Position Description
Principal Advisor – Information Security

Division	Corporate Services
Portfolio	Information Services
Business Unit	Information Security
Level	Band 2
Reports To	Manager Information Services
Prescribed Position	No

Position Objective

The Principal Advisor – Information Security is Council's senior specialist authority (non-executive) for information security, cyber risk, privacy and data governance. The role safeguards Council's information assets and community trust through enterprise governance, risk oversight and assurance.

Operating with delegated authority, the role establishes and maintains Council's Information Security, Cyber Resilience, Privacy and Data Governance frameworks; accepts information/cyber risk within approved tolerance; directs mitigation where risk exceeds tolerance; and escalates material matters to the Executive Leadership Team (ELT), Audit & Risk Committee and Council.

The role performs the functional responsibilities of a Chief Information Security Officer (CISO) and Chief Data Officer (CDO) within Council's governance model (without operational ICT management) and acts as a key control owner within Council's enterprise risk and assurance environment. The role is a standing member of the Information Services Portfolio Senior Leadership Group.

Key Responsibilities

Enterprise Governance & Strategic Leadership

- Provide strategic leadership for information security, cyber resilience, privacy and data governance.
- Establish, own and maintain Council's Information Security, Cyber Resilience, Privacy and Data Governance frameworks, aligned to Council objectives, risk appetite and legislative obligations.
- Act as Council's principal escalation point for information-related risk, exercising delegated authority to accept risk within tolerance, direct remediation where risk exceeds tolerance, and escalate material risks to ELT, Audit & Risk Committee and/or Council.
- Champion a culture of responsible data use, risk awareness, and accountability across the organisation.

Executive, Council & Regulatory Engagement

- Provide independent, authoritative advice to the Executive Leadership Team, the Audit & Risk Committee and Portfolio Business Partners
- Prepare and present formal reports and assurance updates, including annual cyber security and data governance reporting.
- Act as the senior officer contact for high-impact cyber security or information incidents, supporting executive decision-making and coordinating governance responses, investigations and regulatory matters as required.
- Represent Council in formal engagements with regulators, oversight bodies and insurers through established governance and executive channels.

Chief Data Officer (Functional Leadership)

- Perform the functional role of Chief Data Officer, providing enterprise-wide leadership.
- Chair Council's Data & Governance Steering Group, setting enterprise priorities and resolving cross-portfolio issues.
- Establish and oversee Council's data domain and data ownership model, including enterprise standards for data classification/sensitivity, ethical use and disclosure, data quality, and lifecycle management
- Ensure data governance principles are embedded into digital and system design, procurement and third-party arrangements, and business process redesign and transformation initiatives.

Information Security & Cyber Governance

- Provide governance oversight of Council's cyber security posture, aligned to relevant frameworks and legislative obligations (including Essential Eight maturity expectations and local government sector requirements
- Own Council's cyber and information risk registers, including oversight of residual risk positions accepted by executives.
- Chair the Cyber Security Steering Group, ensuring enterprise prioritisation, accountability, and alignment with organisational risk appetite.
- Provide governance and Provide governance oversight of security operations delivered by internal teams and managed service providers, including liaison with Council's managed Security Operations Centre (SOC/SIEM-as-a-Service)
- Oversee incident response and data breach governance arrangements, cyber resilience and recovery scenarios, and organisation-wide security awareness and education.

Risk, Assurance & Control Ownership

- Act as a key control contributor within Council's enterprise risk management framework.
- Lead enterprise information and security risk assessments, including third party, SaaS, and cloud risks.
- Coordinate internal and external audits relating to information security, data governance, and privacy.
- Provide independent assurance to ELT and Audit & Risk Committee on the effectiveness of controls and the maturity of governance frameworks.

People Leadership & Capability Building

- Lead, coach and performance-manage a small specialist team delivering information security, cyber governance, data governance and assurance outcomes.

- Build organisational capability through targeted education, awareness and professional development, and establish effective cross-functional partnerships across Governance & Risk, Legal, Records, ICT, Architecture and business units.
- Influence leaders to embed security and data governance considerations into decision-making, projects and culture.
- Positively contribute to our constructive culture by living our values which guide decision making and delivery of outcomes for our community.
- Actively deliver an innovative customer experience that's effortless, delivered with care and exceeds our customers' expectations.
- Responsible for being actively involved in the identification and management of the day to day risks of their activities and projects.
- Take reasonable care for your own and others health and wellbeing in accordance with the Work Health & Safety Act 2012 and with Council's Work Health & Safety Managements Systems.
- Promote and maintain a child safe environment and take action as per Council's Children and Vulnerable Persons Policy.

Selection Criteria

Skills

- Demonstrated ability to operate credibly and influence decision-making at Executive Leadership Team, Audit Committee, and Council level.
- Proven capability to design, establish, and govern enterprise-wide information security, cyber risk, privacy, and data governance frameworks.
- Strong leadership and people management skills, including the ability to lead, coach, and develop specialist professional teams.
- High-level strategic advisory, assurance, and stakeholder engagement skills in complex, high-risk environments.

Knowledge

- Strong understanding of Australian public sector/local government governance and legislative obligations relevant to information security, privacy, risk management and ethical data use.
- Contemporary knowledge of cyber security standards, governance frameworks and assurance practices applicable to regulated environments.

Experience

- Extensive senior-level experience in information security, cyber risk, privacy, data governance or related enterprise governance roles.
- Demonstrated experience providing authoritative advice, reporting and assurance to senior executives and/or governance committees in complex environments.
- Experience operating within local government or similarly regulated public sector environments, including governance-led operating models.

- Experience governing or implementing Microsoft Purview (or equivalent information governance and security platforms) and managing third-party/cloud risk.

Qualifications & Requirements

• Relevant tertiary qualification in cyber security, information governance, law, risk management, or a related discipline, or equivalent demonstrated experience.	Essential
• Senior professional certifications such as CISSP, CISM, CISO, CGEIT, or equivalent.	Desirable
• Microsoft Certified: Information Security Administrator Associate or equivalent vendor certification.	Desirable