POSITION DESCRIPTION

Position Title:	**Cyber Security Officer**	**Reports to:**	**Manager Information, Communication and Technology**
Department:	Information, Communications and Technology	**Directorate:**	Corporate Services
Stream:	Stream A	**Pay Level:**	Level 6 (Division 2 - Section 1) 12% superannuation & 17.5% leave loading
Award:	Queensland Local Government Industry Award – State 2017	**Agreement:**	The Southern Downs Regional Council Certified Agreement, as amended

1.1 THE DEPARTMENT

The ICT department delivers the ICT strategy for Council, including managing the technology infrastructure that supports day-to-day operations of Council, facilitating communication, enhancing service delivery, ensuring cybersecurity and data protection, and driving innovation and digital transformation. This department plays a key role in improving efficiency, transparency, and the quality of services provided to the community.

The department is also responsible for overseeing the proper handling, organisation, storage, retention, and disposal of records. These records may include physical documents, digital files, and other forms of information that Council needs to maintain for legal, regulatory, and operational purposes. This department plays a crucial role in ensuring transparency, accountability, and compliance with various legal requirements.

1.2 VALUES

Southern Downs Regional Council recognises our people as our strength, and our five values guide how we work with each other, our actions, our decision making and how we serve our community. Our values bring us all together and contribute to our employees having a meaningful and rewarding career, with opportunities to grow and thrive.

Act with Integrity | **One Region, One Team** | **Lead by Example** | **Service Excellence** | **Our People, Our Strength**

1.3 THE OPPORTUNITY AND JOB ROLE

The key function of the role as the Cyber Security Officer is to assist the Manager ICT in the delivery of timely, efficient, customer focussed Cyber Security strategic objectives. The position is an onsite role and will directly contribute to strengthening our cyber security maturity using a combination of identify, protect, detect, response and recover approaches to maximise the continued delivery of the organisational critical infrastructure services.

The role participates in the support of the efficient operation of Council's enterprise networks, hardware platforms, core network infrastructure, communication platforms, applications and access control systems, while maintaining a high-level of system accuracy.

1.4 KEY RESPONSIBILITIES AND DELIVERABLES

The key responsibilities may be modified from time to time to ensure the expected outcomes support the Council's operational and corporate plans. All duties are to be conducted in an efficient, timely, professional and safe manner.

The key responsibilities and deliverables for this role include:

- Promote a collaborative team environment that fosters creativity, innovation, and knowledge capture/sharing to achieve organisational outcomes;
- Undertake day-to-day ICT hardware and software operational support activities to deliver impacted user incident remediation, vendor mitigations for vulnerabilities, and project deliverables as required.
- Triage, assess and formulate recommendations for security related tasks. This involves holding technical discussions relating to cyber security queries within the ICT team, vendors, partners, or non-technical discussions with other business units.
- Apply specialist cyber security knowledge and proactively analyse and respond to current emerging and organisation-specific threats based on private and public threat feeds or reports to drive a reduction in vulnerability exposure.
- Provide specialist operational expertise on time-sensitive detection, identification, and alerting of intrusions, anomalous and misuse activities across all environments to triage and address these events as either incidents or benign activities.
- Promptly and thoroughly identify, report and investigate security breaches including determining potential impact, performing root cause analysis and making recommendations on remediation.
- Support, build upon and enhance cyber security orchestration within the security stack. This may include integrations into third-party security solutions, business applications, and other cloud or on-premises solutions.
- Mentor and guide the agreed cyber defence practices providing technical and framework advice, operational support, and guidance to strengthen security awareness, operations, and resilience across the organisation.
- Work collaboratively across the organisation to manage assessments, audit reviews, vulnerability scanning, penetration tests, preparatory exercises, to enhance capability and resilience.
- Develop, maintain and deliver reporting on maturity levels across functional items such as audit, risk, incident events, threats and response to adhere to organisational policy, standards and guidelines, Industry best practice and relevant Industry standards and frameworks.
- Responsible for maintaining the documentation for ICT Disaster Recovery / Business Continuity processes and incident response procedures on an agreed schedule, ensuring the organisation has a strong cyber-security posture.
- Effectively manage and deliver ICT projects within the agreed timeframes and in accordance with project management principles and frameworks, including the provision of expert advice.
- Responsibly handle potentially sensitive information and maintain records consistent with Council requirements and the Privacy Principles.
- In collaboration with the Manager ICT, and ICT Coordinator, contribute to the development, review and update of ICT policies, procedures and guidelines in a timely manner.
- Implement, develop and maintain cybersecurity initiatives through the delivery of planning various activities and timeframes to achieve a successful outcome.
- Keep up to date with emerging threats, vulnerabilities, and security technologies.

