Cyber Security Analyst

Role purpose

This role protects the Council's systems, data, and digital assets from cyber threats. The role identifies and manages security risks, develops and maintains security policies and response plans, and ensures compliance with relevant legislation. Working across the organisation, the analyst provides expert advice, monitors and responds to security incidents, and supports staff awareness to maintain a strong and proactive security culture.

Role overview

EA & Classification	Hobart City Council Enterprise Agreement 2024 (or its successor) Municipal Officer Level 5
Position Number	4595.01
Number of direct reports	0
Responsible for total staff	0
Delegations & Authority	Nil
Budget level	Nil
Network, Group, & Team	Corporate Services Network, Information and Technology Services Group
Immediate Manager	IT Operations Manager (9866)



Cyber Security Analyst

Role accountabilities Key result areas

Strategic

- Lead the identification, analysis, and mitigation of cyber security risks across Council systems and data.
- Lead organisation wide security initiatives wide security initiative-wide security initiative
- Develop, implement, and review cyber security policies, procedures, and controls to ensure compliance with relevant standards and legislation.
- Provide specialist guidance for enterprise risk management and conduct regular security audits, vulnerability assessments, and penetration testing of Council systems.
- Manage and maintain security tools and platforms (e.g., firewalls, SIEM, endpoint protection).
- Research and evaluate emerging threats, technologies, and regulatory changes, advising on their impact and required actions.
- Maintain up-to-date documentation of security architecture, controls, and incident response plans.
- Support continuous improvement by identifying and implementing enhancements to security processes and technologies.

Corporate

- Prepare reports and recommendations for management on cyber security posture, incidents, and improvement opportunities.
- Collaborate with Technology Group and broader Council to ensure security is embedded in projects, procurement, and change initiatives.
- Monitor security alerts and respond to incidents, conduct investigations and root cause analysis as required.
- Lead or participate in the response to cyber incidents, including coordination with external agencies and vendors as required.
- Provide expert advice for audit committees or governance committees and lead Council-wide security awareness strategy.

Group

- Provide specialist advice and support to Council staff on cyber security best practices, including training and awareness programs.

Leadership

- Supervise or mentor junior staff or contractors as required.

Professional Advice

Represent the Council in relevant forums, working groups, and external engagements on cyber security matters.

- Provide authoritative advice to senior leaders, managers, and project sponsors

WORKING TOGETHER TO MAKE HOBART A BETTER PLACE FOR THE COMMUNITY

- Undertake security impact assessments for major organisational initiatives

Behaviour Standards

- Actively demonstrate the expected behaviours described in the City of Hobart Capability Framework in accordance with the position of classification.

Work Health and Safety

- To take reasonable care that your acts or omissions do not adversely affect the health and safety of yourself or others in the workplace, to comply with any reasonable instructions given to you by the Council and to comply with the requirements of all WHS applicable policies and procedures.
- Ensure compliance with Work Health and Safety and Child and Youth Safety requirements at all times and follow prescribed reporting processes within the required timeframes.

NOTE: **Whilst the key functions and responsibilities for the role are set out above, the Council may direct an employee to carry out such duties or tasks as are within the limits of the employee's skill, competence, and training.**

WORKING TOGETHER TO MAKE HOBART A BETTER PLACE FOR THE COMMUNITY

Cyber Security Analyst

Selection criteria

Qualifications and licences

- Tertiary qualifications in Information Technology, Cyber Security, Computer Science, or a related discipline, along with equivalent industry experience.

Essential

1. Demonstrated experience in leading complex cyber initiatives, cyber security analysis, incident response, and risk management within a complex ICT environment.
2. Strong knowledge of security frameworks, standards, and legislation (e.g. ISO 27001, NIST, Essential Eight, Privacy Act).
3. Demonstrated experience coordinating and managing security incidents, conducting investigations and root-cause analysis, and leading organisation wide incident response activities, cause analysis, and leading organisation wide incident response activities.-cause analysis, and leading organisation-wide incident response activities.
4. Proven ability to conduct security audits, vulnerability assessments, and penetration testing.
5. Experience in developing, implementing, and maintaining security policies, procedures, and incident response plans.
6. Proficiency with security tools and platforms (e.g. SIEM, firewalls, endpoint protection, intrusion detection/prevention systems).
7. Excellent analytical, problem-solving, and investigative skills.
8. Strong written and verbal communication skills, including the ability to prepare reports and deliver training to non-technical audiences.
9. Ability to work independently and collaboratively, managing multiple priorities and deadlines.
10. Commitment to continuous improvement and professional development in the cyber security field.
11. Ability to self-reflect and demonstrate organisational value and behavioural standards.

Desirable

- Industry certifications such as CISSP, CISM, CISA, CEH, or equivalent.
- Experience in local government or the public sector.
- Knowledge of cloud security principles and experience with securing cloud environments (e.g. Microsoft 365, Azure, AWS).
- Experience with project management or leading cyber security initiatives.
- Familiarity with data protection, privacy impact assessments, and compliance requirements relevant to local government.
- Experience mentoring or supervising junior staff or contractors.
- Participation in cyber security forums, working groups, or professional networks.

WORKING TOGETHER TO MAKE HOBART A BETTER PLACE FOR THE COMMUNITY

Cyber Security Analyst

Pre-employment checks

1. National Police check
2. Pre-employment Medical Assessment – Low Risk.

Notes

- Regular checks of the validity and status of essential licences and registrations are undertaken during the term of employment.
- The employee is responsible for notifying any new criminal convictions during the course of their employment.

Our Values







People

We care about people – our community, customers, and colleagues

Focus & Direction

We have clear goas and plans to achieve sustainable social, environmental, and economic outcomes for the Hobart community.

Accountability

We work to high ethical and professional standards are accountable for delivering outcomes for our community.

Teamwork

We collaborate both within the organisation and with external stakeholders drawing on skills and expertise for the benefit of our community

Creativity & Innovation

We embrace new approaches and continuously improve to achieve better outcomes for our community.

WORKING TOGETHER TO MAKE HOBART A BETTER PLACE FOR THE COMMUNITY

City of HOBART