Job title: Information Security Analyst	
Classification: Band 7	**Effective Date**: September 2024
Reports to: Coordinator Cyber and IT Infrastructure	**Tenure**: Full Time Ongoing

About us:

At Whitehorse City Council, community is at the heart of everything we do.

We aspire to be a healthy, vibrant, prosperous and sustainable community. We enable this through strong leadership and community partnerships.

We strive to stay ahead of evolving changes and needs of our community.

Our five key principles empower our employees to be innovative and to provide an excellent customer experience. We are a resilient organisation where everyone belongs.

Excellent Customer Experience and Service Delivery **Great Organisational Culture** **Innovation and Continuous Improvement** **Good Governance and Integrity** **Long Term Financial Sustainability**

We value:

Our shared values and behaviours are integral to how we go about our work, interact with each other and our community. It is expected that all employees 'live' these shared values. In living these values we also ensure that **e**veryone has a voice and that **e**veryone matters.

Collaboration	Respect	Excellence	Accountability	Trust
We work flexibly together to achieve outcomes and solve problems.	We actively listen, value diversity and care.	We adapt, respond, learn and grow.	We take responsibility and follow through on our promises.	We act with integrity and are empowered to make decisions.

Goal Statement

The position supports and partners with the organisation in the development and enhancement of information and cyber security solutions and council's security posture. As a Security Analyst, you will be a part of an exciting and challenging role with the aim of improving our information and cyber security environment within our multi-site network. With a sound practical knowledge of cyber security and a background in operational technology security, along with an ambitious and positive attitude, you will be able to hit the ground running in this fast-paced role.

Key Responsibilities

Position Specific Responsibilities

- Diagnose and resolve security incidents and problems raised by customers via the service desk.

- Research, evaluate, and provide feedback and recommendations on security related technology trends and patterns in customer support requirements.

- Maintain customer incident and problem tracking and resolution information in council's service desk system.

- Develop and maintain security policies and procedures in alignment with industry security standards.

- Ensure the rigorous implementation of information security/information assurance policies, principles, and practices in the delivery of customer support services.

- Enhance the information security threat and risk framework and assessments.

- Monitor and manage audit items and responses.

- Embed a proactive cyber security mindset and raise awareness of IT security across Council staff.

- Contribute to the implementation of information and cyber security awareness and training.

- Manage and report on information security incidents.

- Strengthen the security posture of the organisation.

- Provide technical support for penetration tests, security access and configuration audits, security exercises and phishing testing.

- Work collaboratively with internal and external partners and technology vendors to monitor, detect and report security vulnerabilities, incidents, threats and trends.

- Perform technical and compliance assessments of information security and cyber security controls.
- Ensure change management frameworks and best practice guidelines are followed.
- Manage the installation and integration of systems fixes, patches, updates and enhancements.
- Manage accounts, network rights and access to systems and equipment.
- Ensure systems availability, functionality, integrity, and efficiency.
- Maintain systems configuration, automate system alerts, monitoring and hardening.
- Maintain ASCS Essential 8 Maturity level controls and measures.
- Respond to security advisories from vendors, government agencies and suppliers.

Corporate Responsibilities

- Adhere to all Corporate Policies, Procedures and the Organisational Goals and Values in the current Whitehorse City Council Collective Agreement.
- Understand and adhere to the Risk Management Policy (as it relates to the employees work area) and related procedures that are designed to minimise injury and/or loss to individuals, assets, and equipment.
- Report any matters that may impact on the safety of Council employees or citizens, assets, and equipment.
- Ensure appropriate care and use of assets and equipment.

Authority

Budget: Nil.

Staff responsibility: Nil

Decision Making:

- This position is required to operate with a high degree of professionalism under direction of IT leadership.
- This position involves solving problems, using procedures and guidelines and the application of technical knowledge or knowledge acquired through relevant experience.
- This position requires making operational decisions under general supervision.

- Problems may be of a complex or technical nature with solutions not related to previously encountered situations and some creativity and originality is required.

Key Relationships

- The incumbent liaises with staff at all levels within the Organisation including, Manager of Organisational Technology, Executive, Managers, Business Support teams and the user base. The position is required to maintain a professional relationship with Government departments and agencies, MAV, other Municipalities, service providers, staff associations, suppliers.

- The position will liaise with all IT support staff, suppliers, and council employees, and have the ability to gain co-operation and assistance from clients, contractors and employees.

Skills and Attributes

Qualifications/Certificates/Licences and Experience

- Relevant tertiary or post graduate qualification in Information Technology, Information Security, Computer Science or similar.

