

POSITION DESCRIPTION

Position Title:	Cyber Security and Systems Coordinator	Directorate:	Community & Corporate Services
Position Number:	100348	Department:	ICT
Employment Status:	Full-Time	Section:	Cyber Security and Systems
Employment Type:	Permanent	Location:	Chambers
Classification:	Schedule A, Salary Point 15+2		
Reports to:	Chief Information Officer		

PRIMARY PURPOSE:

The primary function of this role is to coordinate the Council's Cyber Security and Systems team to ensure the ongoing development and delivery of Council's cybersecurity program to manage risk and support Council's strategic needs.

ORGANISATIONAL REPORTING RELATIONSHIPS:

1. Internal:

- The **Cyber Security and Systems Coordinator** reports to the **Chief Information Officer (CIO)** for all operational and management matters.
- The role will work highly collaboratively with other areas of the ICT Team and across the organisation.
- This position supervises the Cyber Security and Systems Team.

2. External:

- The role will liaise with external stakeholders such as contractors, service providers and other professional ICT groups as required.
- The role will liaise with external cybersecurity Government agencies such as the Australian Cyber Security Centre and Tasmanian Department of Premier and Cabinet Digital Strategy and Services (DSS) team.

OUR VALUES:

We respect each other

We respect the skills, knowledge and diversity of our team mates

Everyone is heard and is valued

We care for the well-being and safety of each other

We check in on each other without being prompted

Listening and being listened to matters

We are trusted

I've got your back and you've got mine

We do what we say we will

We are empowered

Have honest and open conversations

We are trusting and trustworthy

We learn from our mistakes and share what we learn

Together we are better

Robust and thoughtful decision making together

Solving important problems together

We reach out to others and across teams for help

We collaborate more and handball less

Share our skills and knowledge

We deliver

We serve and stand up for our community

We knuckle down and focus on what matters

We are courageous and determined to find a way

We seek opportunities to continually improve outcomes and then we act on them

OUR CULTURE:



We foster and model a culture where:

- We **RESPECT** others and their viewpoints as being as important as our own.
- We trust and are **TRUSTED** by each other.
- We know that by working **TOGETHER** we achieve better outcomes.
- We take personal responsibility, and together we **DELIVER** for our community.

This is **OUR WAY** to achieve results through our people and teams to make Glenorchy a better place every day.

KEY RESPONSIBILITIES:

RESPONSIBILITIES/TASKS	DUTIES
Cyber Security uplift	<ul style="list-style-type: none">• Develop and implement programs to uplift Council cybersecurity capability, awareness, and responsiveness.• Collaborate with Council's Governance and Risk department to development business continuity plans (BCP) and disaster recovery plans (DRP).• Collaborate with the Council's Human Resources Department and the wider ICT Team to deliver programs to continually develop staff's digital Cyber literacy and awareness, and to ensure effective cyber work practices.• Ensure that the ICT solutions, products, and services are designed, implemented, and operated with robust security controls.
Cyber Security Incidents	<ul style="list-style-type: none">• Develop response plans and solutions for dealing with cyber security incidents by collaborating with other ICT officers and Council's Governance and Risk and Human Resources departments.• Working with CIO and other nominated Senior Council Officers provide coordination and support during cyber security events.• Upon direction by CIO, lead investigations into cyber security violations and incidents to ensure adequate reporting and resolution.• Collaborate with affect departments in conducting post-incident analysis to identify areas for improvement.
Coordinate ongoing Cyber monitoring & assessment	<ul style="list-style-type: none">• Work with external auditors and Council corporate risk processes to coordinate and schedule ICT auditing activities, including workshops, Scenario testing exercises, interviews, reports and other related activities.• Ensure Council's ICT providers comply with their Cyber Security obligations and have appropriate custodianship of Council's data, and ensure effective measures are in place for ongoing compliance with both Council and legislative requirements.• Continuously develop cyber threat intelligence and investigate, prioritise and address key risk mitigations.
Ensure System availability and continuity	<ul style="list-style-type: none">• Responsible for Council's ICT systems backup and redundancy.• Collaborate with Council's ICT providers to ensure appropriate service levels are attained and sustained to support Councils' digital services and operations and operational resilience.

