# POSITION DESCRIPTION

| | | | |
|---|---|---|---|
| **Position Title** | Cyber Security & Compliance Specialist | **Classification** | Band 8 |
| **Directorate** | Corporate Services | **Department** | Transformation & Technology |
| **Direct Reports** | Nil | **Date** | June 2026 |
| **Reports to** | Coordinator IT Operations & Cyber | | |

## ORGANISATIONAL CONTEXT

Cardinia Shire Council is committed to building a sustainable shire for present and future generations to enjoy. Council plays an important role in supporting the community by delivering a wide range of services that enhance the wellbeing of residents now and into the future.

To support the delivery of these services, Council is focused on building a skilled and professional workforce with the capability to respond to current priorities and future challenges. Employees are expected to contribute to high-quality service delivery, demonstrate sound professional judgement, and work collaboratively to achieve positive outcomes for the community.

Council is committed to providing a safe, inclusive and supportive working environment that enables employees to perform at their best while contributing to the achievement of Council's strategic objectives.

### POSITION OBJECTIVES

The Cyber Security & Compliance Specialist is responsible for strengthening Council's cybersecurity posture by leading the uplift, implementation and assurance of cybersecurity controls, risk management practices and compliance obligations across Council's technology environment.

The role provides specialist input into the direction of Council's cybersecurity capability, combining strategic advice with hands-on delivery of complex operational and compliance outcomes. It also provides authoritative advice across Council services to support informed, risk-based decision making, regulatory compliance, audit readiness and alignment with governance requirement.

The position contributes to emerging technology governance, including artificial intelligence (AI), by supporting the development, implementation and monitoring of controls aligned to recognised standards such as ISO/IEC 42001.

### KEY RESPONSIBILITIES AND DUTIES

Key responsibilities include, but are not limited to:

- Lead the implementation, uplift and ongoing assurance of cybersecurity controls aligned to the Essential Eight and recognised industry frameworks.
- Oversee Managed Security Service Provider and Security Operations Centre outputs, ensuring alerts, reports and recommendations are reviewed, prioritised and translated into actionable outcomes.
- Lead vulnerability management, patch compliance and configuration compliance activities, including prioritisation, reporting, escalation and coordination of remediation actions
- Coordinate cybersecurity incident response and remediation actions, providing specialist guidance to ensure incidents are assessed, escalated, contained and resolved in accordance with Council procedures
- Lead compliance activities including audits and evidence preparation.
- Develop and maintain policies and security documentation.
- Lead vendor and third-party security risk assessments, providing recommendations to manage cyber, data protection and compliance risks associated with external provider.
- Lead the tracking, reporting, and coordination of cybersecurity risk mitigation activities, providing visibility and advice on risk posture and priorities.
- Provide subject matter expert advice to major technology and business projects, including ERP initiatives, to ensure cybersecurity, compliance and risk considerations are incorporated into planning, design and implementation.
- Identify and drive automation, reporting and continuous improvement opportunities to strengthen control effectiveness, operational efficiency and visibility of cybersecurity risks.
- Contribute to AI governance aligned to ISO/IEC 42001.
- Provide functional technical leadership, guidance and mentoring to IT staff to uplift cybersecurity capability, accountability and consistent security practices.

## POLICY AND PROCEDURE COMPLIANCE

- Adhere to (and promote) HR, IT, OH&S/Risk Management policies, procedures and practices.
- Demonstrate understanding and accountability for record keeping policy including the accuracy and capture of data, the sensitivities involved and the release and destruction of documents.

## OCCUPATIONAL HEALTH & SAFETY RESPONSIBILITIES

- Take reasonable care for the health and safety of yourself and others in the workplace, ensuring we provide and maintain a working environment that is safe and without risk to the health of employees, contractors, visitors and the general public, as far as is reasonably practicable.
- Ensure all legislative and regulatory responsibilities are addressed and met in relation to occupational health and safety.
- Responsible for ongoing consultation with employees, employee health and safety representatives and supervisors to identify and eliminate hazards and risks in the workplace.
- Ensure hazards, incidents, near misses and injuries are reported immediately and recorded within the appropriate system.
- Actively participate in the planning and execution of Return-to-Work plans as required.

## ACCOUNTABILITY AND EXTENT OF AUTHORITY

- Deliver a positive internal and external customer experience focussed on the employee lifecycle.
- Provide leadership, specialist advice, direction and expertise on policy, goals and projects to employees, leaders and key stakeholders to support the achievement of the Council Plan and organisational strategy and goals.
  Operate with a high degree of autonomy, influencing practices across teams and providing specialist advice to support risk-based decision making.