- Extensive demonstrated experience in supporting Microsoft Windows Servers, Security concepts, administration of Microsoft Windows Servers, and exposure to virtualisation technologies.

- Security certifications will be highly regarded.

- Experience in ASCS Essential 8 maturity level, NIST CSF 2.0 and other security frameworks will be highly regarded.

- Experience in measuring performance of systems and making recommendations.

- A valid Victorian driver's licence.

- Satisfactory National Criminal History Check.

Technology

- Excellent knowledge of ICT trends, issues and opportunities, particularly those related to information security standards and their applicability, infrastructure, cloud and applications.

- Must have a detailed and demonstrated understanding of security systems and controls, Microsoft Windows Server Operating Systems, Microsoft Office 365 and Azure, VMWare, and related technologies.

- Other technical skills · Demonstrated ability to produce technical server designs, manage upgrades, maintain patch management processes, create, and manage server images, maintain, and monitor infrastructure lifecycle management.

- Experience and technical knowledge in council's core information security systems (Proofpoint Email Gateway, UpGuard, Zscaller, Defender, Purview DLP, Crowdstrike, Airlock Digital, Citrix ADC Netscaler, Fortclient etc) is desirable.

- Experience and technical knowledge in council's network systems (Aruba Airwave and Clearpass, Fortinet firewall and EMS, 802.1x, Network Policy Server etc) is desirable.

- The ability to provide third level help desk support related to IT security advice.

- Highly developed technical skills to monitor, detect and respond to security vulnerabilities, incidents and threats.

Interpersonal:

- The ability to build and maintain effective relationships including demonstrated experience and skills in liaison, negotiation and problem solving with staff at all levels.

- Demonstrated written and oral communication skills to facilitate the provision of advice and support at all levels of the organisation.

- Ability to manage time, prioritise allocated work tasks and handle multiple tasks simultaneously.

- Ability to operate with patience and empathy when under pressure.

- Ability to support strategies, programs and policies of the IT Department and Council.

- Proactive in keeping leadership informed of issues that may impact service standards.

- High level communication skills, both verbal and written.

- An understanding of the operations and services of a dynamic team, and ability to work in a team environment and positively contributing towards the team outcomes.

Leadership/management:

- The successful applicant must have skills in managing time, setting priorities, planning, and organising their own work so as to achieve specific and set objectives in the most efficient way possible within the resources available and within a set timetable.

- Must be familiar with budgeting techniques to ensure that projects are managed within cost constraints.

- Must provide appropriate scheduling of IT tasks to IT support staff.

- Ability to work as an effective and positive member of a team.

- Other Attributes (Desirable)

- Requires a high degree of technical ability tempered by a superb Customer focus philosophy.

Notes and comments:

- The position includes an inherent physical requirement to complete repetitive office-based activities and also some lifting may be required. Please refer to the Physical and Functional Requirements Checklist for more information. Short listed candidates may be required to attend a pre-employment medical examination.

- A clear National Police check is essential, and a driver's licence is desirable.

- The position may be required to attend out of hours meeting.

- The position may be required to work from different locations within the municipality.

Key Selection Criteria

1. Relevant tertiary or post graduate qualification in Information Technology, Information Security, Computer Science or similar.
2. Excellent knowledge of ICT trends, issues, and opportunities particularly those related to information security standards and their applicability, infrastructure, cloud and applications.
3. Demonstrated written and oral communication skills to facilitate the provision of advice and support at all levels of the organisation, with highly developed technical skills to monitor, detect and respond to security vulnerabilities, incidents and threats.
4. The ability to build and maintain effective relationships including demonstrated experience and skills in liaison, negotiation and problem solving with staff at all levels with the ability to provide IT security advice and provide escalated help desk support.

Physical Requirements

Task	Performed Often	Performed Sometimes	Never/Rarely Performed
Keyboard duties	✓		
Reading tasks	✓		
Writing tasks	✓		
Sitting (extended periods)	✓		
Walking/standing (briefly) - counter		✓	
Walking/standing (extended)		✓	
Driving car/utility/truck		✓	
Lifting/carrying duties (light)	✓		
Lifting/carrying duties (heavy)			✓
Pushing/pulling tasks (light)	✓		
Pushing/pulling tasks (heavy)			✓
Chopping/digging tasks			✓
Bending/kneeling requirements		✓	
Climbing stairs/ladders/scaffolds			✓
Handling grease/oils			✓
Exposure to dust/dirt			✓
Exposure to hazardous materials			✓
Exposure to noise		✓	
Repetitive arm/wrist/hand movements		✓	
Other (please specify)			

Any other relevant comments:

- The position may be required to attend out of hours meeting.
- The position may be required to work from different locations within the municipality.