Position Description

Position Title:	Cyber Security Lead
Classification:	Band 8
Business Unit:	Digital and Technology Service
Reports to:	Coordinator Information Governance and Cyber Security
Status:	Full-time
Approved by:	Director, Customer and Corporate Affairs
Reviewed:	April 2024

1. About the City of Glen Eira

The City of Glen Eira is located in Melbourne's south-east suburbs, approximately 10 kilometres from Melbourne's central business district. The City includes the suburbs of Bentleigh, Bentleigh East, Carnegie, Caulfield, Caulfield East, Caulfield North, Caulfield South, Elsternwick, Gardenvale, Glen Huntly, McKinnon, Murrumbeena, Ormond and part of the suburbs of Brighton East and St Kilda East.

Glen Eira has a vibrant and diverse community which is proud of its cultural heritage. It has 68 beautiful parks, 45 sporting ovals, 40 educational institutions, 35 strip shopping centres and almost 6000 businesses. It is home to more than 141,000 people and significant Melbourne icons such as Ripponlea, the Caulfield Cup, Yarra Yarra Golf Club, the Jewish Holocaust museum and much more.

2. About our Organisation

Glen Eira City Council aims to be an organisation that is high performing, values based and one that strives for innovation. We are proud of our achievements and have been recognised as an employer of choice over recent years. We endeavor to recruit people who share our values, are proud of the work they do and have a desire to make a difference to our community.

Glen Eira City Council is committed to reconciliation and supports Aboriginal and Torres Strait Islander aspirations. We encourage applications from Aboriginal and Torres Strait Islander people and value the knowledge, skills and talents they could share with our workforce and community.

Glen Eira City Council plays a leading role in taking strong action on the climate emergency and raising awareness to ensure a sustainable, safe and healthy future for us all. To help us achieve these outcomes, we all have the responsibility to embed climate change action in everything we do. This includes reviewing individual work to identify how we can make a difference in Council and the community to reduce environmental impacts and raise awareness.

<u>Values</u>

We are committed to the values which underpin our organisational culture, and how we work. Our five values are:

- Service Excellence – *Delivering for our community*
- Collaboration – *Working better together*
- Innovation – *Expressing ideas and adding value*
- Respect – *Being understanding and considerate*
- Integrity – *Being open and honest*

Organisational Structure

Glen Eira City Council's structure comprises four Directorates and two executive management portfolios (People and Culture and Finance) all reporting to the Chief Executive Officer. The four Directorates are:

- Sustainability, Assets and Leisure;
- Customer and Corporate Affairs;
- Planning and Place;
- Community Wellbeing
-

These Directorates and the departments within them are responsible for ensuring the delivery of high quality and cost-effective services that make a difference to our community. In conducting their business, they aim to be client focused and open to innovation and continuous improvement.

3. Position Purpose and Background

The Cyber Security Lead will build and maintain the Glen Eira City Council Information Cyber Security Program with a primary focus on the IT Cyber Security infrastructure, platforms, and policies. This includes the administration and future design of the Glen Eira network with a strong focus on Cyber Security and service continuity, ensuring the smooth operation of Council data and voice networks providing maximum security, performance, and system availability.

4. Working Relationships

Internal:

- Chief Information Officer
- Coordinator Information Governance and Cyber Security
- Coordinator Workplace Technology
- Digital and Technology Services Staff
- All Council Staff

External:

- Department of Premier and Cabinet and other relevant Government departments
- Industry experts
- Vendors
- External Service providers

