Position Description – Cybersecurity Operations Manager

Position Details

Position Title: Cybersecurity Operations Manager

Position Number: 50065548

College/Portfolio: Operations

School/Group: Information Technology Services / Chief Information Security Office

Campus Location: Based at the Melbourne campus but may be required to work and/or be based at other campuses of the University.

Classification: HEW10C

Employment Type: Continuing

Time Fraction: 1.0

RMIT University

RMIT is a multi-sector university of technology, design and enterprise with more than 96,000 students and close to 10,000 staff globally. The University's mission is to help shape the world through research, innovation and engagement, and to create transformative experiences for students to prepare them for life and work.
https://www.rmit.edu.au/about
https://www.universitiesaustralia.edu.au/university/rmit-university

Our three main campuses in Melbourne are located in the heart of the City, Brunswick and Bundoora. Other locations include Point Cook, Hamilton and Bendigo, two campuses in Vietnam (Hanoi and Ho Chi Minh City) and a centre in Barcelona, Spain. RMIT is a truly global university.
https://www.rmit.edu.au/about/our-locations-and-facilities

We are also committed to redefining our relationship in working with, and supporting, Indigenous self-determination. Our goal is to achieve lasting transformation by maturing our values, culture, policy and structures in a way that embeds reconciliation in everything we do. We are changing our ways of knowing, working and being to support sustainable reconciliation and activate a relationship between Indigenous and non-Indigenous staff, students and community. Our three campuses in Melbourne (City, Brunswick and Bundoora campuses) are located on the unceded lands of the people of the Woi Wurrung and Boon Wurrung language groups of the eastern Kulin Nation.

Why work at RMIT University

Our people make everything at the University possible. We encourage new approaches to work and learning, stimulating change to drive positive impact. Find out more about working at RMIT University, what we stand for and why we are an Employer of Choice.
https://www.rmit.edu.au/careers

We want to attract those who will make a difference. View RMIT's impressive standings in university rankings.
https://www.rmit.edu.au/about/facts-figures/reputation-and-rankings

College/Portfolio/Group

The Operations Portfolio enables an integrated, enterprise-wide delivery for best practice student and staff experiences.

The Portfolio incorporates the following business units: Enterprise Projects and Business Performance (EPBP), Communications, People, Information and Technology Services (ITS), Office of the Chief Operating Officer, Procurement and Vietnam Operations.

The Portfolio houses significant drivers and delivery components across the staff and student journeys and enables the overall experience for both groups. The Portfolio is integral in bringing the RMIT strategy to life, across the globe. Each of these functions supports the global operations of the University both directly as well as through its controlled entities.

The Information Technology Services (ITS) function provides RMIT University with current and emerging Technology systems and services. Our vision of "unleashing technologies to enable great experiences for RMIT communities" supports a proactive and leading-edge technology ecosystem, mindset and delivery empowering the advancement of the University's commitment to advancing Lifelong Learners.

Position Summary

Reporting to the Chief Information Security Officer (CISO), the Cybersecurity Operations Manager will take ownership, develop and drive the vision for cybersecurity operations within the global University. The role is responsible for managing an RMIT Security Operations Centre (SOC) team and third-party managed service providers, including the identification and work-to-resolution of cyber threats that may impact on the confidentiality, integrity and availability of RMIT's global services.

The Cybersecurity Operations Manager will provide strategic vision and guidance based upon threat intelligence, spearhead the running and continuous improvement of cybersecurity operations, oversee security incident response activities, manage third party Security Operations Centre (SOC) providers, manage a small team of Security Analysts and SMEs and act as the Application Owner for Shared Security applications/toolsets, continuously measure and report on performance of the services.

As a leader in the field, the Cybersecurity Operations Manager delivers strategic cyber thought leadership to RMIT and achieves operational excellence through technical, financial and business acumen.

Reporting Line

Reports to: Chief Information Security Officer

Direct reports: Five

Organisational Accountabilities

RMIT University is committed to the health, safety and wellbeing of its staff. RMIT and its staff must comply with a range of statutory requirements, including equal opportunity, occupational health and safety, privacy and trade practice. RMIT also expects staff to comply with its policy and procedures, which relate to

statutory requirements and our ways of working.

Appointees are accountable for completing training on these matters and ensuring their knowledge and the knowledge of their staff is up to date.

Key Accountabilities

1. Driver of change and Cyber thought leadership across the university that thinks holistically about the pace and scale of disruption to enable RMIT to be enterprise cyber resilient.
2. Manage security operations, focusing on maintaining RMIT's SOC team and vendor accountability and effective communication and collaboration with other ITS teams and stakeholders.
3. Lead security incident response activities including threat hunting, incident response and recovery.
4. Lead the Cybersecurity Operations function across RMIT group of entities providing vision, contemporary thought leadership and direction.
5. Manage third party SOC vendor in their Manage, Detect and Response services.
6. Improve external threat intelligence partnerships.
7. Lead and direct event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
8. Plan and recommend modifications or adjustments based on cyber exercise results or system environment.
9. Actively lead the team using Agile methodologies

Key Selection Criteria

1. Extensive experience with large scale IT Security Operations practices with proven superior understanding of information technology and current threat landscape
2. Expert knowledge across cybersecurity technologies (e.g., Threat Management / Intelligence; Vulnerability Management, Identity and Access Management etc.)
3. Extensive experience in being a persuasive leader who can serve as an effective member of the Leadership Management team and who is able to communicate technology risk related concepts to a broad range of technical and non-technical staff.
4. Demonstrated ability to prioritise tasks and deliver a quality service to the University.
5. Exceptional interpersonal, communication and conflict negotiation skills, with the ability to liaise effectively with internal and external teams, in order to identify and solve issues.
6. Outstanding people leadership experience. Strong people management skills; exceptional teamwork and collaboration expertise.

Qualifications

Tertiary qualification as well as relevant experience and/or certifications in Risk Management and/or Cybersecurity such as CRISC, CISM, CISSP etc. would be an advantage.

Endorsed:	Signature: Name: Title: Date:	**Approved:**	Signature: Name: Title: Date: