

Position Description

Senior Cyber Security Lead

Position No:	50036485
Department:	Security, Risk and Compliance
Division:	Information Services
Campus/Location:	Melbourne (Bundoora)
Classification:	Higher Education Officer 9 (HEO9)
Employment Type:	Full time, Continuing
Position Supervisor:	Security, Risk and Compliance Manager
Supervisor Position Number:	50015253
Other Benefits:	http://www.latrobe.edu.au/jobs/working/benefits

Further information about:

La Trobe University - <http://www.latrobe.edu.au/about>

For enquiries only contact:

Caitlin Hosking TEL: 03 9479 1324 Email: c.hosking@latrobe.edu.au

Position Description

Senior Cyber Security Lead

Position Context:

"As trusted digital thought leaders we connect and enable the University Community to advance learning, teaching and research"

With the University Community at the centre of everything we do, Information Services (IS) is focused on creating and sustaining an innovative information technology culture as one dynamic team. IS consistently engages with our customers delivering value through service performance, continuous improvement and transformational project based outcomes. The La Trobe Cultural Qualities of being innovative, accountable, connected and caring are fundamental to engaging and empowering our people.

The Security, Risk and Compliance department is accountable for establishing information security policy and standards which, in a number of cases, will be administered within Enterprise Services. In addition the department will provide co-ordination for vulnerability management, threat detection, incident response and reporting.

Working closely with both the Office of the CTO and Enterprise Services (and other IS Departments), the Security, Risk and Compliance department develops the security requirements, controls and designs to ensure that the University's information and technical environments are secure and risks are known understood and communicated.

The Security, Risk and Compliance department will translate the Universities risk appetite into actionable security plans to achieve targets set.

The Security, Risk and Compliance department is also responsible for the University's IS Security Strategy, IS Risk and Compliance Framework, IS Security policies, standards and procedures and IS risk and compliance activities.

This position is primarily responsible for the following.

- The design, tuning, operation and use of the IS Security tools to enhance the defence, detection and response capability of the University.
- Undertake IS Security related investigations.
- Taking a risk-based approach to the design and implementation of pragmatic security controls for use across at La Trobe University.
- Provides Security consulting and expert advice to IS Architecture and other teams, Projects, University staff and external partners such as suppliers of IT security products; and vendors of services.

Duties and level of responsibility include, but are not limited to:

- The design, tuning, operation and use of the University IS Security tools that provide defence, detection and response. This includes the monitoring of relevant threat feeds and intelligence sources and the ingestion of appropriate indicators into security tools where possible.
- Undertake IS Security related investigations as required by an authorized officer.
- In conjunction with other IS staff, co-ordinate and manage security incidents as delegated and ensure the identification of issues and escalation where appropriate.
- Facilitate the third-party vendor security assessments and tests, such as the execution of regular Penetration Tests.
- Translate technical vulnerabilities into business risk terminology for Faculties/Business Units and developing risk mitigation strategies and ensuring timely corrective actions where required.
- Take a risk-based approach to the design and implementation of pragmatic security controls for use across at La Trobe University to enable IS strategic directions and roadmaps.
- Actively contribute to the IS Security Strategy, Policy and Governance.
- Develop security requirements and security controls that will align with the overall IS Enterprise and Infrastructure architecture.
- Provides Security consulting and expert advice to other IS teams, projects, University staff and external partners such as suppliers of IT security products; and vendors of services.
- Where appropriate, conduct rigorous testing for new security and access tools, services, and hardware, to ensure a resilient and highly protected network.
- Ensure compliance with implemented ITIL processes.
- Develop and maintain an up-to-date documentation of University security infrastructure as it relates to configurations, processes and designs.
- Work in collaboration with all Faculties/Business Units and appropriate teams across the IS Division to proactively identify and resolve security issues.
- Operate within a project management framework undertaking activities related to small or large projects either as a subject matter expert or quality assurance resource.
- Provide 24 hour/7 days-a-week rostered, on-call support for critical IT services in accordance with the La Trobe University Collective Agreement On-Call Arrangements, as required.
- Supporting a culture of empowerment and achievement, inspiring others to learn, develop, unlock their potential and succeed.
- Role modelling the La Trobe values and Cultural Qualities, holding themselves and others accountable for demonstrating targeted behaviours.
- Actively contributing to shaping the team within the context of the division and in alignment with La Trobe strategies.
- Improving own professional capability and expertise through appropriate development and/or professional activities in alignment with La Trobe's Career Success framework.
- Understanding the whole of University context and supporting the CIO and IS leadership in executing assigned initiatives.
- Responding flexibly to changing circumstances, assists leaders with the creation of a flexible environment that supports and enables others to meet changing demands.
- Offers support to the team in times of high pressure, seeks assistance as required. Encouraging the celebration of success and engaging in activities to maintain morale.
- Making personal short-term commitments without authorisation from higher levels, takes into consideration personal accountabilities and workload, ensuring that divisional processes, practices and standards are adhered to.
- Instituting personal reflection and evaluation practices to drive a continuous model of improvement.

- Interacting with all stakeholders including managers, peers, team members and colleagues as customers, as defined within the University Customer Service Charter.

Key Selection Criteria:

- Significant subject matter knowledge and expertise across cybersecurity technologies (e.g., Threat Management / Vulnerability Management; Identity Management; Event Detection and Response)
- Experience using security incident and event management tools for hunting and investigating security incidents.
- Demonstrated ability to contribute to Security Strategy and Governance.
- Demonstrated knowledge of security concepts, scripting languages and/or technical solution design.
- Demonstrated knowledge of network and web related protocols, (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols).
- Proven capability of managing IT Security incidents.
- Relevant certifications and/or qualifications eg. IT degree, CISSP, CISM, GCIH, GIAC etc
- Knowledge of ITIL, namely Change Management, Incident Management, and Problem Management.
- Proven ability to apply theoretical knowledge or management expertise to bring together diverse and sometimes conflicting information to solve complex problems, that may affect one or many areas of the organisation.
- Proven record of developing innovative solutions for strategic change, with the ability to be responsible for development and implementation.
- Has the ability to be reflective, be innovative and able to deliver continuous improvement with a demonstrated high level of self-motivation and personal management skills.
- Demonstrated ability to establish and maintain positive working relationships with internal and external stakeholders (including vendors) and communicate effectively on a range of sensitive and complex issues, including the ability to negotiate, motivate, influence and build relationships.

Essential Compliance Requirements:

To hold this La Trobe University position the occupant must:

- hold, or be willing to undertake and pass, a Victorian Working With Children Check; AND
- take personal accountability to comply with all University policies, procedures and legislative or regulatory obligations; including but not limited to TEQSA and the Higher Education Threshold Standards.

Position Flexibility

La Trobe University is committed to providing a diverse, inclusive and respectful working environment for all staff. We offer flexible work arrangements that can assist you in balancing your work and other responsibilities.

La Trobe Cultural Qualities:

Our cultural qualities underpin everything we do. As we work towards realising the strategic goals of the University we strive to work in a way which is aligned to our four cultural qualities:

- *We are **Connected***: We connect to the world outside — the students and communities we serve, both locally and globally.
- *We are **Innovative***: We tackle the big issues of our time to transform the lives of our students and society.
- *We are **Accountable***: We strive for excellence in everything we do. We hold each other and ourselves to account, and work to the highest standard.
- *We **Care***: We care about what we do and why we do it. We believe in the power of education and research to transform lives and global society. We care about being the difference in the lives of our students and communities.

For Human Resource Use Only

Initials: Date: