POSITION DESCRIPTION

POSITION TITLE:	**Security Analyst**
DIVISION:	**Organisational Performance**
DEPARTMENT:	**Information Technology**
SECTION:	**Cyber and Information Security**
CLASSIFICATION:	**Band 5**

POSITION OBJECTIVES:

The Security Analyst plays a crucial role in monitors, investigates, and responds to cybersecurity threats to protect the Council's information systems and data integrity.

Reporting to the Security Operations Lead, responsible for ensuring the security and integrity of Hume's information systems and assets, protecting Hume from cyber threats and maintaining compliance with relevant legislations.

The key objectives of the position are:

- Uplifting Councils security posture to align to best practice and ensure policies, process and controls are effectively maintained to promote security hygiene.
- Identifying areas for improvement and implementing new security measures and technologies.
- Ensuring continuous monitoring of vulnerabilities and security alerts whilst managing security tools and technologies to detect and respond to threats and risks promptly.
- Manage the effective cyber incident response and recovery efforts aligned to process, policy and best practice.
- Overseeing the independent assessment of security controls throughout Council to ensure ongoing compliance and improvement opportunities.

KEY RESPONSIBILITIES AND DUTIES:

Cyber Strategy and Governance:
Information Security - Defining and operating a framework of security controls and security management strategies:

- Provide advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
- Contribute to development of information security policy, standards and guidelines.
- Obtain and act on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigate major breaches of security and recommend appropriate control improvements.
- Develop new architectures that mitigate the risks posed by new technologies and business practices.

Cyber Security Resilience:
Security Operations - Delivering management, technical and administrative services to implement security controls and security management strategies:

- Maintains operational security processes and checks that all requests for support are dealt with according to agreed procedures.
- Provides advice on defining access rights and the application and operation of elementary physical, procedural and technical security controls.
- Investigates security breaches in accordance with established procedures and recommends required actions. Provides support and checks that corrective actions are implemented.

Threat Intelligence - Developing and sharing actionable insights on current and potential security threats to the success or integrity of an organisation:

- Collates and analyses information for threat intelligence requirements from a variety of sources.
- Contributes to reviewing, ranking and categorising qualitative threat intelligence information.
- Creates threat intelligence reports.
- Evaluates the value, usefulness and impact of threat intelligence sources.

Cyber Incident Management:
Incident Management - Coordinating responses to incident reports, minimising negative impacts and restoring service:

- Ensures that incidents are handled according to agreed procedures.
- Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents.
- Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents.
- Contributes to testing and improving incident management procedures.

Digital forensics - Recovering and investigating material found in digital devices:

- Applies standard forensic tools and techniques to examine digital devices.
- Recovers and analyses damaged, deleted or hidden data from various digital sources and devices.

- Maintains the integrity of digital evidence and ensures its collection adheres to legal admissibility standards.

Vulnerability Management:
Vulnerability assessment - Identifying and classifying security vulnerabilities in networks, systems and applications and mitigating or eliminating their impact:

- Collates and analyses catalogues of information and technology assets for vulnerability assessment.
- Performs vulnerability assessments and business impact analysis for medium complexity information systems.
- Contributes to selection and deployment of vulnerability assessment tools and techniques.

Secure software and systems assurance:
Information assurance - Protecting against and managing risks related to the use, storage and transmission of data and information systems:

- Performs technical assessments and/or accreditation of complex or higher-risk information systems.
- Identifies risk mitigation measures required in addition to the standard organisation or domain measures.
- Establishes the requirement for accreditation evidence from delivery partners and communicates accreditation requirements to stakeholders.
- Contributes to planning and organisation of information assurance and accreditation activities. Contributes to development of and implementation of information assurance processes.

Penetration testing - Testing the effectiveness of security controls by emulating the tools and techniques of likely attackers:

- Selects appropriate testing approach using in-depth technical analysis of risks and typical vulnerabilities.
- Produces test scripts, materials and test packs and tests new and existing networks, systems or applications. Provides advice on penetration testing to support others.
- Records and analyses actions and results and modifies tests if necessary.
- Provides reports on progress, anomalies, risks and issues associated with the overall project.

