Flinders University

Position Description – *Information Security Specialist*

Updated 12/05/2023

POSITION DETAILS

College/Portfolio	***Corporate Services***
Organisational Unit	***Information and Digital Services***
Supervisor (Title)	***Information Security Lead***
Classification	***Higher Education Officer Level 7***
Employment Type	***Continuing, full-time***

POSITION SUMMARY

Under broad direction the Information Security Specialist is accountable to the Information Security Lead and is responsible for ensuring that the technical aspects of the cyber security are implemented effectively to reduce IT risk to the University. The role will include the research and evaluation of procedural and technical solutions that can be applied to the University's infrastructure and applications.

This role will also work closely with relevant managers and IT architects to ensure the ongoing protection of the University's information 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 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.

This role requires Australian citizenship and a current Defence security clearance of Baseline or above, or the ability and willingness to be processed for such a clearance.

A Nationally Coordinated Criminal History Check which is satisfactory to the University will be required by Flinders University before the successful applicant can commence in this position.

KEY POSITION RESPONSIBILITIES

The Information Security Specialist has responsibility for ensuring that the technical requirements of the University's information security processes are fully addressed; and that the security measures implemented are protecting and supporting the University's core business activities. The incumbent is responsible for providing guidance and advice to the broader University on IT security matters and has an enterprise wide remit, operating across both the academic and corporate divisions.

The Information Security Specialist is accountable for:

1. Configuring, deploying and maintaining new and existing security platforms, including advanced email filtering, firewall, intrusion prevention/detection systems, anti-malware, VPN, and host protection.
2. Providing technical leadership in the identification, review and implementation of technological developments in information security and developing reports as necessary to keep the group and wider stakeholders apprised of information security threats and planned equipment or software changes that could impact system and network security and availability.
3. Managing configuration and improving the University's proactive security monitoring systems to ensure the incidents and security weaknesses can be identified and mitigated to reduce the potential impact to the wider University.
4. Maintaining configuration control of security infrastructure and monitoring controls applied to the centralised network and systems supporting the operation of the University.
5. Promoting information security initiatives across all University stakeholders, developing communication and written guidance.
6. Providing technical advice on security matters relating to disaster recovery, ensuring that disaster recovery plans appropriately address security requirements in maintaining the provision of services.
7. 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.
8. Ensuring operational procedures and work practices are current, documented and fit for purpose.
9. Any other responsibilities in line with the level of the position as assigned by the Supervisor and/or University.

KEY POSITION CAPABILITIES

- Appropriate tertiary qualification in Information Technology or relevant technical area, and / or equivalent relevant experience in an IT environment.
- Demonstrated knowledge and experience in network security. Experience implementing, managing, configuring and monitoring hardware (such as firewalls, intrusion prevention/detection systems, anti-malware, security information and event monitoring solutions).
- Demonstrated experience in providing technical security advice and guidance in relation to IT projects and demonstrated ability to explain complex technical or security issues to ensure that non-technical stakeholders understand the risk/security trade-offs.
- Demonstrated ability to interact effectively with colleagues and clients at all levels across the University including senior management, students and visitors, and a commitment to providing a high level of client service.

- Demonstrated ability to analyse 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.
- Demonstrated experience in performing support and administration tasks to manage cyber security in the context of a University environment, with particular reference to balancing cybersecurity with objectives of privacy, academic freedom, intellectual property, open systems and academic enterprise networks.
- Well-developed written communication skills, and an ability to compile and prepare correspondence reports, submissions and similar documents.
- Good negotiating and problem-solving skills.
- Well-developed oral communication skills including presentation skills.
- Higher education experience advantageous.