Position Description – Information Security Officer

July 2025

POSITION DETAILS	
Portfolio	**Corporate Services**
Organisational Unit	**Information and Digital Services (IDS)**
Supervisor (Title)	**Senior Information Security Audit and Risk Specialist**
Classification	**Higher Education Officer Level 6**
Employment Type	**Fixed-term, full-time**

POSITION SUMMARY

Under general to broad direction the Information Security Officer is responsible for providing a support function for the University's information security services. The role will include the research and evaluation of procedural and technical controls and solutions that can be applied to provide security to the University's IT networks and systems and to comply with relevant laws and regulations.

This role will also work closely with other practitioners and teams to ensuring the ongoing security and effectiveness of the University's network and system assets, and the stable and continuous operation of the University's mission-critical systems and applications.

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.

An up to date COVID-19 vaccination may be required as a condition of employment, in accordance with the Flinders University COVID-19 Vaccination Policy (2022). If required, 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 Information Security Officer has responsibility for supporting and carrying out the technological requirements of the University's IT security processes are fully addressed. Under the management of the Chief Information Security Officer and the Senior Information Security Audit and Risk Specialist, the Information Security Officer is accountable for:

1. Managing the queue of requests via initial telephone/email support for issues assigned to the Cyber Security GRC team.
2. Maintaining and implementing effective security policy for new and existing security platforms and tools, to ensure a positive security posture and sustainable IT services environment for the University.
3. Identifying technological trends and developing reports as necessary to keep IDS management apprised of information security threats and planned equipment or software changes that could impact system and network security and availability.
4. Supporting and assisting with the ongoing application of the IDS Risk Register; identifying and ensuring the management of key risks that may impact on the security of the University's systems and networks.
5. Undertaking security reviews of new cloud-based systems and platforms intended to be used by the University, in order to ensure the levels of protection appropriate to their use.
6. Maintaining and implementing the university's cyber security awareness and training program.
7. Contributing to the periodic review and auditing of network and system activity. In collaboration with the Senior Information Security Lead and other team members, supporting the implementation of agreed mitigations.
8. Implementing guidelines, processes, systems and metrics in pursuit of best practice and to establish a culture of continuous improvement.
9. Implementing security policies and procedures and ensuring understanding and compliance by other technical staff.
10. Providing advice on security matters relating to disaster recovery and business continuity, ensuring that disaster recovery plans and business continuity plans appropriately address security requirements in maintaining the provision of services.
11. Working collaboratively across the University to ensure positive outcomes, including any support that may be required for the effective operation of the Information Security team, and assisting other IDS team members when and where appropriate.
12. Completing and presenting all reports requested to the Senior Information Security Audit and Risk Specialist, Chief Information Security Officer, or other senior IDS leaders.
13. Any other responsibilities in line with the level of the position as assigned by the Chief Information Security Officer, the Senior Information Security Lead, and/or the University.

Flinders University

KEY POSITION CAPABILITIES

1. A degree in computer science, business technology or other relevant qualifications or an equivalent combination of experience and/or education and/or training.
2. Familiarity and experience in information security.
3. Familiarity with security policy controls and how to implement them effectively in ways to both protect and enable University business services.
4. Experience in providing security advice and guidance in relation to IT projects and explaining complex technical or security issues to ensure that non-technical stakeholders understand the risk/security trade-offs.
5. Demonstrated ability to gain trust and partner with internal and external stakeholders at all levels in a customer and business focused manner.
6. Demonstrated ability to interact and collaborate positively and effectively with colleagues and clients at all levels. Is a good team player.
7. Demonstrated ability to analyses issues, solve problems and make decisions by applying sound judgements, including the implications of proposed security solutions on business processes and existing networks and infrastructure.
8. Demonstrates initiative, work ethic and ability to work effectively responding to management direction. Completes tasks and assignments with good accountability.
9. Very good written and verbal communication skills, and an ability to compile and prepare correspondence reports, submissions and similar documents.
10. An understanding of IT security in the context of higher education environment, with particular reference to systems, networks and applications that are used and how these relate to attaining a good cybersecurity posture.
11. Demonstrated understanding of cybersecurity risk management practices.