ORGANISATIONAL RELATIONSHIPS:	
Reports to:	Security Operations Lead
Supervises:	NIL
Internal Contacts:	ICT Team, End Users
External Contacts:	Partners and Auditors

ORGANISATIONAL CONTEXT

VISION

Hume City Council will be recognised as a leader in achieving social, environmental and economic outcomes with a common goal of connecting our proud community and celebrating the diversity of Hume.

MISSION

To enhance the social, economic and environmental prosperity of our community through vision, leadership, excellence and inclusion.

OUR VALUES

At Hume City Council, our Values underpin everything that we do.

WORK HEALTH & SAFETY (WHS)

Employees are required to participate in the WHS process by:

- Following established safe working instructions, procedures and policies.
- Taking reasonable care for their own Work Health and Safety and that of others.
- Seeking assistance when unsure of practices, procedures and policies to perform a task.
- Reporting all incidents, injuries, near misses, damage to property and hazards as soon as practicable to their supervisor and the WHS Team.
- Actively participating and contributing to inspections, audits, team meetings and training.
- Ensure that relevant WHS legislation is complied with.

RISK MANAGEMENT

Contribute to a positive risk management culture by complying with the *Risk Management Policy*, assisting with the implementation of the Risk Management Strategy and reporting risk management concerns and improvements to their supervisors and/or managers.

Manage risks in area of responsibility by complying with the WHS Policy and Processes and implementing appropriate risk management strategies.

Demonstrate Council's commitment to implementing best practice risk management processes.

STATEMENT OF COMMITMENT TO CHILD SAFE STANDARDS

Hume City Council is a child safe organisation with zero tolerance for child abuse. Council adheres to the Victorian Child Safe Standards and related legislation and Council acknowledges the cultural safety, participation and empowerment of all children, especially children from Aboriginal and Torres Strait Islander, or culturally and/or linguistically diverse backgrounds and those with a disability. As such, all staff must ensure that their behaviours and actions are consistent with these standards.

SERVICE PLANNING & CONTINUOUS IMPROVEMENT

It is a requirement of the Service Performance Principles of the *Local Government Act 2020* for Councils to continuously improve service delivery and service performance. Managers and Coordinators are responsible for undertaking service planning and continuous improvement in their area/s of responsibility and ensuring implementation of service plan actions in accordance with Council's Service Planning Framework.

ASSET MANAGEMENT

Staff are responsible for undertaking Asset Management functions in accordance with Council's Asset Management Policy to ensure Council assets continue to be appropriately managed and maintained.

ENVIRONMENTAL SUSTAINABILITY

Hume City Council has a strong and enduring commitment to environmental sustainability and prides itself on its leadership on a range of environmental issues. Council's Waste & Sustainable team and Climate Action Integration team lead Council activities in this area, however all Council departments have a direct responsibility for implementing

environmental sustainability actions across all Council operations and services to the community.

Council's *Live Green Work Green* employee behaviour change program encourages staff participation in reducing the environmental impact of Council operations. Staff are encouraged to join the environmental leadership team, the *Green Team*, which guides action in this area.

POLICE CHECK:
The incumbent must have and maintain a current Police Check

WORKING WITH CHILDREN CHECK: The incumbent must have and maintain a current Working with Children Check ☐ YES ☒ NO

PRE-EMPLOYMENT MEDICAL CHECK

- The incumbent must undergo a Pre-Employment Medical Check (including fitness for work and functional capacity assessments, muscular-skeletal screening and drug & alcohol test. May also include cognitive assessment.) ☐ YES ☒ NO
- The incumbent must undergo a Pre-Employment Audio Test ☐ YES ☒ NO

PSYCHOMETRIC ASSESSMENT
The incumbent must undergo a series of psychometric assessments (Psychometric testing can take various forms, such as numerical, mechanical, logical, verbal, or skills tests) to ensure suitability for the position ☐ YES ☒ NO

OTHER DUTIES
Responsibilities and duties included in this position description are subject to the *Multi-skilling* provisions of the *Hume City Council Enterprise Agreement* as varied from time to time.

