

Position Description

CORPORATE INFORMATION

Position title	Security Engineer		
Directorate	Corporate Services	Branch/Section/Unit	Information and Technology
Position number		Level	6-7
Award	Queensland Local Government Industry (Stream A) Award – State 2017 Division 2, Section 1		
Line Manager	Coordinator ICT Operations		
Direct reports	Nil		
Indirect Reports	Nil		

SCOPE OF POSITION

Position Summary

This stimulating new role will be responsible for ensuring the security and resilience of Council infrastructure is maintained through deploying, administering, monitoring, managing and patching appliances and operating systems. The role will also be responsible for auditing and compliance of security policy and controls, and ensuring that Cybersecurity playbooks, processes and plans remain up-to-date and current, along with the continuous improvement of the cyber security posture.

The role will also need to support the ICT Infrastructure Engineer in maintaining council's network and server infrastructure.

Key Responsibilities of the Role

- Verify servers are designed, configured with security controls and monitored before release into production and on an ongoing basis to ensure adequate infrastructure protection.
- Grant, monitor, and remove access to the cloud/infrastructure environment according to company policy.
- Managing the currency, integrity, monitoring and appropriate alerting of security appliances and technology within Gympie Regional Council.
- Monitor and assess the environment for vulnerabilities and apply patches according to its criticality and schedule.

- Participate in incident response planning, training and implementation. Respond/support response to security incidents as needed.
- Participate in Business Continuity activities and maintain, test and update the Disaster Recovery plan as needed. Maintain backup schedule as planned.
- Ensuring that disaster recovery plans are maintained and tested against a variety of Disaster scenarios and implementing strategies that ensure resilience and availability of critical systems, and patching is maintained and optimised
- Collaborating with different technical teams across the ICT team to identify and mitigate or monitor unusual or malicious activities
- Advising, leading and implementing as required new controls, processes, playbooks and technology to maintain and uplift the overall maturity as and when the time comes.

Mandatory Licence/Competency (Ticket) Requirements

- Queensland 'C' Class driver's licence that is current and maintained

Essential Knowledge/Skills/Qualifications Criteria

- A tertiary qualification in an IT discipline and/or years' work experience in an IT related role that included security functions and duties
- Industry specific certification in Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP)
- Relevant technology certifications across the Infrastructure landscape (Cisco, Microsoft)
- Experience in enterprise and hybrid technology environments
- Good understanding of Cyber Security Frameworks
- Cloud Security – Hands on experience in managing the following cloud applications
 - Endpoint EDR/XDR - Microsoft Defender and Endpoint Manager (intune) ecosystems
 - Server EDR/XDR – Trend Micro
 - Email and content filtering – Microsoft Defender, CISCO Umbrella
- Exchange Online - Hands on experience in managing Exchange Online
- Active Directory – Hands on experience with Azure AD and on-premises Active Directory
- Firewall – Demonstrated Firewall configuration and design
- Ability to understand and disseminate industry terminology and concepts to technical and non-technical stakeholders
- Experience within IT and OT environments highly desired
- Working knowledge in uplift and maintenance of SIEM platforms
- Excellent understanding of security within the different layers of the IT Landscape.
- Understanding of ISO 27001 security standards
- Experience in documenting designs, executive and technical reports, proposals, statement of work and as built guides

- Experience in supporting large, critical and complex business environments governed by ITSM/ITIL framework
- Experience with Email Security
- Experience in working with AWS, Azure, M365, VMWare ESX, Hyper-V etc, cloud and virtual environments (highly desirable)
- Strong analytical and communication skills both written and verbal
- Ability to work autonomously and under high pressure environment with strict SLAs and project deadlines
- Outstanding customer service skills
- Continuous improvement mindset

Physical Requirements of the Position

- an ability to perform tasks for extended periods whilst in a sitting position and occasionally pushing, pulling or handling objects exerting a force up to 5kg
- an ability to walk up and down stairs whilst occasionally carrying weights up to 15kg
- an ability to clearly hear directions and instructions being provided at normal speech levels.

Special Requirements

- Occasional out of hours work (including weekends).
- Regular local travel.
- Respond to Emergency/Disaster events in accordance with Council's Emergency Management plans and systems.

ORGANISATIONAL INFORMATION

Safety

Behaviours

Maintain a positive attitude towards acquiring an understanding of work health and safety (WHS) legislation, including Council WHS policies and procedures.

Fostering and maintaining a positive attitude towards WHS within the individual work teams.

Responsibility

Applying Council policies and procedures in every day work activities to assist Council in ensuring a safe work environment.

To meet the standards imposed by any relevant safety legislation as required by Queensland's *Work Health and Safety Act 2011*.

Related documents

- WHS Policy statement WHSPOL004.

- Work Health and Safety Responsibility and Accountability Statement WHSPOL008.
- The WHS KPIs are located in the Work Health and Safety Management Plan WHSPOL010 and should be referenced as applicable with this position.

Code of Conduct

As per the Staff Code of Conduct (OCPOL001), employees must conduct all business with integrity, honesty and fairness and comply with all relevant laws, regulations, codes, policies and procedures.

Records Management

Council employees are required to ensure adequate records of actions taken and decisions made whilst undertaking their duties are created and maintained, in accordance with Council's Recordkeeping Policy.

Council's Vision

Gympie Regional Council has a vision for embracing opportunities, promoting wellbeing and celebrating strong communities.

Council's Values

Accountability – We are open, transparent and take responsibility for our actions.

Communication – We consult with the community, actively listen to and respond to the input of residents, and keep people informed.

Customer Service Focused – We meet the needs of the community in an efficient and effective manner. We strive to continually improve, show empathy and are environmentally aware in our service delivery.

Integrity – We act with honesty and respect in all we do and respect all residents, colleagues and visitors.

Teamwork and Collaboration – We recognise and support everyone's contributions. We are inclusive and contribute respectfully working as a team. We will care for ourselves and others.

Position Description

POSITION APPROVAL AND ACCEPTANCE

Approved by

Name		Position	
Signature		Date	

Accepted by

Name			
Signature		Date	

The scope and requirements of this position as well as the organisational structure is subject to change by Council as required by business needs.