity risks and issues.

- May be required to attend conferences, meetings or similar events relating to the IT industry, to general Council operations or to specific commercial arrangements and to liaise with other bodies or companies as appropriate.

- Must always act within Council and Digital and Technology Services Branch Policies and Procedures.

- Has the freedom to act in the investigation and/or prevention of system security or integrity breaches with reference to Branch management at the earliest opportunity

Safety & Risk

- Minimise risk to self and others and support safe work practices through adherence to legislative requirements and Council policies and procedures.

- Report any matters which may impact on the safety of Council employees, community members, or Council assets and equipment.

- Yarra City Council is committed to prioritising and promoting child safety. We adhere to the Victorian Child Safe Standards as legislated in the Child, Wellbeing and Safety Act 2005 and have robust policies and procedures to meet this commitment.

- Demonstrate leadership in reducing Yarra’s emissions and building a climate resilient future by embedding climate considerations into all of Councils activities.

At Yarra Every Job is a Climate Job
Acting on the climate emergency requires that we change the way we think, make decisions, and prioritise action. We must embed proactive climate responses in the ways we govern, live our lives, and conduct our work. Every choice we make today and into the future will have an impact; this is true for Council and the community.
Acknowledging the scale of this crisis, at Yarra we are committed to ensuring that every job is a climate job meaning that each staff member will play a key role in shaping our climate response.

Yarra Values

- Behave according to the following values which underpin our efforts to build a service-based culture based on positive relationships with colleagues and the community:
    - Accountability
    - Respect
    - Courage

JUDGEMENT AND DECISION MAKING

- Exercise independent professional judgment and adaptability in evaluating and deciding on appropriate methods, procedures, and practices for achieving Branch objectives and in reviewing and recommending improvements to those methods, procedures, and practices.

- Problems are often of a complex nature with solutions not related to previously encountered situations or existing documentation. Some creativity and originality are therefore required.

- Policy development and advocacy skills and experience would be highly desirable.

- The incumbent is expected to work autonomously with limited guidance within the organisation.

- Exercise sound judgement and decision making on complex and sensitive cybersecurity matters, based on the analysis of information, data, and evidence, and the consideration of risks, impacts, and alternatives.

- Apply critical thinking and problem-solving skills to identify and resolve cybersecurity issues and challenges, and to develop and implement effective and efficient cybersecurity solutions.

- Consult and collaborate with relevant stakeholders and subject matter experts, and seek approval from senior management when required, to ensure the quality and consistency of cybersecurity decisions and outcomes.

- Educate and train other staff members on IT security awareness and procedures.

SPECIALIST KNOWLEDGE AND SKILLS

- Broader Information Technology background

- Proficient in cloud security best practice and implementation.

- Proficient in assessing and implementing best practices for SaaS and application security.

- In-depth knowledge of information security principles, practices, frameworks, standards, regulations, such as ACSC Essential 8, NIST CSF, NIST 800-207, VPDSS.

- Familiar with various security tools and techniques such as SIEM, IDS/IPS, log analysis, forensics, etc; Familiar with various security threats such as malware, ransomware, phishing, DDoS, SQL injection, XSS.

- Experience in using Microsoft 365 Defender for Endpoint to manage vulnerabilities, weaknesses, and recommendations; Knowledge of Microsoft 365 Defender and Azure Sentinel integration to enable seamless threat detection and response across endpoints and cloud.

- Proficient in developing internal IT policies, procedures.

- Familiar with IT service management frameworks and methodologies, such as ITIL, COBIT, and Agile.

- Having experience in a Victorian council working environment is a significant advantage. This familiarity not only demonstrates an understanding of local governance and community needs but also showcases the ability to navigate the specific processes, regulations, and cultural nuances unique to the region. Such experience can enhance collaboration with stakeholders and contribute to more effective decision-making within the council framework.

MANAGEMENT SKILLS

- Excellent leadership and management skills, with the ability to motivate, inspire, and empower cybersecurity staff and contractors, and to foster a positive and collaborative team culture.

- Strong project management and organisational skills, with the ability to plan, coordinate, and deliver multiple cybersecurity projects and initiatives within the scope, time, budget, and quality expectations.

- Effective stakeholder management and communication skills, with the ability to build and maintain strong relationships with internal and external stakeholders, and to communicate cybersecurity information and issues clearly and persuasively.

INTERPERSONAL SKILLS

- High level of interpersonal and communication skills, with the ability to communicate effectively and respectfully with people from diverse backgrounds, cultures, and perspectives, and to adapt to different communication styles and situations.

- High level of emotional intelligence and resilience, with the ability to manage stress, emotions, and conflicts, and to cope with ambiguity and change.

- High level of professionalism and ethics, with the ability to act with honesty, integrity, and accountability, and to uphold the values and reputation of Yarra City Council.

- Collaborate effectively with various teams within Yarra City Council, fostering teamwork and shared objectives. Possess strong interpersonal skills to persuasively engage with clients, community members, and colleagues, utilizing negotiation and consensus-building to achieve positive outcomes. This ability enhances the Council's commitment to delivering efficient, customer-focused services and strengthens relationships with stakeholders.

QUALIFICATIONS AND EXPERIENCE

- Degree or Diploma in Cybersecurity, Information Technology, Computer Science, or a related field plus post graduate qualifications. Or lesser formal qualifications with extensive and Diverse experience working with security tools such as Firewalls, IPS/IDS, SIEM, MS Defender alongside experience with cloud platforms like Azure.
- At least 5 years of experience in cybersecurity role is desirable.
- Certification in information security such as CISSP, CISM, GIAC, CEH, SANS, OSCP is highly desirable.
- Certification in Microsoft security such as SC-200/300/400/900 is highly desirable.
- Cybersecurity Prowess: Security standards (e.g., VPDSS, ACSC Essential 8, NIST, ISO27001), and have experience with security encryption protocols, in solving security threats, incidents, and vulnerabilities through proactive solutions.

KEY SELECTION CRITERIA

- Demonstrated ability to oversee the cybersecurity function of a large and complex organisation, ensuring the protection of information assets and systems from cyber threats and risks, and compliance with relevant standards and regulations.

- Demonstrated ability to apply data security best practices to protect the confidentiality, integrity, and availability of the organisation’s data assets and systems, and to comply with relevant data protection laws and regulations.

- Demonstrated ability to oversee the cybersecurity operations, including threat intelligence, vulnerability management, incident response, forensics, and recovery.

- Demonstrated extensive knowledge and experience in cybersecurity principles, practices, and standards, such as NIST CSF, NIST 800-207, ACSC Essential 8, and VPDSS.

- Demonstrated proficiency in cybersecurity technologies and tools, such as firewalls, antivirus, encryption, SIEM, IDS/IPS, and VPN.