5. Key Responsibilities

- Provide high level and in-depth cyber security advice, training, and assistance to a range of stakeholders across Glen Eira Council.
- Identify whether the appropriate Cyber Security controls are in place and assess the control effectiveness, gathering appropriate evidence to meet regulatory requirements.
- Work with the Digital and Technology team to manage Cyber Security incidents effectively through continuous improvement in the prevention, reaction, detection, and response controls.
- Develop controls that are aligned to the Glen Eira Council's framework and based on selected industry frameworks (e.g. ISO27001/2, NIST CSF) and relevant compliance requirements (e.g. PCI-DSS, CPS 234, VPDSS).
- Process definition and management in the design of new controls, retirement of expired controls and integration into management controls.
- Lead Cyber Security control maturity assessments periodically to identify control deficiencies and coordinate remedial works with controls owners.
- Ensure controls are assessed for operational efficiency by implementing measures such as Key Control Indicators (KCI) and Key Performance Indicators (KPI).
- Develop threat models and security risk assessments, and recommend mitigations and countermeasures to address risks, vulnerabilities, and threats.
- Test and evaluate Cyber Security software and systems to eliminate problems and submit recommendations for improvements.

- Analyse information collected from the monitoring system and network security risks and current posture as well as network stability and usage.
- Review and validate security documentation, including the system security requirements definition and system security plans. Perform audit and security compliance checks, including network penetration testing, vulnerability scans, and other analysis work.
- Ensure the ongoing development of Cyber Security awareness, training programs and resources.
- This role may also be required to carry out other such duties as are within the limits of the employee's skills competence and training.

5.1 OHS, Risk Management, Equal Opportunity, Charter of Human Rights & Child Safe Standards

- Adhere to policies and procedures to minimise injury and damage to assets and property.
- Adhere to Council's Health and Safety, equal opportunity and risk management policies, plans and procedures and relevant legislation as well as act in accordance with the Charter of Human Rights.
- Actively participate in reporting matters of health, safety and Council asset damage.
- Demonstrate and promote workplace behaviour that does not discriminate, bully or harass.
- Take reasonable care for your safety and the safety of others who may be affected by your actions or omissions;
- Contribute to the effective protection of Council in accordance with the Council's risk management policy and procedures;
- Act compatibly with human rights and consider human rights when making decisions; and
- Cooperate with any reasonable, lawful instruction to comply with relevant legal requirements
- Commit and adhere to Council's zero tolerance of child abuse, its principles of being a child safe organisation and its reporting requirements for child safety.
- Adhere to the Victorian Child Safe Standards and related legislation, including Failure to Disclose, Failure to Protect and Grooming offences.

5.2 Accountability and Extent of Authority

The following outlines the Accountability and Extent of Authority required by the Cyber Security Lead:

- The role provides specialist advice and service to the organisation through support requirements with a primary focus on maintaining the IT facilities and associated security infrastructure.
- Acts within relevant legislation, Council policies, procedures, and best practice technical processes.
- Accountable for the quality, effectiveness, cost and timeliness of the programs, projects or work plans within area of responsibility and for the safety and security of the assets being managed.
- Follow established procedures to ensure the ongoing availability and integrity of Council's Network Security.
- Maintaining confidentiality of Council information.
- Provide input into the development of policies within IT.

- Freedom to act is wide and limited only to the areas nominated in this position description. The advice and counsel provided by this position is relied upon heavily across the organisation. The implications of the decisions may have wide spread impact for the community as well as the organisation.

Judgement and Decision Making Skills

The following outlines the extent of judgement and decision making required by the Cyber Security Lead:

- Develop methods, procedures and policies that support operations of Council's Cyber Security that are based on best practice and applying specialist knowledge to identify and provide solutions on an unspecified range of problems.
- Problem solving may involve application of these techniques to new situations and the identification of an unspecified range of options before a recommendation can be made.

5.3 Management Skills

The following describes managerial skills required by the Cyber Security Lead:

- Plan and organise tasks to meet set timeframes.
- Demonstrated high degree of multi-tasking, teamwork, and prioritisation with a confident, positive, and professional manner.
- The ability to apply skills in managing time, setting priorities, and planning and organising own and other's work within the resources available and within a set timeframe despite conflicting priorities.
- Management and leadership skills are required to achieve objectives and goals, successfully negotiating balanced and positive net outcomes while taking account of sometimes competing business unit priorities Initiate and lead improvements to technical support systems.
- Lead and contribute to the long-term goals of the organisation particularly regarding the use of relevant industry standard and contemporary Information Technology.