ACCOUNTABILITY AND EXTENT OF AUTHORITY:

The incumbent is responsible and accountable for:

- Accountable for the quality, effectiveness, cost and timelines of the programs, projects or work plans under their control and for the safety and security of the assets being managed.
- Provide direct support and assistance to more senior employees, the freedom to act is not limited simply by standards and procedures, and the quality of decisions and actions taken will often have an impact upon the performance of the employees being supported.
- Perform a variety of tasks using a range of security skills.
- Work is carried out under routine supervision, either individually or as part of a team.
- Display and promote Hume Values & Guiding Behaviours.
- Compliance with all Council's policies, procedures and guidelines.
- Respond to critical and major security incidents that occur outside of standard business hours, with a rotating roster requiring the employee to be accessible via phone or email to provide immediate support and incident response.

JUDGEMENT AND DECISION MAKING:

The incumbent is accountable for:

- Works are well defined but the method, technology, process, or equipment to be used must be selected from a range of available alternatives.
- Guidance and counsel may be available within the time available to make a choice.
- Implement and executes policies aligned to Cyber strategic plans.
- Perform an extensive range and variety of complex technical and/or professional work and security deployment activities.

- Undertake work which requires the application of fundamental principles in a wide and often unpredictable range of contexts.
- Engage and coordinate with subject matter experts to resolve complex issues as they relate to customer/organisational requirements.
- Understand the relationships between own specialism and customer/ organisational requirements.

SPECIALIST KNOWLEDGE AND SKILLS:

The following knowledge and skills are required to be utilised:

- Thorough understanding of the relevant technology, procedures and processes used within their operating unit.
- Understanding of the role and function of the senior employees to which they provide support, an understanding of the long-term goals of the unit in which they work, and an appreciation of the long-term goals of the wider organisation.
- Understanding of the function of the position within its organisational context, including relevant policies, regulations and precedents.
- May provide guidance and on-the-job training to other employees where required
- Knowledge of risk assessment methodologies, risk mitigation strategies, and risk monitoring techniques.
- Knowledge of corporate governance principles, best practices and internal control frameworks.
- Ability to analyse complex data, identify trends, and assess Cyber risks.
- meticulous attention to detail in reviewing policies, procedures, and audit findings.
- Ability to adapt to changing regulatory requirements and technological advancements.

MANAGEMENT SKILLS:

The following management skills are required:

- Managing time, setting priorities, and planning and organising one's own work and that of supervised employees to achieve specific and set objectives in the most efficient way possible within the resources available and within a set timetable.
- Understanding of and ability to implement basic personnel policies and practices including those related to equal employment opportunity, occupational health and safety and employees training and development.

INTERPERSONAL SKILLS:

The following interpersonal skills are required to be demonstrated:

- Ability to gain co-operation and assistance from clients, members of the public and other employees in the administration of defined activities and in the supervision of other employees or groups of employees.
- Expected to write reports in their field of expertise and to prepare external correspondence of a routine nature.
- Require skills in oral and written communication with clients, other employees and members of the public and in the resolution of minor problems.
- Communicate complex regulatory and risk-related information to both technical and non-technical audiences.
- Work with various departments to facilitate productive discussions regarding security operations matters.

- Liaise with stakeholders to support the adoption of security and compliance measures.

QUALIFICATIONS AND EXPERIENCE:

The following knowledge and skills are required to be utilised:

