

<b>Position Title</b>	Cyber Security Analyst
<b>Department</b>	People and Performance
<b>Unit</b>	Information Communication and Technology
<b>Team</b>	ICT Governance and Risk
<b>Supervises</b>	Nil
<b>Reports To</b>	Coordinator ICT Governance and Risk
<b>Grade Range</b>	I
<b>Date Prepared</b>	1/04/2023
<b>Date Last Updated</b>	21/06/2023

## Our Vision & Values: A leading organisation that collaborates & innovates



We are committed to **safety**



We work as one **team**



We act with **integrity**



We care about our **customers**



We **continuously improve**

## Primary purpose of position

This role is responsible for proactively identifying, investigating, and mitigating security incidents and risks. This role will drive the implementation and continuous improvement of the cyber security function in alignment with Council's Cyber Security framework and roadmap ensuring a strong security posture.

## Accountabilities

- Conduct regular security assessments and audits of systems, networks, and applications to identify vulnerabilities and potential threats and to ensure appropriate control measures are in place.
- Undertake problem determination and root cause analysis of security incidents and work with stakeholders to investigate and resolve ensuring corrective actions are implemented appropriately
- Implementation and maintenance of security controls including the ASD Essential 8
- Monitor and analyse security logs, alerts and network traffic to detect security breaches and potential threats
- Stay up-to-date with the latest latest cyber development, risks, standards and frameworks
- Develop and maintain security policies, procedures, and guidelines
- Develop and maintain accurate technical designs, specifications, and documentation.
- Provide expert input to the strategic direction of technology investments to ensure Council maintains a strong security posture
- Development, management, testing and execution of an Incident Response Plan and lead investigations in to security incidents and breaches.
- Additional duties as required within the limits of the employee's skill, competence and training

## Position capabilities and level

Below is the full list of capabilities and the level required for this position. The capabilities in bold are the focus capabilities for this position. Refer to the next section for further information about the focus capabilities.

Capability Profile – Senior Technical/ Professional Specialist		
Capability Group	Capability Name	Level
 Personal Character	Lead Self	Advanced
	<b>Display Resilience</b>	Adept
	Act with Integrity	Advanced
	Safety and Accountability	Advanced
 Relationships	Communicate and Engage	Adept
	Customer and Community Focus	Adept
	<b>Work Collaboratively</b>	Advanced
	Influence and Negotiate	Adept
 Results	<b>Plan and Prioritise</b>	Advanced
	Think and Solve Problems	Adept
	Innovate and Improve	Advanced
	Deliver Results	Advanced
 Resources	Finance	Adept
	Assets and Tools	Adept
	Technology and Information	Adept
	Procurement and Contracts	Adept
 People Leadership	Manage and Develop People	N/A
	Inspire Direction and Purpose	N/A
	Optimise Workforce Contribution	N/A
	Lead and Manage Change	N/A

## Focus Capabilities

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

### CBCity Capability Framework - Focus Capabilities

Group & Capability	Level	Behavioural Indicators
<b>Relationships</b>		
Work Collaboratively	Advanced	<ul style="list-style-type: none"> <li>• Builds a culture of respect and understanding across the organisation</li> <li>• Facilitates collaboration across units and recognises outcomes resulting from effective</li> <li>• Builds co-operation and overcomes barriers to sharing across the organisation</li> <li>• Facilitates opportunities to develop joint solutions with stakeholders across the region and sector</li> <li>• Models inclusiveness and respect for diversity in people, experiences and backgrounds</li> </ul>
<b>Personal Character</b>		
Display Resilience	Adept	<ul style="list-style-type: none"> <li>• Is flexible, showing initiative and responding quickly to change</li> <li>• Accepts changed priorities and decisions and</li> <li>• Gives direct and honest feedback/ advice</li> <li>• Listens when challenged and seeks to</li> <li>• Raises and works through challenging issues and seeks alternatives</li> </ul>
<b>Results</b>		
Plan and Prioritise	Advanced	<ul style="list-style-type: none"> <li>• Ensures business plans and priorities are in line with organisational objectives</li> <li>• Uses historical context to inform business plans and mitigate risks</li> <li>• Anticipates and assesses shifts in the</li> <li>• Ensures that program risks are managed and strategies are in place to respond to variance</li> <li>• Implements systems for monitoring and evaluating effective program and project</li> </ul>

\* Focus Capabilities are those judged to be the most important at the time of recruiting to the position. The mix of “focus” capabilities can change over time, reflecting changing work priorities and current team strengths.

## Delegations

Decisions associated with this position are to be made in accordance with the Delegations of Authority (Policy186) approved by the General Manager.

## Code of Conduct

All staff are required to adhere to the Code of Conduct (CP25).

## Work Health & Safety

All staff are required to adhere to Council's WHS&E Responsibilities and Authorities document (REF229) and associated policies and procedures.

## Records Management

All staff are required to comply with Council's Records and Information Management policies, procedures and guidelines.

## Qualifications and Experience

### Essential Qualifications

- Tertiary qualifications in Information technology, security or related discipline and/or equivalent knowledge skills and experience with a demonstrated commitment to ongoing professional development

### Essential Experience

- Extensive IT technical/operational background in a Windows based environment including knowledge in databases, operating systems, M365, networking and their security.
- Proven knowledge of and experience in applying security compliance, privacy, government policy and industry frameworks, including ISO 27001, NSW Cyber Security Policy and ASD ISM.
- Experience in, and demonstrated understanding of threat intelligence and analysis, which involves monitoring and analysing threats and vulnerabilities to identify potential risks to an organisation.
- Experience with vulnerability scanning solutions, antivirus, identity management and security software
- Extensive experience of risk management processes (e.g., methods for assessing and mitigating risk) and dealing with cyber threats and vulnerabilities.
- Experience in utilising intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Extensive written and verbal communications skills, with the ability to communicate technological solutions related concepts to technical and non-technical audiences at various levels.
- Extensive analytical and problem-solving skills with the ability to manage multiple concurrent customer requests within Service Level Agreements from initiation to resolution.

## Desirable Qualifications and or Experience

- Relevant certifications such as CISSP, CISM, or CISA
- ITIL certification
- Project management certification or equivalent experience
- Previous Public Sector experience

HUMAN RESOURCES USE (SELECT YES OR NO)	YES	NO
Does this position fall under the definition of child related employment?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Does this position require incumbent to undergo criminal reference check?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Does this position require incumbent to demonstrate good driving Licence class required: C Class Drivers Licence	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Will incumbent need to make disclosure of pecuniary interest?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Could there be a conflict of interest with secondary employment?	<input checked="" type="checkbox"/>	<input type="checkbox"/>