

**Position Description**

 **Position Title:** Manager (Cybersecurity Operations)

 **Position Classification:** Level 9

 **Position Number:** 317968

 **Faculty/Office:** University IT

 **School/Division:** Cybersecurity and Technology Risk

 **Centre/Section:**

 **Supervisor Title:** Associate Director (Cyber Security ad Technology Risk)

 **Supervisor Position Number:** 317935

**Your Work Area**

UWA is making significant investments in the Information and Technology Services area to enable its strategic direction and goals. Information Security is one of these areas and is undergoing an uplift in capability and delivery of new services to align with the University’s risk strategy.

It is expected that the Cybersecurity unit will cover all aspects of the cyber security domain, from network security, platform security, security operations toolkit including monitoring/analytics solutions and vulnerability management solutions.

**Reporting structure**

Reports to: Associate Director (Cybersecurity and Technology Risk)

Direct reports: Analyst/Senior Analyst (Cybersecurity)

**Your role**

As the appointee, you will have a significant role in managing all operational and support activities associated with Information Security service delivery, including monitoring performance and incidents to agreed Service Levels. Your will also be responsible for identifying and implementing ways to continuously improve the way IT delivers Information Security services to the University as well as leading Security Awareness activities. You will undertake security assurance and consultative activities, ensuring that the appropriate security solutions are in place and working effectively to support information security, and that existing solutions comply with security standards and requirements.

**Your key responsibilities**

Manage and monitor security events and incidents, evaluating information security risks and performing assurance activities such vulnerability assessments then design reviews

Initiate and drive operational efficiency improvements, including process and toolkit optimisation through methods such as solution enhancements and automation

Drive adoption and adherence to Information Security policy, standards and guidelines

Audit access controls, identify breaches of inappropriate access levels and analyse breaches and activities for patterns, and recommend improvements to processes or policies

Lead the security support team, embedding a culture of service excellence, innovation and continuous improvement founded on cohesiveness, team work and flexibility

Perform a security assurance role to ensure that security rules and principles are embedded within the design of technology and services developed, and that best practice process and technologies across the security landscape are in place

Actively contribute to other initiatives and activities in the information and cyber security space including policy and standards design, security awareness and security solutions development

Identify strategic initiatives and areas requiring risk remediation

Network with industry peers and the wider community, contribute and share ideas

Act as escalation point for security application problems and incidents

Other duties as directed

**Your specific work capabilities (selection criteria)**

Relevant tertiary qualification or demonstrated equivalent competency

Relevant industry certifications including CISSP, CISM or other security/control certifications

Substantial and extensive IT experience in information and cyber security, including a strong understanding of the cyber kill chain and advanced threats and malware techniques and tactics

Excellent written and verbal skills with demonstrated ability to communicate with influence, establish positive stakeholder relationships at all levels of the university, and negotiate competing priorities whilst always remaining fully customer focused

Excellent planning and organisational skills

Demonstrated ability to contribute to long term planning and key strategic direction

Proficiency in a range of computing skills including word processing, spreadsheets, databases, internet, and email

Demonstrated experience working within or managing a security operations function, including experience with incident response, security event monitoring, vulnerability assessments and firewall configuration and rule-base creation

Demonstrated experience with security solutions covering at least 3 of the following areas: Cloud Computing & Security, Anti-Malware solutions, including APT and advanced threat solutions, Malware reverse-engineering and cyber forensics, Endpoint threat detection, prevention and response solutions, Security monitoring and security analytics solutions, Identity & Access Management, Application Security, including source code and vulnerability assessment, Infrastructure and network security

Demonstrated experience with Windows and Unix operating systems to a sys admin level

Relevant experience with infrastructure and networking concepts and technologies

Demonstrated experience with the operating model of security operations, processes and requirements

Knowledge of information security standards and best practices including Data Retention Act (2015) and ISO-27001

Relevant experience in security analytics experience (e.g. Splunk or Hadoop)

Relevant software development or shell scripting experience and skills

Working knowledge of the Higher Education sector is desirable

**Special requirements (selection criteria)**

No special requirements

**Compliance**

Workplace Health & Safety

All supervising staff are required to undertake effective measures to ensure compliance with the Occupational Safety and Health Act 1984 and related University requirements (including Safety, Health and Wellbeing Objectives and Targets).

All staff must comply with requirements of the Occupational Safety and Health Act and all reasonable directives given in relation to health and safety at work, to ensure compliance with University and Legislative health and safety requirements. Details of the safety obligations can be accessed at <http://www.safety.uwa.edu.au>

Inclusion & Diversity

All staff members are required to comply with the University’s Code of Ethics, Code of Conduct and Inclusion and Diversity principles. Details of the University policies on these can be accessed at <http://www.hr.uwa.edu.au/policies/policies/conduct/code>, <http://www.web.uwa.edu.au/inclusion-diversity>.