

# Position Description

## Senior Cybersecurity Specialist



### Position Details

<b>Position Title</b>	<b>Senior Cybersecurity Specialist</b>
<b>Position Number</b>	100734
<b>Classification</b>	Band 8
<b>Division</b>	Corporate Services
<b>Branch</b>	Digital and Technology Services
<b>Unit</b>	Technology Services
<b>Reports To</b>	Senior Cybersecurity Lead
<b>Employment Essentials</b>	<ul style="list-style-type: none"><li>• WORKING WITH CHILDREN CHECK</li><li>• POLICE CHECK</li></ul>

Yarra City Council is 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 Islander peoples, 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.

### 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.

### 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

# Position Description

## Senior Cybersecurity Specialist



within the Branch and with colleagues in other branches and divisions developing sound working relationships with a range of internal and external parties

<b>Position reports to:</b>	Senior Cybersecurity Lead
<b>Reporting to this Position:</b>	N/A
<b>Internal Relationships:</b>	Closely liaise with staff in the Digital and Technology Branch and with Technology Services Unit. and Liaise with staff at all levels across the organisation on IT security support issues.
<b>External Relationships:</b>	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

### Position Overview

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.

### Key Responsibilities

#### All Yarra employees:

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

- 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. 2 September 2024 Senior Cybersecurity Specialist
- 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

# Position Description

## Senior Cybersecurity Specialist



- Responsible for leading incident response.

### Accountability and Extent of Authority

- **Resource management:** freedom to act set by broad goals, policies and budgets; may have a substantial effect on the unit or public perception of the organisation,
- **Manage specialist or regulatory units:** freedom to act subject to goals, policies and legislation; may have a substantial effect on the community,
- **Develop policy options and strategic plans:** wide freedom to act; may have a substantial impact on the organisation or community.

### Judgement and Decision Making

- Generally involves both problem solving and policy development.
- Typically requires identification and analysis of an unspecified range of options.
- Employees will identify and develop policy options for management or employer consideration.

### Management Skills

- Typically management of large numbers of employees or tertiary qualified employees.
- Management skills to achieve goals and objectives.

### Interpersonal Skills

- Ability to persuade, convince or negotiate with clients, members of the public, employees, tribunals etc.
- Ability to lead, motivate and develop other employees.

### Risk and Safety Requirements

- 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.

### Specialist Skills and Knowledge

- May be outside original field of specialisation.
- Understanding of legal, socio-economic and political context.
- Sound knowledge of budgeting and accounting/financial procedures (except for specialist positions)
- 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.

# Position Description

## Senior Cybersecurity Specialist



- 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.

### Qualifications and Experience

- Tertiary qualification in Cybersecurity, Information Technology, Computer Science, or a related field plus post graduate qualifications with relevant experience plus post graduate qualifications or qualifications/experience in another field or lesser formal qualifications with extensive and diverse experience, or intensive specialist experience.
- 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
- 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

1. 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.
2. 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.
3. Demonstrated ability to oversee the cybersecurity operations, including threat intelligence, vulnerability management, incident response, forensics, and recovery.
4. Demonstrated extensive knowledge and experience in cybersecurity principles, practices, and standards, such as NIST CSF, NIST 800-207, ACSC Essential 8, and VPDSS.
5. Demonstrated proficiency in cybersecurity technologies and tools, such as firewalls, antivirus, encryption, SIEM, IDS/IPS, and VPN