POSITION DESCRIPTION

Position Descriptions form a part of an integrated planning process to ensure that individual performances align with the strategic and corporate directions for the City. The Position Description also provides the basis on which selection criteria for the position are determined.

POSITION TITLE:	**CYBERSECURITY ANALYST**
WORKPLACE AGREEMENT:	CITY OF SALISBURY MUNICIPAL OFFICERS ENTERPRISE AGREEMENT NO.14, 2021
CLASSIFICATION:	MOA Level 7
DEPARTMENT / DIVISION:	**CORPORATE DEVELOPMENT / BUSINESS SYSTEMS AND SOLUTIONS**
POLICE CLEARANCE:	REQUIRED
REPORTS TO:	CYBERSECURITY AI LEAD
DIRECT REPORTS:	NIL
POSITION NUMBER:	**NEW**

POSITION OBJECTIVES:	• Deliver and accelerate the implementation and ongoing uplift of cybersecurity capability across the organisation by leading the development and execution of delegated program components under the broad direction of the Cybersecurity Lead. • Operate as a senior cybersecurity practitioner, applying broad expertise across governance, risk, compliance, incident response and awareness to enhance the organisation's security posture. • Independently assess, prioritise and address cybersecurity risks within assigned areas, supporting informed decision-making and effective risk management outcomes. • Provide authoritative specialist advice to stakeholders, influencing decisions and enabling secure business and technology initiatives. • Enhance organisational capability by developing, refining and embedding practical cybersecurity processes, controls and practices within a defined program of work. • Contribute to the ongoing maturity and optimisation of the cybersecurity program, supporting timely delivery of security and compliance outcomes.
VALUES AND BEHAVIOURS:	These Values empower us to **REACH** towards our Vision, deliver exceptional community experiences, quality outcomes and a great place to work. **Respectful** • Create a sense of belonging & pride in the Salisbury community • Respect individual differences • Speak up when you don't feel respected, or are not being treated respectfully • Look after the wellbeing of our community, ourselves and those around us

	Empowerment • Take initiative and act with confidence • Make informed decisions and own the outcome • Share ideas, feedback and solutions • Learn and grow while supporting others to do their best work **Accountable** • Take personal ownership and follow through • Deliver on what we say we will do • Believe that the Community comes first • Speak up when it is important **Collaborative** • Work together, committed to a common purpose • Openly share information • Find ways to connect people for better outcomes **Helpful** • Listen and focus on what we can do • Create new futures and look for opportunities • Make a positive difference
KEY RESPONSIBILITIES:	**Cybersecurity Delivery and Implementation** • Lead the development, implementation and uplift of delegated cybersecurity program components, ensuring alignment with strategic direction. • Translate cybersecurity strategy, frameworks and policies into practical, scalable and sustainable operational solutions. • Operate with a high degree of autonomy to determine delivery approaches, prioritise activities and execute outcomes within assigned scope. • Set outcomes, priorities and delivery approaches within assigned areas of responsibility, operating with limited direction. • Plan, prioritise, coordinate, control and evaluate cybersecurity activities to ensure effective delivery of program outcomes. • Coordinate and control delivery of assigned cybersecurity initiatives in alignment with organisational priorities. • Contribute to the efficient delivery of cybersecurity initiatives, enhancing organisational capability and supporting effective risk and compliance outcomes. **Cybersecurity Risk Assessment and Treatment** • Independently identify, assess and prioritise cybersecurity risks across systems, processes and third-party engagements. • Develop and implement risk-informed control improvements and treatment activities, aligned to organisational frameworks and risk appetite. • Exercise sound judgement in balancing risk, operational needs and compliance considerations, escalating where appropriate. • Exercise delegated decision-making authority within assigned areas, including determining appropriate risk treatment and control implementation approaches. • Design and establish operational practices and procedures that support consistent cybersecurity risk management outcomes. • Support the consistent and effective application of cybersecurity risk management practices through practical implementation and stakeholder engagement. **Cybersecurity Advice and Stakeholder Influence** • Provide authoritative cybersecurity advice and consultative support to internal stakeholders across a range of complex matters. • Translate technical cybersecurity considerations into clear business impacts and practical actions, supporting informed decision-making.

	• Influence stakeholders to adopt appropriate and proportionate security controls, negotiating outcomes where required. • Work collaboratively across the organisation to integrate cybersecurity considerations into business processes and initiatives. **Cybersecurity Capability Uplift and Awareness:** • Develop and deliver targeted cybersecurity awareness and training initiatives, aligned to organisational priorities and risk profile. • Evaluate effectiveness and implement enhancements to improve engagement and behavioural outcomes. • Promote a culture of shared accountability for cybersecurity, supporting consistent adoption of secure practices. • Develop practical tools, artefacts and guidance that enable sustainable and scalable cybersecurity practices across the organisation. **Cybersecurity Operations and Incident Response** • Lead the investigation and coordination of cybersecurity incidents, particularly those requiring advanced analysis or judgement. • Develop and refine incident response procedures, playbooks and operational practices to support consistent and effective organisational outcomes. • Apply independent judgement in complex or ambiguous incident scenarios, ensuring timely and appropriate response actions. • Contribute to the continuous improvement of detection, response and resilience capabilities through analysis of trends and outcomes.
WHS RESPONSIBILITIES:	• Observe and comply with all health and safety policies and procedures within the City of Salisbury, including all safe operating procedures or instructions. • Take all reasonable steps to ensure personal safety and that of others is not put at risk through any act or omission in relation to the above. • Report any identified hazards, incidents including near misses or injuries which arise in the course of work, using the systems and/or documentation available for such reporting. • Fulfil individual requirements to meet any documented WHS objectives arising from biannual performance and development reviews. • Not endanger personal safety or that of others by undertaking work whilst under the influence of alcohol or a drug in breach of Council's Drug and Alcohol Policy. • Undertake WHS training where required, in order to perform duties (refer to WHS Competency Assessment).
GENERAL RESPONSIBILITIES:	• To comply with the City of Salisbury Code of Conduct and all other policies and procedures adopted by the City of Salisbury as varied from time to time. • To manage all Corporate Records in accordance with required procedures. • Responsible for purchasing goods and services in accordance with purchasing guidelines and delegated financial limits.
COMPETENCIES:	• To be determined and written into the individual training plan upon commencement – see Organisational Wellbeing.
ESSENTIAL SELECTION CRITERIA:	• Demonstrated experience as a cybersecurity practitioner with broad capability across multiple domains (e.g. GRC, incident response, architecture). • Proven ability to independently deliver complex cybersecurity initiatives or workstreams within a broader program of work. • Strong understanding of cybersecurity frameworks, controls and practices, and the ability to apply them effectively in organisational contexts. • Demonstrated ability to exercise sound judgement and solve complex problems in dynamic or evolving environments. • Proven ability to influence stakeholders and translate technical considerations into business outcomes.

	• Ability to manage competing priorities and deliver outcomes within defined timeframes, supporting multiple concurrent initiatives.
DESIRABLE SELECTION CRITERIA:	• Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field, or equivalent workplace experience. • Certifications (e.g. CISSP, CISM, GIAC or equivalent) • Knowledge of privacy and cybersecurity legislation as it applies to the South Australian Local Government sector.
SPECIAL CONDITIONS:	• Some out of hour's work may be required.
EXTENT OF AUTHORITY:	• Responsible for purchasing goods and services in accordance with purchasing guidelines and delegated financial limits.

POSITION INCUMBENT NAME:	**SIGNATURE:**	**DATE:**