

Position Description



Job Details

Job Title:	Lead Cyber Security and Systems Specialist
Reports to:	ICT Operations and Infrastructure Manager
Group:	City Development
Position Number:	IM0119
Grade:	Grade 8
Date:	October 2024
Objective Doc Ref:	N/A

Position Purpose/Job Summary

The Lead Cyber Security and Systems Specialist is responsible for the design, implementation, administration, and monitoring of ICT security and evaluating Council systems. This position is also responsible for supervising the ICT security audits (internal and external) and for leading the Cyber Security, Risk and Analyst Team.

This role responsible for leading and maintaining the confidentiality, integrity and security of Council's information and systems and contributes to the design, implementation and maintenance of systems and requires a synergy of leadership, administrative and technical expertise, analytical skills, and effective communication.

Responsible for the identification, design, implementation, administration, support and usage of Councils cyber security, risk management and monitoring systems and procedures, with key partnerships in business continuity, disaster recovery and incident response.

This role also supervises and engages in cyber security audits (internal and external) to ensure the access, authorisation and accountability of Council systems remains optimal and liaises with various stakeholders for threat intelligence, risk assessment, vulnerability identification and management and cyber control maturity and assurance.

Recognised as a critical role within the Technology, Infrastructure and Security Operations team working closely with the Infrastructure and Operations Manager to plan, develop and operate robust and secure infrastructure and technologies.

Position Description



Selection Criteria - Knowledge, Skills, Qualifications and Experience required

Essential

- Qualifications and/or experience in Information Technology, System Administration, Information Risk and Cyber Security and IT Network Administration and/or equivalent experience and qualifications such as such as CC\CISSP, CEH, CompTIA.
- Demonstrated capacity to provide cyber leadership for project initiatives and operations, and collaborate with the ICT team to assess, prioritise, and plan maintenance and remediation for councils' various business systems and information against and from cyber security threats.
- Ability to interpret and apply relevant legislations and regulations
- Prepare documentation including procedure, technical and presentations with excellent communication, interpersonal, presentation and written communication skills
- Ability to work in a flexible and timely manner as a team player and ability to adapt to fluctuating workloads and changing priorities.
- Demonstrated ability under pressure to investigate issues, analyse threats, conduct a root-cause analysis, and resolve system and cyber security issues and solve incidents, issues, and problems.
- Conduct detailed system and cyber threat analyses, including the evaluation of existing and onboarding systems and the identification of weakness and vulnerabilities.
- Develop and implement strategies to defend and recover against cyber threats and maintain business continuity.
- Coordinate with other IT professionals to improve security.
- Stay current with the latest cybersecurity trends and threat intelligence and participate in the development and testing of new security solutions, including providing recommendations for security enhancements.
- Assist in the development and operating of organisation-wide best practices for IT security.
- Experience with cybersecurity, control, and risk frameworks like NIST, ISO 27001, Essential8 and/or CIS Controls.
- Oversee the deployment of awareness and training and guidance to staff on cybersecurity best practices.
- Monitor the organization's networks for security breaches and investigate violations when they occur
- Install and use software, such as vulnerability assessment tools, audit software, governance software and data encryption programs.

Desirable

- Knowledge of various security methodologies and processes, and technical security solutions (firewall and intrusion detection systems), including TCP/IP, computer networking, routing, and switching
- Familiarity with web-related technologies (Web applications, Web Services, Service Oriented Architectures) and of network/web related protocols
- Conduct and managed control assurance activities such as penetration testing

Key Accountabilities – Position Specific

Position Description



1. Leadership of ICT Security Function and Team using the performance management and development process that provides an overall context and framework to encourage employee contribution and includes goal setting, feedback, and performance development planning.
2. Undertake research on ICT security technology to assess the best ICT security technology alternatives and provide recommendations on the suitability of new ICT security technology and infrastructure including appropriate resourcing.
3. Develop, implement, monitor, test and review ICT security systems, policies, procedures, and processes for all sites, to move towards best practice ICT security principles and practices.
4. Manage cyber-attacks or cyber breaches to ensure impact on systems and data is minimised and experience is used to minimise future threats and/or strengthen systems and procedures.
5. Collaborate with ICT team and relevant business units to provide accurate estimates, define project priorities, schedule work, and identify opportunities for use of new technologies.
6. Negotiate effectively with team members, vendors, subcontractors, customers, and consultants to define roles, requirements, and approaches for producing the ICT security solution.
7. Establish and maintain ICT security roles, responsibilities, policies, standards, and procedures. Security monitoring, periodic testing and implementing corrective actions for identified security weaknesses or incidents.
8. Provide recommendations, cost benefit analysis and ad hoc consultancy on the suitability of new ICT security technology and solutions. Also provide advice and guidance to project managers and ICT specialists on tools, technology and methodology related to the design and development of ICT security solutions
9. Define ICT security strategy, policies, processes, and procedures to monitor and report on security plans, vulnerabilities and resolve accidents.
10. Manage and participate in team roster to respond to after hours' call outs as required.