- Completion of a degree or diploma course with little or no relevant work experience, or through lesser formal qualifications with relevant work skills, or through relevant experience and work skills commensurate with the requirements of work in this Band.
- Proven experience as a security operations or similar role, preferably within government or enterprise environments.
- Strong understanding of information security principles with demonstrated success.
- Analytical and problem-solving skills with a keen attention to detail.
- Exceptional communication and interpersonal skills with the ability to collaborate effectively with cross-functional teams and stakeholders.
- Diverse Cyber background with knowledge across a broad range of technologies, including and not limited to:
    - Identity management (EntraID)
    - Endpoint detection and Response (Trend and Microsoft Defender)
    - SecOps & GRC (ISO 27001, E8, PCI DSS and VDPSF)
    - Vulnerability management (Rapid7)
    - URL Filtering (Cisco Secure Access)
    - Email Security (Abnormal)
    - DNS Security (SPF, DKIM, DMARC)
    - System Security (Microsoft Server and Endpoint)
    - Database Security (SQL Server)
    - Cryptography and PKI (Microsoft Certificate Authority)
    - Network Security (Fortinet, Cisco & Meraki)
    - Cloud Platforms (M365, Azure)
    - SaaS application, RBAC and Integration Security concepts (TechnologyOne)

TASK ANALYSIS

In undertaking the inherent requirements of their duties, a person in this position may be expected to work in or be exposed to the following conditions or activities as marked.

Condition/Activity	Constant	Frequent	Occasional	N/A
Manual handling weights – above 10kgs	☐	☐	☒	☒
– below 10kgs	☐	☐	☒	☐
Manual handling frequency	☐	☐	☐	☒
Repetitive manual work	☐	☐	☐	☒
Repetitive bending/twisting	☐	☐	☐	☒
Repetitive kneeling/squatting	☐	☐	☐	☒
Working with arms above head	☐	☐	☐	☒
Lifting above shoulder height	☐	☐	☐	☒
Using hand tools – vibration/powered	☐	☐	☐	☒
Operating precision machinery	☐	☐	☐	☒
Close inspection work	☐	☐	☐	☒
Wearing hearing protection	☐	☐	☐	☒
Wearing eye protection	☐	☐	☐	☒
Wearing safety shoes/boots (steel cap) / gum boots	☐	☐	☐	☒
Wearing other relevant PPE	☐	☐	☐	☒
Working in dusty conditions	☐	☐	☐	☒
Working in wet/slippery conditions	☐	☐	☐	☒
Working with chemicals/solvents/detergents	☐	☐	☐	☒
Washing hands with soap (hygiene)	☐	☐	☒	☐
Working at heights	☐	☐	☐	☒
Working in confined spaces	☐	☐	☐	☒
Working in chillers (+4 degrees C)	☐	☐	☐	☒
Performing clerical duties	☒	☐	☐	☐
Working on a keyboard	☒	☐	☐	☐
Driving cars and/or trucks	☐	☐	☒	☐
Other (Sitting for long periods)	☒	☐	☐	☐

VARIATION TO CONDITIONS OF EMPLOYMENT:

These conditions of employment, your duties and your location may be varied by Council during the term of your employment.

The key responsibilities and duties in this position description are to be undertaken in accordance with the General Employee Handbook.

AGREEMENT:

I hereby accept and agree that by placing my electronic signature in the text box, this shall be considered as an original signature for accepting the duties in this position description. I understand that key responsibilities and duties in this position description will be undertaken in accordance with the Employee Handbook and I agree to abide by the terms and conditions stipulated therein.

Name (Please print):	
Signature:	Date:

SELECTION CRITERIA:

Selection will be based on the following selection criteria; however, reference will also be made to other listed skills, knowledge and attributes as required in the position description:

1. Degree or Graduate Diploma in cyber security or similar field with relevant experience in Information Security.
2. Understanding of security principles, practices, and technologies.
3. Experience, qualifications and dedication to the Cyber Security and knowledge of IT governance, cybersecurity, risk and compliance requirements in ICT.
4. Proficiency in various security tools and frameworks, such as SIEM, firewall, vulnerability management, threat intelligence and incident response.
5. Ability to influence stakeholders at all levels that drives the success of security projects and objectives.
6. Familiarity with regulations and standards specific to the Local Government and Victorian Government security industry would be highly beneficial.
7. Understanding of IT risk management principles and the ability to assess and prioritise cybersecurity risks in the context of asset and data protection.
8. Strong commercial acumen to engage and manage third party vendors to deliver efficient and effective services to the organisation.