

## Principal Cyber Security Analyst

### Position Description

<b>Directorate</b>	Digital Innovation and Technology	<b>Department</b>	Digital Innovation & Technology
<b>Reports To</b>	Infrastructure and Security Manager	<b>Direct Reports</b>	Yes

#### Position Purpose

The Principal Cyber Security Analyst oversees the information security program to ensure Council data remains secure. They look for opportunities to improve security awareness and business practices to strengthen the organisations security posture.

To ensure Council information is secure, available, accessible and complies with applicable laws and regulations

#### Key Responsibilities and Outcomes

As an Principal Cyber Security and member of the Digital Innovation & Technology Team you will:

##### **Main Tasks:**

- Implement, maintain, and monitor policies and procedures in relation to ICT security.
- Manage Council's suite of security tools to ensure effective monitoring and response to security incidents.
- Ensure the ongoing delivery of ICT and cloud services are within agreed security expectations.
- Promote security awareness and knowledge across the Technology Services department.
- Engage Council and external stakeholders on ICT security matters

##### **Accountable for:**

- Ensuring Councils security policies are fit for purpose, current and are correctly implemented.
- Leading the active monitoring and response to security threats to Council's ICT and cloud environments.
- Acting as a key point of contact, providing expert technical advice to management and other stakeholders on ICT security matters.

##### **Responsible for:**

- Developing and maintaining ICT security policies and procedures
- Developing, maintaining, and testing security incident response plans and playbooks.
- Managing the ICT security awareness training program
- Managing vulnerability assessments and the penetration testing program.
- Facilitating communication and engagement with stakeholders on ICT security matters

##### **Contributes to:**

- Preparation of budgets related to ICT security
- Preparation of security strategies and road maps

## Our Values

Our values shape the way we behave, how we interact with each other and our customers. They underpin our decision making and are our guiding principles for how we work every day. As a team member you will take individual accountability for demonstrating the values expectations and behaviours.

SERVICE

TEAMWORK

INTEGRITY

RESPECT

SUSTAINABILITY

## Decision Making

<i>Budget</i>	N/A
<i>Delegations</i>	Delegations under the Local Government Act 2009 and as directed and published in Council's Delegation Register

## Knowledge & Experience

### **Experience:**

Expert level role having five years or more of experience in the discipline and is generally considered an authority in their area or expertise.

### **Reach:**

Internal and External

Influences widely across the organisation and coordinates activities with external organisations in own area of expertise.

### **SFIA Responsibility Skills required:**

#### **Autonomy**

- Works under broad direction. Work is often self-initiated.
- Is fully responsible for meeting allocated technical and/or group objectives.
- Analyses, designs, plans, executes, and evaluates work to time, cost and quality targets.
- Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities.

#### **Influence**

- Influences organisation, customers, suppliers, partners, and peers on the contribution of own specialism.
- Makes decisions which impact the success of assigned work, i.e. results, deadlines, and budget.
- Has significant influence over the allocation and management of resources appropriate to given assignments.
- Leads on user/customer and group collaboration throughout all stages of work. Ensures users' needs are
- met consistently through each work stage.
- Builds appropriate and effective business relationships across the organisation and with customers, suppliers, and partners.
- Creates and supports collaborative ways of working across group/area of responsibility.
- Facilitates collaboration between stakeholders who have diverse objectives.

#### **Complexity**

- Contributes to the development and implementation of policy and strategy.
- Performs highly complex work activities covering technical, financial, and quality aspects.
- Has deep expertise in own specialism(s) and an understanding of its impact on the broader business and wider customer/organisation.

## **Business Skills**

- Demonstrates leadership in operational management.
- Analyses requirements and advises on scope and options for continual operational improvement.
- Assesses and evaluates risk.
- Takes all requirements into account when making proposals.
- Shares own knowledge and experience and encourages learning and growth.
- Advises on available standards, methods, tools, applications and processes relevant to group specialism(s) and can make appropriate choices from alternatives.
- Understands and evaluates the organisational impact of new technologies and digital services.
- Creatively applies innovative thinking and design practices in identifying solutions that will deliver value for the benefit of the customer/stakeholder.
- Clearly demonstrates impactful communication skills (oral, written and presentation) in both formal and informal settings, articulating complex ideas to broad audiences.
- Learning and professional development — takes initiative to advance own skills and identify and manage development opportunities in area of responsibility.
- Security, privacy, and ethics — proactively contributes to the implementation of appropriate working practices and culture.

## **Knowledge**

- Is fully familiar with recognised industry bodies of knowledge both generic and specific, and knowledge of the business, suppliers, partners, competitors, and clients.
- Develops a wider breadth of knowledge across the industry or business. Applies knowledge to help to define the standards which others will apply.

## **SFIA Professional Skills required:**

### **Information Security (SCTY)**

- Develops and communicates corporate information security policy, standards, and guidelines
- Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards, and guidelines.
- Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits, and risks.
- Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.

### **Security Operations (SCAD)**

- Develops policies, standards, processes, guidelines for ensuring the physical and electronic security of systems
- Ensures that the policy and standards for security operations are fit for purpose, current and are correctly implemented.
- Reviews new business proposals and provides specialist advice on security issues and implications.

### **Vulnerability Management (VUAS)**

- Plans and manages vulnerability assessment activities within the organisation
- Evaluates and selects, reviews vulnerability assessment tools and techniques.
- Provides expert advice and guidance to support the adoption of agreed approaches.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems

### **Risk Management (BURM)**

- Plans and implements complex and substantial risk management activities within a specific function, technical area, project, or programme.
- Implements consistent and reliable risk management processes and reporting to key

stakeholders.

- Engages specialists and domain experts as necessary
- Advises on the organisation's approach to risk management.

#### **Technology Service Management (ITMG)**

- Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance, and effective use of specific technology services.
- Leads the delivery of services, ensuring that agreed service levels, security requirements and other quality standards are met. Ensures adherence to relevant policies and procedures.
- Ensures that processes and practices are aligned across teams and providers to operate effectively and efficiently.
- Monitors the performance of technology services. Provides appropriate status and other reports to managers and senior users.

#### **Stakeholder Relationship Management (RLMT)**

- Identifies the communications and relationship needs of stakeholder groups. Translates communications/stakeholder engagement strategies into specific activities and deliverables.
- Facilitates open communication and discussion between stakeholders.
- Acts as a single point of contact by developing, maintaining, and working to stakeholder engagement strategies and plans. Provides informed feedback to assess and promote understanding.
- Facilitates business decision-making processes. Captures and disseminates technical and business information.

#### **Supplier Management (SUPP)**

- Manages suppliers to meet key performance indicators and agreed targets.
- Manages the operational relationships between suppliers and ensures potential disputes or conflicts are raised and resolved.
- Performs benchmarking and makes use of supplier performance data to ensure that performance is adequately monitored and regularly reviewed. Use suppliers' expertise to support and inform development roadmaps.
- Manages implementation of supplier service improvement actions. Identifies constraints and opportunities when negotiating or renegotiating contracts.

#### **Qualifications**

- Degree in information technology, information systems or other relevant field, or suitable relevant experience.
- Current "C" Class Driver's Licence.

*Note: This position description reflects a summary of the key accountabilities of the position, it is not intended to be an all-inclusive list of duties, steps and tasks. Leaders may direct team members to perform other duties at their discretion.*