5.4 Interpersonal Skills

The following describes the interpersonal skills required by the Cyber Security Lead:

- Well-developed communication skills, both verbal and written with the ability influence stakeholders.
- This role has the ability to influence and negotiate with clients, members of the public, other employees, stakeholders and persons in other organisations in the pursuit and achievement of specific set objectives as set out by the CIO.
- Ability to lead, motivate and develop team members and associated stakeholders where relevant Demonstrated experience working in collaboration with clients to better understand, anticipate and meet their needs combined with excellent customer service skills.
- Ability to advise, and develop capability across the wider Digital and Technology department, Executive and relevant Governance Committees.

5.6 Specialist Skills and Knowledge

The following describes the specialist knowledge and skills required by the Cyber Security Lead:

- Strong knowledge of security systems including but not limited to: Email Gateways, Multi-Factor Authentication, EDR, Firewalls and SIEM platforms.
- Substantial experience with Microsoft 365 security and Compliance management, Microsoft Defender and cloud-based infrastructure technologies such as Azure and AWS.
- Strong working knowledge of project management methodologies.
- Identify, develop and update policies, procedures, and practices from policies relevant to IT Security.
- Ability to apply expert knowledge and experience in Networks and Operating Systems. Strong working knowledge of the 'ASD Essential 8 Program'.
- High level analytical and investigative skills.
- Demonstrated financial acumen and experience managing budgets.

5.7 Qualifications and Experience:

- Tertiary qualifications in Computer Science or Cyber Security combined with significant relevant experience or lesser qualifications together with extensive and diverse experience or intensive specialist experience relevant to this role.
- Relevant industry certifications.
- Demonstrated experience in the implementation of cybersecurity frameworks, governance and reporting.

6. Performance Review

The Cyber Security Lead will be required to participate in the Council's Performance Development and Review process. This involves planning and agreeing work and skill development objectives, and reviewing and assessing achievements on a regular basis.

The Cyber Security Lead may also be required to carry out other such duties as are within the limits of the employee's skills, competence, and training. These will be discussed as part of the Performance Review process.

7. Selection Criteria

- Demonstrated commitment and adherence to organisational values and behaviours.
- Analytical and investigative skills and knowledge in a variety of applications and infrastructure including MS Windows Servers, Microsoft Active Directory, DNS, DHCP, NPS, Certificate (PKI), Group Policy, Exchange (Hybrid), Microsoft 365, VMware, HP switching, Palo Alto Firewalls and Rapid 7 SIEM monitoring and configuration.
- Demonstrated experience in applying risk management processes and procedures across a broad range of stakeholders in diverse and complex environments which are hosted in cloud, hybrid, and on-premises ICT systems.
- Demonstrated ability to analyse existing and future systems across an organisation and review security architectures and develop solutions that integrate information security requirements to proactively protect information.
- Experience in leading Computer Incident Response Team (CIRT) activities, including forensic analysis, threat hunting and review and assessment of security events and logs via cyber security /event management tools (SIEM).
- Well-developed understanding and ability to articulate the impacts changes will have on the monitoring, maintenance, and operation of Cyber Security Systems.

- Comprehensive understanding of security standards and frameworks such as Essential 8, ISO27001-2, NIST, VPDSS, PCI DSS, HIPAA and MITRE ATT&CK.

8. Other Information

- Position is subject to the satisfactory completion of Police Records Check and Employee Working with Children Check.
- Victorian Drivers Licence is desirable.
- The position is located at the Glen Eira Town Hall, however the incumbent may be required to travel to other Council offices from time to time.
- Glen Eira has embraced a hybrid work model which includes the ability to work from home part-time, subject to team and operational requirements.