Other duties as directed by the supervisor.

1.5 SELECTION CRITERIA

ESSENTIAL CRITERIA

1. Experience working in a team environment to deliver shared outcomes through communication skills and the ability to work with stakeholders, vendors and delivery partners.
2. Proven experience in delivering high quality ICT support to clients supporting at least one of the following Cyber Security activities such as: Incident Response, Vulnerability Management, Cyber Threat Intelligence or Cyber Defence Tools, with an emphasis on self-managing workloads, prioritising tasks and working unsupervised.

3. Demonstrated expertise in the support, configuration, monitoring and implementation of ICT environments in one or more of the following technical domains: ICT infrastructure, server and desktop hardware, network peripherals, mobile devices, networking, information systems, enterprise applications.
4. Sound knowledge of Cyber Defence technologies and concepts in relation to items such as applications, end user devices, enterprise infrastructure, or networks and taking a proactive customer focused approach to service delivery.
5. Knowledge of at least one of these standards or frameworks – ASD E8, ISM, NIST CSF, IS 18 and ISO/IEC 27000 series
6. Sound written and verbal communication skills alongside a demonstrated ability to build relationships in an onsite customer support facing role.
7. Ability to travel and attend different Southern Downs Council work sites to meet, support and collaborate with our various business areas. Occasional travel within SE QLD for conference or training purposes will also be required.

DESIRABLE CRITERIA

1. A sound understanding and general interest in Local Government operations.
2. Working knowledge of the importance of timely Cyber Security actions and the ability to document and explain technical details clearly and concisely to both technical and non-technical audiences.
3. Knowledge of the various functions, common toolsets, and their purposes within Security Operations.
4. Industry knowledge of current risks, threats and systemic issues that organisations face, and what causes them.
5. The completion or active progression through industry certifications, training certificate or degree qualifications in information technology or cyber security practices.

1.6 TRAINING

- On the job training will be provided to ensure that the position holder maintains a satisfactory knowledge and skill base.
- The position holder will be encouraged to attend virtual and in-person workshops and seminars relevant to the position to ensure ongoing professional development.

1.7 WORK HEALTH AND SAFETY RESPONSIBILITIES

- Comply with the Work Health and Safety Act, Regulations, Codes of Practice and Council's Work Health and Safety Policies and Procedures.
- Comply with instructions given by the relevant manager and/or supervisor in respect of the health and safety of themselves and the health and safety of other persons.

1.8 ORGANISATIONAL RESPONSIBILITIES

- Comply with all the requirements of Council policies and procedures as amended from time to time.
- Ensure complete and accurate records are captured, created and maintained.
- Deliver high-quality customer service within the organisation and to the public.
- Ensure the security and appropriate intended use of Council information at all times.

1.9 REQUIRED LICENCES AND QUALIFICATIONS

- A person in this position will need to hold tertiary qualification(s) in ICT-related disciplines, OR related ICT industry certifications and demonstrate sufficient subject matter experience and knowledge within the ICT industry.
- A Class C (car) licence or greater is required in this role.

1.10 DESIRABLE LICENCES AND QUALIFICATIONS

- Experience with Information Technology Service Management (ITSM) tools and methodologies (e.g. ITIL).

- A qualification(s) in Project Management, OR demonstrated relevant experience and knowledge, would be highly regarded.

1.11 OTHER POSITION REQUIREMENTS

PROBATION PERIOD

- This role is subject to a three (3) month Probation period to a maximum of six (6) months, during which time the employee will be assessed for suitability as part of ongoing development in the role.

