

## Position Description

### Chief Information Security Officer

---

<b>Position No:</b>	50147857
<b>Business Unit:</b>	Chief Operating Officer (COO)
<b>Division:</b>	Information Services (IS)
<b>Department:</b>	Cybersecurity
<b>Classification Level:</b>	ESMC2
<b>Employment Type:</b>	Fixed Term – 3 years
<b>Campus Location:</b>	Bundoora, Victoria
<b>Other Benefits:</b>	<a href="http://www.latrobe.edu.au/jobs/working/benefits">http://www.latrobe.edu.au/jobs/working/benefits</a>

Further information about:

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

---

## **Position Context/Purpose**

La Trobe is a top-rated independent research university with world-leading research and global impact. The university is seeking a cyber security leader to protect the university, its partners and community against current cyber threats and emerging. Higher education presents one of the most complex and diverse cyber threat environments of any sector which must be managed while enabling the university to grow and innovate.

The Chief Information Security Officer (CISO) is the leader of the Office of the CISO. The CISO is accountable for the information security of the University, including:

- The design and implementation of the University's Cyber Security Strategy.
- The maintenance and implementation of the Information Services (IS) Risk and Compliance Framework.
- Supporting Business Continuity Planning and disaster response.
- The security operations function.
- Build trust with internal and external university stakeholders, supporting strategic priorities while managing risk.

The CISO has responsibility and accountability for information security regulatory obligations including under the Security of Critical Infrastructure (SOC) Act, and the Privacy Act.

The CISO reports into the Chief Information Officer (CIO) and is part of the Information Services Executive Team. The CISO would be expected to regularly report on cyber security maturity to the Information Services Executive team, and other stakeholders if required.

## Key Duties and Accountabilities

### Reporting Structure

- Accountable for the University Cyber Security function, reporting to the Chief Information Officer (CIO).
- Accountable to develop, implement and maintain the University Cyber Security Strategy and Roadmap, and Business continuity planning for our technology environment ensuring on-going monitoring of a comprehensive Information Security, Risk, and Compliance Management Framework, related to the availability, integrity, and confidentiality of University information.
- Accountable to deliver a program of work for Cyber and ensuring delivery of cyber security projects and initiatives, including support and compliance for Defence Industry Security Program, Security of Critical Infrastructure (SOCI) Act requirements, and foreign interference mitigation.

### Strategic Planning

- Participate in forward planning for the Information Services strategic plan and objectives, evaluates the environment and identifies fundamental issues to be resolved.
- Focus on a multi-year strategic planning horizon of 3-5 years and actively contribute to the development of the University's Strategic Plan.
- Delegated accountability for resources budgets. Meets agreed planning targets with the allocated budget and reports regularly to the Information Services Executive Team on the progress against annual operational and longer-term strategic plans and identify areas of concern.
- Consider relevant industry context and strategic cyber intelligence in developing cyber security strategy and initiatives.

### Security Operations

- Responsible for managing the University's security operation functions, specifically:
  - Protect: coordinating the prioritised implementation of cyber security controls to protect University information assets.
  - Detect: managing the internal and external Security Operations Centre (SOC) and SIEM capabilities.
  - Respond: prepare and coordinate the University's incident response capability.
- Provide subject-matter expertise and be the final decision maker on security tooling decisions.
- Assess and prioritise technical security control implementation based on University risks and priorities.

### Leadership

- Effectively lead the Office of the CISO.
- Encourage and motivate people to engage in continuous learning and empower them by delegating tasks. Agree to clear performance standards and gives timely constructive feedback, praise and recognition, and deals with under-performance promptly.
- Engage with and manage third-party providers to achieve improved cyber outcomes for the university.

### Assurance and Advice

- Responsible for compliance and reporting, including breaches, for both IT Cyber Security and working through audit items, operational matters, and process improvements, ensuring on-going review of our foundational processes, roles, and responsibilities to seek continuous improvement through digital tooling.
- Provide expert advice in establishing practices, templates, policies, tools, and partnerships to expand and mature these capabilities for the organisation.

