Department of Education

GOVERNMENT OF WESTERN AUSTRALIA

Job Description Form

Cyber Security Specialist - Operations

Position number	00045040
Agreement	Public Sector CSA Agreement 2022 or as replaced
Classification	Level 7
Reports to	Cyber Security Manager
Direct reports	Nil

Context

Education Business Services (EBS) is the key provider of professional business services and support for Western Australian public schools, statutory boards and divisions of the Department. These highly valued services are delivered through the areas of finance, information and communication technologies (ICT), and infrastructure. We continually strive to enhance the capability and responsiveness of our staff, systems and processes across the organisation to deliver high quality education.

We are committed to contemporary work practices and adhere to the following service delivery principles:
Responsive: We respond to and reflect the needs of our customers.
Flexible: We are flexible and understand that our customers are not all the same.
Transparent: We are clear and open about our services, processes and decision making.
Accountable: We hold ourselves to high standards and deliver on our commitments.
Collaborative: We work in partnership with our customers.

Delivery of Information and Communication Technology (ICT) services provides support for the Department's educational outcomes by developing initiatives and technical support strategies to ensure all 800 Western Australian public schools can be individual, distinctive and responsive to their local communities while still benefiting from being part of a system.

The ICT Operations and Customer Service Directorate is part of the ICT Division and is the primary entry point to ICT for any responses to operational issues, requests or problems customers of ICT may have. As the highest frequency contact point for customers in many respects it is the 'face' of ICT.

The ICT Cyber Security, Security Operations Centre (SOC) supports the Department with the ongoing development, implementation and maintenance of information systems risk and security controls to protect the assets of the Western Australian Department of Education. In an environment of constraint, ensures that resources including financial, physical, technological and information requirements are efficiently applied to maintain a high level of products/service delivery.

Visit education.wa.edu.au to find out more information about the Department of Education.

Key responsibilities

Specialist Services

- Manage the daily operation of the Department's SOC, which performs security event and incident monitoring and response.
- Perform threat identification, management, and modelling, as well as enhance the alerting and monitoring of Department services and applications.
- Develop and maintain whole of Department threat intelligence capabilities, validate incident findings and clearly communicate identified control gaps and detected adversary activity to the appropriate teams.
- Coordinate the SOC in the performance of incident identification, assessment, quantification, reporting, communication, mitigation and monitoring tasks.
- Is responsible for leading and motivating staff in the development and achievement of the SOC business goals.
- Provide proactive, timely advice to the Cyber Security Manager and stakeholders in relation to cyber security threats, incidents and mitigations.
- Perform threat management and threat modelling, identify threat vectors and develop use cases for security monitoring.
- Manage the daily operations and actively work to enhance the Department's Security Information and Event Management (SIEM) and associated systems.
- Is responsible for integration of standard and non-standard logs into the SIEM system, using cost effective, appropriate, high value sources.
- Maintain a current working knowledge of the artefacts relevant in attack scenarios and how to obtain relevant evidence.
- Provide support to the Cyber Security Manager in the management of cyber security incidents, including incident coordination and response, conducting investigations, providing recommendations, and assisting in implementing mitigation measures.
- Revise and develop processes to strengthen the Security Operations Framework, review policies and highlight the challenges in managing Service Level Agreements (SLAs).
- Continuously update risk assessment methodologies to align with evolving cyber security landscape.

Branch Support

- Work within corporate policies and procedures, act with integrity and demonstrate ethical behaviours aligned with the Department Code of Conduct.
- Contribute to the uplift of the Department's cyber security posture and awareness.
- Ensure compliance to SLAs, process adherence and process improvement to achieve operational objectives.
- Within the Branch, promote a culture supportive of innovation and continuous business process improvement.
- Take reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the *Work Health and Safety Act 2020*.

Client and Stakeholder Support and Liaison

- Build and maintain positive working relationships with key internal and external stakeholders to maintain business knowledge, understand prioritisations and effectively liaise, consult, negotiate and collaborate to achieve these.
- Communicate complex information in a clear, articulate and compelling manner to engage and influence internal and external stakeholders.
- Prepare reports, briefing notes and correspondence for internal and external stakeholders, where required.

- Contribute to the achievement of corporate objectives by ensuring that stakeholders are dealt with in a professional and timely manner.

Selection criteria

1. Demonstrated extensive experience and knowledge of information technology and cyber security, including principles, concepts and current trends with specific knowledge and experience relevant to large corporate or government environments using on-premises and cloud-based technologies.
2. Demonstrated experience in the operation and management of a Security Operations Centre.
3. Demonstrated experience managing a Microsoft Sentinel SIEM, ideally at enterprise scale.
4. Demonstrated experience with Cyber Threat Intelligence, Threat Hunting, Detection Engineering, Threat Intelligence Platforms and Security Incident Response.
5. High level knowledge of Australian Government policies and frameworks, in particular, the ACSC's Essentials Eight, NIST CSF and ASD's ISM.
6. Demonstrated high-level verbal and written communication and interpersonal skills with the ability to effectively liaise with key internal and external stakeholders at a senior level, and to build and maintain strong relationships.
7. Demonstrated strong work ethic and the ability to proactively manage own workload and tasks to deliver outcomes as part of a small, dynamic team.

Eligibility and training requirements

Employees will be required to:

- hold a tertiary qualification in information technology/cyber security, relevant industry qualifications or equivalent extensive experience
- consent to a Nationally Coordinated Criminal History Check and obtain a current Screening Clearance Number issued by the Department of Education's Screening Unit prior to commencement of employment
- complete the Department's induction program within 3 months of commencement
- complete any training specific to this role required by Departmental policy
- complete the Department's training in Accountable and Ethical Decision-Making within 6 months of appointment and every 3 years thereafter
- complete the Department's Aboriginal and Torres Strait Islander cultural awareness online course within 3 months of commencement.

Certification

The details contained in this document are an accurate statement of the responsibilities and other requirements of the position.

ENDORSED

Date 15 August 2024
Reference D24/0591050