## JUDGMENT AND DECISION MAKING

- Operate in a specialised environment with limited day-to-day management.
- Involves both problem solving and policy development.
- Methods, procedures and processes are less well-defined, and employees are expected to contribute to their development and adaptation

- Requires identification and analysis of an unspecified range of options before choice can be made.
- Identify and develop policy options for senior management or employer consideration.
- Exercises independent judgement in risk prioritisation, incident response, and control implementation.
- Work involves the application of improvement suggestions, recommendations and problem solving
- Solve complex and high-risk problems.

**SPECIALIST KNOWLEDGE AND SKILLS**

- Strong cybersecurity operations, compliance frameworks, Microsoft security stack, and AI governance awareness.
- An understanding is required of the long-term goals of the wider organisation and of its values and aspirations and of the legal and socio-economic and political context in which it operates.
- Ability to translate risks into practical actions and implement automation improvements.
- Demonstrated ability to implement and sustain security and compliance improvements across operational teams
- Demonstrate initiative in managing work outcomes, opportunities and challenges.
- Demonstrate specialised analytical and problem-solving skills.

**INTERPERSONAL SKILLS**

- Ability to persuade, convince or negotiate with clients, members of the public, employees, tribunals etc. and persons in other organisations in the pursuit and achievement of specific and set objectives.
- Ability to lead, motivate and develop other employees
- Demonstrate self-awareness and a commitment to personal growth.
- Display resilience and agility in a changing work environment.
- Possess excellent communication, negotiation, and interpersonal skills with the ability to clearly articulate and present information as required.
- Ability to manage a variety of tasks and issues concurrently.
- Proven ability to build and maintain productive and respectful relationships and partnerships.
- Ability to work effectively as part of a to deliver positive organisational outcomes.
- Proven ability to maintain high levels of confidentiality.

**MANAGEMENT SKILLS**

- Ability to effectively coach and support employees throughout the organisation.
- Be proactive and prioritise activities according to level of urgency with the ability to achieve objectives despite conflicting pressures.
- Ability to make independent decisions, good judgement and work with autonomy, initiative, and minimum supervision.
- Promote a culture of learning by proactively seeking opportunities to challenge and develop team members and provides practical feedback to maximise performance.
- Support high performance through regular coaching with peers, and role modelling shared leadership.
- Ability to manage own time, set priorities and achieve targets within allocated budgets and resourcing.
- Influence a collaborative and innovative values-based culture.
- Foster innovation and improves work practises and processes.

**QUALIFICATIONS AND EXPERIENCE**

- Relevant tertiary qualification in Information Technology, Cybersecurity or a related discipline, or equivalent practical experience.
- Demonstrated experience in cybersecurity operations, risk, and compliance within a complex environment.
- Experience supporting audits and managing compliance activities across recognised frameworks.

- Experience working with managed security service providers and external vendors.
- Experience mentoring or guiding technical staff to uplift capability and accountability.
- Strong data analysis and reporting capability.
- Experience working in a complex, multi-disciplinary organisation.
- A current Victorian Driver Licence.

**KEY SELECTION CRITERIA**

- Demonstrated ability to deliver cybersecurity and compliance outcomes within a complex organisational environment, including vulnerability management, patching, incident response, and audit readiness.
- Strong analytical and problem-solving capability, with the ability to assess risk, prioritise remediation activities, and deliver practical, outcome-focused solutions.
- Ability to operate independently and exercise sound judgement in managing cybersecurity operations and compliance obligations with minimal supervision.
- Demonstrated experience implementing or uplifting controls aligned to recognised frameworks (e.g. Essential Eight, ISO 27001, NIST or CIS).
- Strong communication, negotiation and stakeholder engagement skills, with the ability to influence outcomes across technical teams and business units without direct authority.
- Proven experience working with external providers (e.g. MSSP, vendors, auditors) to achieve measurable security and compliance outcomes.
- Ability to translate complex security and compliance requirements into practical, implementable actions across IT teams.
- Demonstrated ability to uplift capability within a team environment through knowledge sharing, mentoring, and driving accountability for security practices.
- Understanding of emerging cybersecurity and technology risks, including AI governance, data protection, and regulatory compliance obligations relevant to local government.
- Ability to identify opportunities for automation and continuous improvement to enhance efficiency, visibility, and control effectiveness.

## CONDITIONS OF EMPLOYMENT

Terms and conditions of employment are in accordance with the Cardinia Shire Council Enterprise Agreement 2024 and Cardinia's policies and procedures.

| | |
|---|---|
| Tenure | This is a full time ongoing position |
| Pre-employment checks | All appointments are subject to a National Police Record Check, pre-employment medical check, and a six-month probationary period (new employees only). Certain positions may also require a Financial Background Check, Traffic Check or Working with Children Check. |