



POSITION DESCRIPTION FORM

File No: PDF-F0257207

POSITION IDENTIFICATION

Title:	Cyber Security Administrator	Level:	Level 10
Service Unit:	Information Services	Award:	Local Government Industry Award 2020 Industrial Agreement
Directorate:	Corporate & Governance	Date Effective:	15 November 2021
Reporting to:	Deputy Chief Executive Officer	Date Last Reviewed:	1 December 2023

PURPOSE OF POSITION

- To develop, manage and maintain a strong organisational cyber security and cyber resilience readiness posture for the Shire of Dardanup as a response to an increasing threat landscape.
- Ensure a consistent and systematic approach is being applied to information security practices, system security, and data integrity across the organisation.
- Actively promote cyber security awareness to all staff and elected members.
- Provide advice and recommendations on Information security and associated risks across the organisation.

SUMMARY OF ACCOUNTABILITIES & RESPONSIBILITIES

- Help develop the Shire of Dardanup's Cyber Security and Cyber Resilience strategic plan.
- Liaise with technology teams to ensure secure-by-design engineering practices are applied to all phases of systems and infrastructure implementation.
- Align organisations security practices with relevant industry standards and best practices.
- Undertake regular reviews of the organisation's hardware and software infrastructure to identify key vulnerabilities that need to be addressed.
- Liaise with technology teams to ensure patching is applied within agreed timeframes.
- Develop, implement and regularly review/refine corporate and departmental information security policies and processes to ensure security controls are in place and are being followed.
- Implement and manage cost effective practices to monitor, detect and protect the Shire of Dardanup's information system/network/endpoint environment to minimise the risk of equipment and data loss, theft or tampering.
- Develop and execute plans to respond to incidents and minimise their impact.
- Undertake regular internal/external security risk assessments to stay on top of the Shire of Dardanup's security landscape and highlight to management and stakeholders the key risks posing a threat to the organisation and prioritise recommendations to remediate.

SUMMARY OF ACCOUNTABILITIES & RESPONSIBILITIES

- Coordinate with external agencies and auditors as required.
- Regular reporting to the Audit and Risk committee.
- Participate within the information services disaster recovery project team.
- Provide awareness training and technical advice to staff and elected members on the effective use of information security and of the current threat landscape.
- Assist the technology team to maintain high levels of business system security, integrity and confidentiality.
- Any other duties as directed by the line supervisor / manager.
- Undertake on the job and off the job training as required to develop the necessary knowledge for the position.
- Undertake the established role with other contracted Local Government Entities

ORGANISATIONAL RELATIONSHIPS

Responsible for: Information Security

Internal Relationships: All Shire of Dardanup employees, Elected Members and other contracted Local Governments.

External Relationships: Federal and State government agencies, other local government authorities, community groups and organisations, private sector stakeholders.

POSITION DIMENSIONS

Work Location: Eaton Administration Centre.

Delegated Authority: As defined by the Chief Executive Officer. Authority to sign purchase orders for supplies and services under delegated authority.

Driving Requirements: C (Car) or CA (Car Automatic) class motor vehicle licence (preferable).

EXTENT OF AUTHORITY

This position operates under direction of the Deputy Chief Executive Officer, and in liaison with Manager Information Services within established guidelines, procedures and policies of Council as well as statutory provisions of the Local Government Act and other legislation. Regular communication with the Manager Information Services is required.

CORPORATE ACCOUNTABILITIES

- All employees are bound by the requirements of the Local Government Act 1995 to act with integrity, and in a way that shows a proper concern for the public interest;
- Comply with Council's Code of Conduct, management directives and approved policies and procedures.

CORPORATE ACCOUNTABILITIES

- Avoid participation in any activities that may represent a conflict of interest with Council transactions and your obligations.
- Maintain obligations described within the Shire of Dardanup’s Customer Service Charter.
- Comply with all requirements for capturing corporate information and understand that the Local Government is the owner of all Intellectual Property rights in all documents, materials or other things created or contributed to by the Employee in the course of their employment.
- Exercise discretion and maintain confidentiality in dealing with sensitive and high-level issues.
- Deliver effective use of Shire resources within the level of accountability for this position.
- Ensure your own safety and health at work by undertaking your work duties in a safe and proficient manner. Exercise your duty of care by having thought and regard for others by ensuring that you avoid adversely affecting, the safety or health of any other individual through any of your acts or omissions at work as per Council’s WHS policies and Work Health and Safety legislation.
- Employees shall cooperate with the Shire of Dardanup in the carrying out of the obligations imposed on the Shire under Work Health and Safety legislation.
- Provide an ongoing commitment to risk, emergency management and business continuity principles.
- Employees shall demonstrate the Shire’s Values “Trust, Respect, Accountability, Customer/Community, Excellence, Support” within the workplace.

VALUES

Our Values – TRACES

The Shire of Dardanup is building a culture where openness and transparency are the norm; and where we all hold ourselves accountable to deliver excellence for our customers and community.

T RUST	R ESPECT	A CCOUNTABILITY	C USTOMERS & COMMUNITY	E XCELLENCE	S UPPORT
	"We are committed to recognising and acknowledging each person's unique contribution."		"We are committed to providing a positive experience for our customers and our community."		"We are committed to being a true team."
"We are committed to showing confidence and belief in each other and ensuring we do what we say we will do."		"We are committed to transparency, good governance and accept responsibility for our actions."		"We are committed to being the best we can be within the organisation."	

SELECTION CRITERIA

Essential:

1. Tertiary qualifications in Cyber Security or a related discipline and/or professional certification such as CISSP or CISM.
2. Knowledge of on premises and public cloud infrastructure and security implications including deploying products in the cloud.
3. An understanding of security frameworks such as ISO27001, NIST, SANS.
4. An understanding of common security practices such as attack surface analysis, OWASP, vulnerability scanning, SEIM, SOAR.
5. An understanding of risk management frameworks such as ISO31000
6. Good communication and report writing skills
7. Proven organisational ability with the capacity to work unsupervised, manage priorities and meet deadlines under pressure.
8. Proven experience in user education, training and support within a team environment.

Desirable:

1. Experience in the management of server & virtual environments, backup and restoration, networking (switch/router), data classification, data loss prevention, firewalls, IDS/IPS and identity management.
2. Knowledge of security requirements across the software development lifecycle.
3. Audit and Incident response and undertaking technical investigations/analysis.
4. Knowledge of or experience working in Local Government.