Key Accountabilities – Core
1. Use Corporate IT Applications/Systems, ensuring compliance with Council standards and policies, to facilitate achievement of required outcomes.
2. Comply with the requirements of Council's Work Health Safety Management System (WHSMS) and fulfil relevant WHS responsibilities as per WHS-01.1.1 Responsibilities, Authority and Accountability Guideline whilst employed by or acting on behalf of the Council
3. Comply with the reasonable requests and directions of management whilst employed by or acting on behalf of the Council. This includes undertaking other tasks or duties that may be allocated from time to time
4. Comply with Council's Code of Conduct, policy and procedures whilst employed by or acting on behalf of Council
5. All employees are required to treat colleagues and customers with respect and professionalism without regard to non-relevant criteria or distinctions, as well as report any suspected case of discrimination or harassment that they witness. This requirement is in accordance with Fairfield City Council's Values and commitment to equal employment opportunity and a workplace free of discrimination and harassment.

Position Description



Reporting Relationships

Direct: Nil

This position Reports Directly to the Infrastructure, Security and Operations Manager

No. of Indirect: Nil

Key Relationships

1 Internal

Communicating with	Nature of Communication
Chief Information Officer & ICT Operations & Infrastructure Manager	Face to face and written basis, to brief, seek feedback, report and/or to present recommendations for senior management approval.
Staff within ICT Division and/or Branch	Face to face and written basis, to inform, respond to enquiries, seek feedback, investigate, influence, provide advice, facilitate and/or participate in meetings and work planning.
Staff within the organisation	Face to face and written basis, to answer enquires/requests for ICT security data and information, provide support, advice and guidance and build and maintain relationships.

Key Relationships

2 External

Communicating with	Nature of Communication
Third Party ICT vendors and/or external stakeholders, suppliers, and consultants	Face to face and written basis, to seek input, request quotes, exchange information, investigate issues and provide advice and feedback where necessary. The position is responsible for contractor management including authorisation of work performed or services provided.

Position Dimensions

This position has delegations in accordance with section 378 of the Local Government Act. Responsibilities are to be exercised in accordance with Council's Delegation of Authority. Contact the Governance and Legal Division for delegations designated to this position.

Decision making Authority & Accountability

Position Description



1. The City Manager authorises you to take the actions required to make your workplace safe and to fulfil your WHS responsibilities in WHS-01.1.1
2. The position has the autonomy to plan and prioritise workloads to ensure the efficient co-ordination of ICT security and system analysis.
3. The position takes into consideration information gathered, needs of customers, users, and stakeholders in determining and implementing appropriate solutions and action.
4. The position is guided in its decision making by relevant Council policies, legislation, procedures and other relevant guidelines and regulations to ensure that information provided is relevant and current.
5. The position refers matters that are highly technical or complex or where customers are not satisfied to the manager for resolution.
6. The position is accountable for a specialised and technical function that requires consistent research, investigation, analysis, change management and review to ensure ICT security technology solutions and processes adopted are cost effective, resourced, compatible and software applications and continues to secure council's IT systems over time, and in a constantly changing technological environment.

Problem Solving

1. The position operates in a complex environment where methods, techniques or processes are not well defined requiring the development of new policy, procedures, and standards.
2. This role is expected to work innovatively, collaboratively, and effectively to deliver outcomes that meet the changing ICT security requirements.
3. The position is expected to analyse problems and determine a suitable course of action for issues that may arise in the execution of responsibilities.

Competencies

Performance in this role will be assessed on 6 core competencies that apply consistently to all jobs within Council. Each year performance criteria including 6 relevant job specific competencies (identified in the Job Specific Skills Dictionary) and an Individual Work Plan will be negotiated and established in consultation with your manager.

Signature

Employee:	Signature	Date
Authorised by: (Manager)	Signature	Date