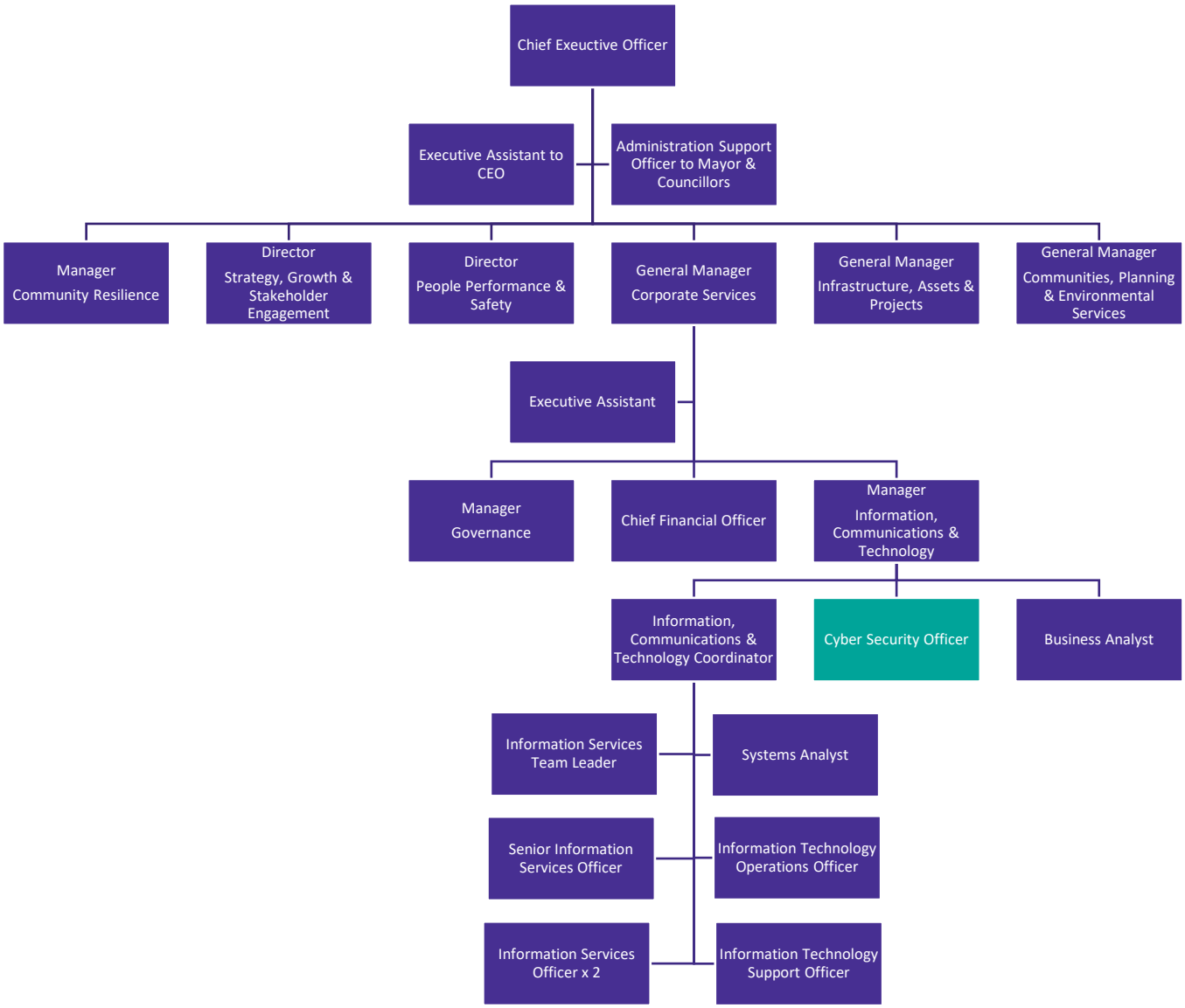
PRE-EMPLOYMENT CHECKS

- Prior to employment external candidates **will** be subject to the following checks in most instances:
    - National Criminal History Check (mandatory)
    - Pathology Drug and Alcohol screening (mandatory)
    - Reference Checks (mandatory)
    - Health Declaration (mandatory)

- Prior to employment external candidates **may** also be subject to the following checks:
    - Functional Capacity Assessment / Fitness for Work (to assess physical suitability for the role)
    - Formal qualifications check
    - Rights to Work in Australia – VEVO check
    - Licence disqualification / traffic history checks with Queensland Government
    - Blue card Working with Children Check
    - Any other check that is reasonably required by Southern Downs Regional Council

1.12 REPORTING STRUCTURE

ORGANISATIONAL RELATIONSHIP



Council values diversity and welcomes applications from people of all backgrounds and cultural heritage, that have working rights in Australia.