POSITION DESCRIPTION/SPECIFICATION

1. POSITION IDENTIFICATION

Title	Cyber Security Analyst	**Level**	6/7
Business Unit	Information Technology	**Position Number**	01613
Directorate	Corporate Service	**Date Established**	February 2023
Reporting to	Coordinator IT Infrastructure	**Date Updated**	March 2025

2. KEY OBJECTIVES

- Responsible for monitoring and reporting on the security and integrity of information assets and performance of IT services and infrastructure implemented by the City.
- Develops policies, procedures and frameworks to secure the confidentiality, integrity and availability of information assets.
- Provides security event monitoring, vulnerability management, patching and analysis of security incidents across the City's IT infrastructure.
- Provides development and maintenance of the City's network & cyber security services.
- Provides information security policy, technical and operational advice to key stakeholders.
- Participate in a team environment providing high level technical support in relation to the City's computer network meeting the business needs while ensuring network security, cost effectiveness and reliability.
- Provide support to the ongoing development and maintenance of information systems risk and security controls to protect the information assets of City of Joondalup.

3. KEY ACCOUNTABILITIES

- Undertake activities in accordance with the Business Unit Plan, Corporate Business Plan and Strategic Community Plan.
- Ensure all financial activities are undertaken in accordance with the City's purchasing protocols and practices.
- Customer service is delivered in accordance with the City's Customer Service Charter and relevant protocols and procedures.
- Ensure prompt capture of corporate information and documentation in accordance with the City's record keeping system and associated policies, protocols and practices.
- Comply with Work Health and Safety (WHS) legislation, City protocols, procedures and other WHS related requirements, and actively support the City safety systems.

4. KEY ACTIVITIES

ACTIVITIES

Outcome: Cyber Security Maintenance and Improvement

- Perform and support scheduled vulnerability scans, reviews and compliance testing to ensure the City meets the Essential Eight Maturity Level requirements for patching software and hardware.
- Monitor, support and review authentication and access control, next-gen firewalls, endpoint protection and relevant cloud security solutions.
- Develop and review the City's cyber security related policies, procedures and guidelines.
- Build collaborative relationships with team members, internal stakeholders and external partners.
- Monitor, assess and assist in the continual improvement of the performance of cyber security services and capability.
- Develop and delivery of cyber security awareness training to the City of Joondalup.
- Undertake analysis and reporting of cyber security threat intelligence.
- Identify and implement security processes to protect the City's corporate computer network.
- Administer EDR/XDR software and further develop a multi-layered cyber protection strategy.

Outcome: Effective Network Security Management

- Provide technical support, recommendations and system improvements for the City's:
  - Security Vulnerability Management
  - Patching of software and hardware based on vulnerability assessment report
  - Mobile device management
- Perform periodic network capacity planning and organise the replacement of network equipment which includes providing recommendations and justifications, purchasing of equipment and participation in the installation and implementation of new computer network equipment.
- Develop and contribute to strategies, protocols and processes ensuring the computer network is reliable.
- Monitor the performance of the City's local and wide area networks.
- Maximise network uptime by being proactive and monitoring the City's network and faulty network points.
- Liaise with IT Infrastructure team and Help Desk teams to provide high level support regarding network & cyber security support issues.
- Evaluate the compatibility and effectiveness of hardware and software that may be introduced to the City's network.
- Identify improvements to security infrastructure to increase performance.
- Evaluate and recommend specific network products and technologies.
- Recommend budget requirements for ongoing network improvements.
- Develop and apply IT infrastructure support procedures and methodologies.

Outcome: IT Infrastructure Support

- Assist in investigating, assessing and responding to enquiries, requests and correspondence relating to computer network issues/requests.
- Provide backup support to the Systems & Network Administrators as required for Network switches, routers, firewalls, Windows, Servers, backup systems and database support.
- Provide support on corporate network & security issues.
- Provide training to other employees on basic cyber security skills where necessary.

- Perform other duties as requested within the scope of this level and in accordance with skills, knowledge and experience.

5. WORK RELATED REQUIREMENTS

Essential Skills, Knowledge, Attributes and Qualifications:

Skills

- Well-developed interpersonal, verbal and written communication.
- Organisational, planning and time management.
- Conceptual and analytical ability.
- Proven ability to develop and maintain strong relationships with key stakeholders, ensuring effective communication and understanding of business priorities.
- Willingness to learn and positive can-do attitude.
- Passion to deliver excellent customer service.
- Ability to work independently and/or within a team environment.

Comprehensive Knowledge

- Cyber security management processes including network security, malware prevention, monitoring information technology risks and security vulnerabilities.
- Processes to conduct network security and vulnerability assessment activities including routing, switching, diagnostics, firewalls, scanning, and testing.
- Monitoring security platforms and applications to assist in protecting the organisation against attacks, intrusions and unusual, unauthorised or illegal activity.
- Practical knowledge of cyber security procedures and frameworks, ASD Essential 8, ISM, NIST Cyber Security Framework, ISO 27000-series, MITRE, Entra ID, Microsoft Purview.
- Vulnerability management, threat intelligent platforms, endpoint protection.
- Current and emerging networking technologies, trends and standards.
- Information security controls, IT risks, cyber frameworks risk analysis, policies, security awareness training, network penetration testing and vulnerability assessments.
- Relational database systems, web-based systems, software distribution tools, administering Windows and servers.
- And/or experience in the implementation of cybersecurity frameworks e.g. NIST, ISO2701 (desirable).

Demonstrated Experience

- Exposure to the administration of endpoint security software, firewall administration, internet and email gateways management.
- Cyber security assessment techniques, standards and auditing.
- Development, implementation and/or support of incident management planning and processes.
- Working across Information Security, Cyber Security, IT Support Services.
- Desirable not essential experience in implementing and assessing against Essential Eight.

Qualifications / Clearances:

- Diploma, Advanced Diploma or a Bachelor's Degree in Cyber Security or related discipline.
- Desirable not essential relevant industry certifications for security (e.g., Security+, CC, CISM, CISSP).
- Current National Police Clearance (NPC) no older than 3 months.
- Current WA 'C' Class Drivers' License.

6. EXTENT OF AUTHORITY

- Freedom to act within defined established guidelines.
- Work outcomes are clearly defined and monitored.
- Problems can usually be solved with reference to procedures, documented methods and instructions. Assistance is available when problems occur.
- Scope to exercise initiative in the application of established work procedures.

7. WORKING RELATIONSHIPS

Level of Supervision:

- Works under limited supervision

Internal:

- All other business units

External:

- IT hardware and software vendors
- IT Service Provision Companies
- IT Consultants and Contractors

8. POSITION DIMENSIONS

NUMBER OF EMPLOYEES DIRECTLY REPORTING TO THE POSITION	0