- Manage internal stakeholders; engage with key business and technical stakeholders, ensuring full awareness of current state activities and alignment of deliverables with expectations.
  - Provide internal status reporting.
  - Negotiate between other internal stakeholders.
  - Mediate between the conflicting interests of different stakeholders.
- Provide authoritative counsel and advice in key University forums and committees.
- Represent the University to external stakeholders on cyber security matters. Build confidence and develop relationships with third parties.

## Essential Criteria

### Technical skills required for this position:

- Knowledge and understanding of relevant legal and regulatory requirements, such as:
  - The Defence Industry Security Program.
  - The Security of Critical Infrastructure (SOCl) Act.
  - The Privacy Act.
- Knowledge of relevant information security management frameworks, including:
  - NIST Cyber Security Framework.
  - NIST 800-53.
- Some familiarity with other common information security frameworks, such as:
  - ISO27001.
  - ASD Essential 8.
- Sound knowledge of current information security and cyber security technologies across the security operations capabilities of detect, protect, and respond.
- Demonstrable knowledge of risk management concepts including:
  - Risk management frameworks.
  - Business Continuity Planning.
  - Incident response and disaster recovery.
  - Business impact assessments.
- Excellent written and oral communication skills, including experience briefing senior non-technical stakeholders. Demonstrated ability to adapt communication approaches to different audiences.

### Other Skills and knowledge required for the position:

- Tenacity and resilience in striving for goals. Developing creative, innovative, and sustainable long-term solutions.
- Exemplary leadership supporting a performance-orientated and accountable team culture.
- Demonstrated experience in strategy and/or policy development for a large organisation.
- Outstanding interpersonal skills including conflict resolution, and a capacity to negotiate outcomes with stakeholders and achieve results in an environment that is characterised by competing expectations and views.
- Acts as a subject-matter expert in cyber security. Supports the University's key leaders to make informed decisions on cyber security matters.

## 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.
- Take personal accountability to comply with all University policies, procedures and legislative or regulatory obligations; including but not limited to the Tertiary Education Quality and Standards Agency (TEQSA) and the Higher Education Threshold Standards.

## Other Information

The position description is indicative of the initial expectation of the role and subject to changes to University goals and priorities, activities or focus of the job.

## Position Flexibility

We offer flexible work arrangements that can assist you in balancing your work and other responsibilities.

## Why La Trobe:

- Develop your career at an innovative, global university where you'll collaborate with community and industry to create impact.
- Enjoy working on our inspiring and stunning campuses – the perfect hub for industry, students and academics
- Help transform the lives of students, partners and communities now and in the future

This is more than just a job. Working at La Trobe offers opportunities to demonstrate excellence and transform lives.

Here, you'll join exceptional people, partners and communities, who power our operations with ambition and purpose.

Our success can be attributed to its strong sense of community. We have a long-standing commitment to diversity, inclusion and social justice; we are committed to providing a workplace where all staff feel valued, respected and supported to achieve their full potential. We strive to build a workplace where all employees of diverse backgrounds, abilities, experiences, sexuality, gender, religion and age are welcome, valued, respected and one that is representative of our community. We demonstrate our cultural qualities by holding ourselves accountable and creating a culture of trust and innovation while genuinely caring for one another.

## La Trobe's Cultural Qualities:

### WE ARE CONNECTED



We are **connected** to each other and the communities around us. We engage with those communities to learn from our past, inform our present and impact our future.

### WE ARE INNOVATIVE



We are **innovative** in tackling the most important issues of our time. We are inquisitive and seek to develop new ideas that positively impact the way we work and the world around us.

### WE ARE ACCOUNTABLE



We are **accountable** for what we do and share a commitment to excellence. We are courageous and respectful in the way we hold ourselves and each other to account.

### WE CARE



We **care** about what we do and value the power of education and research. We care about each other and strive to create a safe and inclusive community.

---

For Human Resource Use Only

Initials:            Date: