Position Description – Senior Information Security Strategy & Governance Lead

Updated 10/06/2022

POSITION DETAILS	
Portfolio	**Corporate Services**
Organisational Unit	**Information and Digital Services (IDS)**
Supervisor	**Chief Information Security Officer (CISO)**
Classification	**Higher Education Officer 10**
Employment Type	**Continuing, full-time**

POSITION SUMMARY

Under generally unguided direction, the role is responsible for leading the ongoing development, implementation and continuous improvement of the cyber and information security strategies and related governance activities for Flinders University.

The role is also responsible for maintaining pace with the cyber threat landscape and new technologies, and providing expert advice on cyber and information security strategies to executive, senior management, and other relevant stakeholders across the University.

The role works closely with the Chief Information Security Officer (CISO) and relevant IDS and University stakeholders to ensure the successful delivery of the cyber and information security program.

UNIVERSITY EXPECTATIONS AND VALUES

All staff at Flinders are responsible for understanding their obligations and responsibilities as set out in the University's code of conduct and are expected to:

- demonstrate commitment to the University's values of Integrity, Courage, Innovation, Excellence and the underlying ethos of being Student Centred;
- contribute to the efficient and effective functioning of the team or work unit in order to meet the University's objectives. This includes demonstrating appropriate and professional workplace behaviours, providing assistance to team members if required and undertaking other key responsibilities or activities as directed by one's supervisor;
- promote and support an inclusive workplace culture which values diversity and embraces the principles of equal opportunity;
- perform their responsibilities in a manner which reflects and responds to continuous improvement; and
- familiarise themselves and comply with the University's *Work Health and Safety, Injury Management and Equal Opportunity* policies.
- *A National Police Certificate which is satisfactory to the University will be required by Flinders University before the successful applicant can commence in this position. If you have any queries in this regard please raise them with the named contact person in this Position Description in the first instance.*
- *COVID-19 vaccination in accordance with the Flinders University COVID-19 Vaccination Policy (2022) is a condition of employment with the University. Any offer of employment will be subject to the successful candidate presenting their COVID-19 Digital Certificate as evidence of vaccination or showing evidence of a valid medical exemption where relevant.*

KEY POSITION RESPONSIBILITIES

The key position responsibilities include:

Technical Vision & Roadmap

1. Working with the CISO, CIO and relevant stakeholders to develop, support, maintain and deliver an information security strategy and associated roadmap of activity to support and drive the appropriate focus of ongoing maturity uplift activities and investment in the information security capability and posture for the University.
2. Working with CISO, CIO and relevant stakeholders to ensure an appropriate information security governance ecosystem is established, maintained, supported, and continuously reviewed for improvement and effectiveness.
3. Working with the CISO, CIO and relevant stakeholders and committees to confirm the appropriate maturity models and frameworks for the University to provide a basis for peer, industry, and general maturity benchmarking.
4. Updating and maintaining maturity benchmarking information for the purposes of management reporting as well as to support the setting and prioritisation of the information security work program.

Technical Management & Support

5. In collaboration with the CISO and relevant IDS stakeholders, proactively providing and coordinating information security advice and solutions to University stakeholders.
6. Developing and drafting relevant IDS directives, policies, and procedures in relation to information security, to support maintaining an appropriate risk profile and posture for the University.
7. Working with the CISO to ensure that relevant government policy, legislation and notices are appropriately reviewed and considered, with recommendations proactively provided to senior management.
8. Working with the CISO to draft University responses to government and industry bodies who are seeking input and feedback from the University regarding information security related matters.
9. Working with the CISO and CIO to develop and complete regular management reporting regarding information security strategy, maturity, benchmarking, project activity, environmental factors, threats, and vulnerabilities.

Technical Knowledge & Excellence

10. Reviewing University policies and processes in relation to information security and providing recommendations for changes and updates.
11. Developing and implementing an ongoing cyber and information security awareness and education training program for the University.
12. Conducting both formal and informal market scanning and benchmarking activities to be aware of emerging market offerings and trends.
13. Periodically participating in knowledge building activities and events to be aware of latest/best practices related to the role and to keep skills and knowledge up to date.

Risk, Governance & Ways of Working

14. Leading and maintaining an agile based way of working to manage, refine, and prioritise the activity backlog based on relevant customer and IDS priorities.
15. Identifying, managing, and mitigating risks related to the activities being undertaken by the role in line with IDS and Flinders University policies and procedures
16. Ensuring compliance with all relevant IDS and Flinders University policies and procedures.

Other Responsibilities

17. Any other responsibilities in line with the level of the role as assigned by the Supervisor and/or the University.

KEY POSITION CAPABILITIES

- Appropriate tertiary qualification in Information Technology or relevant technical area, and / or equivalent relevant experience in an IT environment.
- At least two or more valid industry recognised security certifications, for example Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), Certified in Risk and Information Systems Control (CRISC).
- Extensive knowledge of international cyber and information security legislation, regulations and standards and frameworks (e.g., International Organisation for Standardisation ISO27001, National Institute of Standards and Technology (NIST), ACSC Essential Eight).
- Demonstrated expert knowledge of cyber and information security in the context of a university environment, with reference to balancing cyber security with objectives of privacy, academic freedom, intellectual property, open systems, and academic enterprise networks.
- Advanced strategic thinking, planning and analytical skills and actively contributes to achieve outcomes and meet the University's strategic goals.
- High level skills in leading and managing a team to its full potential, including advanced interpersonal and relationship management skills and the ability to manage staff performance.
- Extensive experience in building and managing customer relationships in a strategic and long-term context.
- Extensive experience in agile ways of working including exposure to scaled agile methodologies and/or collaborating and delivering through a matrix structure.
- High level self-improvement and growth mindset/approach to the role and fosters it amongst the wider team.
- Advanced interpersonal influence and demonstrated ability to negotiate and communicate effectively with staff and customers across a diverse organisation particularly during the design, management, and implementation of customer solutions.
- Higher education experience advantageous.