CITY OF SYDNEY

Position Description (Employee)
IT Security Officer

Division	**People, Performance and Technology**
Business Unit	**Technology & Digital Services**
Grade/Band	**Band 8**
Date position description approved	**2 August 2019**

Council overview

At the City of Sydney our people are our most important asset and central to achieving our exciting and ambitious Sustainable Sydney 2030 – developing a green, global and connected city. The City of Sydney works to build socially sustainable communities that support a more inclusive Sydney – a city that is also more connected, liveable and engaged.

From our high-quality facilities to local services and initiatives, we are dedicated to delivering the best city environment for business, work, living and recreation.

Council values

Our people are custodians of public trust and confidence. In recognising this, we are committed to building a high performing culture built on the values of collaboration, courage, integrity, innovation, quality and respect. These six core values guide everything we do at the City.

Primary purpose of the position

The IT security officer plays an integral part in the development, implementation, and compliance of information technology security across the organisation. The officer is responsible for managing risks related to information security, network security, business continuity planning, crisis management, privacy, and compliance. Partnering with diverse stakeholders to provide advice and support on information security concerns, culture, capability, and continuous improvement to help the City deliver on its purpose to Lead, Govern and Serve and achieve Sustainable Sydney 2030.

In addition, the officer ensures all staff members are trained on the City and best practice security requirements through cyber security awareness programs.

Key accountabilities

- Provide strategic and tactical security recommendations and advice on new and existing products and services, business processes, infrastructure solutions, and technology and business applications to drive successful outcomes for the business and employees.
- Lead and contribute to managing security risk assessments and related project initiatives aimed at meeting the strategic objectives of the City's IT Security Strategy.

- Monitor and investigate, security incidents/issues, and ensure that they are responded to and resolved promptly based on their risk level.
- Oversee network and business application user privileged access reviews to ensure the access is in line with the role requirements.
- Coordinate and maintain regular vulnerability assessments as well as annual network penetration testing and remediation processes to ensure patches and upgrades are applied and prioritised based on vulnerability risk.
- Ensure that security policies, standards, procedures, records and registers are maintained to provide continued security assurance and governance.
- Support the management of the City's Managed Security Services Provider.

Key challenges

- Delivering accurate and consistent work within a high volume environment
- Building security culture and developing security awareness programs for a diverse group of people leaders and employees with various levels of skills, knowledge and experience.
- Establishing and maintaining effective partnerships with multiple stakeholders and consulting effectively to drive strategic objectives.

Key relationships

Who	Why
Internal	
Manager	• Receive advice and report on progress towards business objectives and discuss future directions • Provide expert advice and contribute to decision making • Identify emerging issues/risks and their implications and propose solutions
Project Teams	• Guide, support, coach and mentor team members on security related topics • Lead discussions and decisions regarding key projects and deliverables
Stakeholders (All Business units and departments)	• Provide expert advice on a range of project related issues and strategies • Optimise engagement to achieve defined outcomes • Manage expectations and resolve issues
External	
Stakeholders	• Engage in, consult and negotiate the development, delivery and evaluation of projects • Manage expectations and resolve issues
Vendors/Service Providers and Consultants	• Act as a liaison between the Managed Security Services provider and the City to work on cyber security incident escalations and service related inquiries • Communicate needs, facilitate routine business transactions and resolve issues • Negotiate and approve contracts and service agreements • Manage contracts and monitor the provision of service to ensure compliance with contract and service agreements

Key dimensions

Decision making

The position is accountable for decisions regarding all security operational objectives and for the provision of security advice to project team members and relevant stakeholders on day to day operational decisions.

Reports to

Manager, IT Security and Risk

Estimated number of indirect reports

None

Essential Knowledge, Skills & Experience

- A solid knowledge of cyber security methodologies and frameworks, such as ISO 27001, 27002 and 27005, NIST and ISM.
- Working knowledge of Endpoint Protection Products (knowledge of McAfee ePO and McAfee Endpoint Security products is highly desirable).
- Knowledge of Email and Web Security, Microsoft Office 365 Security, Microsoft EOP/ATP.
- A solid knowledge of infrastructure and network security technologies.
- A relevant degree qualification in Information Security or industry certifications (CISSP, CISA or CISM).

Capabilities for the position

The City's capability framework outlines the capabilities everyone needs to work well in their role. They are expressed as behaviours that show expected knowledge, skills and our values. There are capabilities for **employees** and managers which provide clarity, common language and consistency.

Capability Group	Capability Name	Level
Personal attributes	Act with Integrity and Courage	Adept
	Demonstrate Accountability	**Advanced**
	Manage Self	Adept
	Display Resilience and Adaptability	Adept
Relationships	Work Collaboratively	Adept
	Communicate and Engage Respectfully	Adept
	Community and Customer Focus	Adept
	Influence and Negotiate	**Adept**
Results	Deliver Quality Results	Intermediate
	Create and Innovate	Intermediate
	Plan and Prioritise	Adept
	Think and Solve Problems	**Adept**
Resources	Finance	Intermediate
	Technology and Information	**Advanced**
	Assets and Tools	Intermediate
	Procurement and Contracts	Adept

***This profile is subject to an organisation-wide review of capability profiles. The final profile may vary slightly.*

Focus capabilities

The capabilities in bold are the focus capabilities for this position. The focus capabilities are those judged to be most important at the time of recruiting to the position. That is, the ones that to be met at least at a satisfactory level for a candidate to be suitable for appointment.

Group and Capability	Level	Behavioural Indicators
Personal Attributes Demonstrate Accountability	Advanced	• Is prepared to make decisions involving tough choices and weighing of risks • Addresses situations before they become crises and identifies measures to avoid recurrence • Takes responsibility for outcomes, including mistakes and failures • Coaches team members to take responsibility for addressing and resolving challenging situations • Oversees implementation of safe work practices and the risk management framework
Relationships Influence and Negotiate	Adept	• Builds a network of work contacts/relationships inside and outside the organisation

		• Approaches negotiations in the spirit of maintaining and strengthening relationships • Negotiates from an informed and credible position • Influences others with a fair and considered approach and sound arguments • Encourages others to share and debate ideas
Results Think and Solve Problems	Adept	• Draws on numerous sources of information, including past experience, when facing new problems • Demonstrates an understanding of how individual issues relate to larger systems • Makes appropriate recommendations based on synthesis and analysis of complex numerical data and written reports • Uses rigorous logic and a variety of problem solving methods to develop workable solutions • Anticipates, identifies and addresses risks and issues with practical solutions • Leads cross team/unit efforts to resolve common issues or barriers to effectiveness
Resources Technology and Information	Advanced	• Implements appropriate controls to ensure compliance with information and communications security and use policies • Implements and monitors appropriate records, information and knowledge management systems • Seeks advice from technical experts on leveraging technology to achieve organisational outcomes • Stays up to date with emerging technologies and considers how they might be applied in the organisation