	<ul style="list-style-type: none"> Foster a culture of risk awareness and management, and ensure the team adheres to ICTs change management framework.
ICT Systems	<ul style="list-style-type: none"> Lead key technology sourcing arrangements. Manage existing “as-a-Service” arrangements for telephony, network, and ICT cloud services. Manage key centralised Identify and Access systems and ensure best practice approaches to their use and effectiveness. Manage relevant third party suppliers, vendors and contractors, and related Service Level Agreements. Investigate and develop proposals for new technologies and service approaches to enhance Councils ICT supporting systems and provisioning models. Manage infrastructure that support a Managed Operating Environment covering Councils End user technologies. Develop, implement and monitor project management plans to ensure successful implementation of new or upgraded systems where appropriate. Collaborate with the business Services Team to manage system change and new systems implementation activities.
Manage the Cyber Security and ICT Systems Team and staff	<ul style="list-style-type: none"> Responsible for the management of the Cyber Security and Systems Team, and proactively managing its priorities and resources to meet Council’s digital priorities. Be proactive in supporting and building a culture of high performance, continuous learning, and teamwork by modelling a collaborative and empowering approach. Manage day-to-day activities of all staff, ensuring appropriate outcomes are met in a timely and customer focused manner. Provide input, advice and assistance as required into the development of the Council’s policies, directives, strategies and guidelines.
Financial Requirements	<ul style="list-style-type: none"> Support CIO in the development of the annual ICT Budget. Responsible for complying with Council’s Code for Tenders and Contracts.
Customer Service	<ul style="list-style-type: none"> Promote the positive image of Council as a whole. Ensure that a high standard of customer service is maintained to both internal and external customers. Engage, listen to and act where appropriate on feedback from our customers. Implement, evaluate and continuously improve quality systems and processes for the section.
General	<ul style="list-style-type: none"> Assist in the achievement of agreed outcomes consistent with department business plans and budgets. Perform any other duties as directed.
Organisational Responsibilities	<ul style="list-style-type: none"> Support and adhere to Council’s policies and procedures, code of conduct and relevant acts. The incumbent is required to commit to use Council’s electronic content management (ECM) system to retain records and documents relating to Council business as part of their employment.

This role may require reasonable after-hours activities and overtime when required by business needs.

Employees may be required to undertake additional duties within the limits of their skill, competence and training, consistent with their classification level, in any area of Council, as directed.

SPECIALIST DELEGATIONS:

- Nil

KEY SELECTION CRITERIA:

1. Completion of a degree/diploma in a computer related discipline with at least 5 years' experience or equivalent industry experience in a complex ICT operation.
2. Experience and knowledge in Microsoft 365 and cloud-based technologies and in contemporary service delivery and applying Cyber Security in a complex ICT environment.
3. Demonstrated team management and leadership skills and the ability to work effectively in a multi-disciplinary ICT team, with the ability to coordinate and deliver outcomes.
4. Highly developed communication (written and verbal) and interpersonal skills with the ability to build and maintain productive working relationships.
5. Highly developed conceptual, analytical and problem-solving skills and experience in applying solutions to complex problems and issues.
6. Experience in the management of third-party suppliers, including procurement and contract management.

AUTHORISATION:

I hereby agree that this position description accurately reflects the work requirements.

Manager Name:	Craig Pitt		
Manager Signature:		Date:	/ 5 / 2025
Director Name:	Tracey Ehrlich		
Director Signature:		Date:	/ 5 / 2025

I have read and agree to abide by the requirements of this position description.

Employee Name:			
Employee Signature:		Date:	