Federation University

Greater together

Position description

Position title	Senior IT Security Specialist
Institute/School/Centre/ Directorate/VCO	Information Technology Services (ITS)
Campus	Mt Helen Campus. Travel between campuses may be required.
Classification	Within the HEW Level 8 range
Time fraction	Full-time
Employment mode	Fixed-term employment
Reason for fixed term	Replacement employee
Probation period	This appointment is offered subject to the successful completion of a probationary period.
Further information from	Leigh Vincent, Head, IT Security Risk Telephone: (03) 5327 9386 Email: l.vincent@federation.edu.au
Recruitment number	JR101554

Position summary

As the Senior IT Security Specialist, you will deliver high-level technical expertise, strategic security advice and specialist guidance to safeguard the University's digital assets, strengthen its cyber security posture and protect its critical information systems.

The position is responsible for developing and implementing IT security procedures and processes that align with the University's goals, risk appetite, industry good practice and regulatory obligations. It provides authoritative technical input on complex security matters and supports effective security outcomes across the organisation.

You will work closely with other teams within the organization to identify potential security risks, develop plans to mitigate those risks, and provide guidance on security best practices. Additionally, you will be responsible for ensuring that all security systems are up to date and functioning properly, and that any security incidents are promptly investigated and resolved.

Portfolio

Information Technology Services (ITS) strives to be an innovative and reliable partner to the University, engaging all areas of the business in a collaborative and adaptable approach. ITS provides dependable services, whilst ensuring excellence in what we do, with quality and integrity.

Comprising of several cross-functional teams supported by an underpinning service support layer and governed by an overall strategic services and business solutions framework, ITS ensures that investment in technology is f it for purpose and benefits the University.

Background

At Federation University, we are driven to make a real difference to the lives of every student, and to the communities we serve.

We are one of Australia's oldest universities, known today for our modern approach to teaching and learning. For 150 years, we have been reaching out to new communities, steadily building a generation of independent thinkers united in the knowledge that they are greater together.

Across our University and TAFE campuses in Ballarat, Berwick, Gippsland, and the Wimmera, we deliver world-class education and facilities. With the largest network of campuses across Victoria, we are uniquely positioned to provide pathways from vocational education and skills training at Federation TAFE through to higher education.

To be successful at Federation University you must be willing to enthusiastically embrace the University's ambition as expressed in Federation University's 2040 Strategic Plan and share the University's values of:

INCLUSION, we champion access and equity for all, creating a welcoming, supportive environment for our diverse learners and staff.

INNOVATION, we innovate to transform, embracing new ideas in teaching, research and operations to continually improve and stay ahead.

EXCELLENCE, we strive for excellence in all that we do, holding ourselves to high standards of quality, integrity and impact.

EMPOWERMENT, we support and trust our people, empowering learners, staff and partners to contribute, lead and succeed.

COLLABORATION, we are stronger together; teamwork and strong partnerships are at the heart of how we operate.

Key responsibilities

1. Provide authoritative technical leadership, specialist guidance and escalation support across complex IT security matters. Drive knowledge sharing and technical capability development, while collaborating with colleagues and key stakeholders to coordinate security initiatives, resolve complex challenges and deliver effective, risk-informed security outcomes.
2. Develop and implement IT security procedures and processes: You will be responsible for creating and updating the University IT security processes and procedures to ensure that they align with industry best practices and comply with regulatory requirements.
3. Conduct comprehensive security assessments of the University's information assets to identify, evaluate and prioritise vulnerabilities and potential security risks. Partner with relevant technical teams and stakeholders to develop, coordinate and oversee the timely implementation of appropriate remediation strategies and risk mitigation measures, strengthening the University's overall security posture.
4. Take an active role in security incident investigations: Apply specialist expertise to undertake investigations into cyber attacks, data breaches and other security-related events, working with relevant stakeholders to support timely containment, remediation and reporting.
5. Stay up-to-date with the latest security trends and threats: You will need to stay current with the latest security trends and threats and make recommendations to senior management regarding new security technologies and strategies to mitigate risks.
6. Collaborate with other teams: You will need to collaborate with other IT teams and departments within the University, such as network operations, system administration, enterprise data, IT projects and compliance, to ensure that IT security is integrated into all aspects of the University's operations.
7. Reflect and embed the University's strategic plan, and operational purpose, priorities, and goals.
8. Embed effective risk management practices to ensure continuous service delivery. Participate in training and exercises to remain prepared for potential disruptions.

9. Undertaking the responsibilities of the position adhering to:
    - the Staff Code of Conduct, Child Safe Code of Conduct, and Conflict of Interest Policy and Procedure;
    - Equal Opportunity and anti-discrimination legislation and requirements;
    - the requirements for the inclusion of people with disabilities in work and study;
    - Occupational Health and Safety (OHS) legislation and requirements; and
    - Public Records Office of Victoria (PROV) legislation.

Level of supervision and responsibility

The Senior IT Security Specialist operates as a senior individual contributor, providing authoritative technical advice, coordinating complex security work and contributing to planning, prioritisation and resource decisions. The position provides strategic support and advice to ITS and the wider University community, without direct staff-management responsibility.

The Senior IT Security Specialist works under the broad direction of the Head, IT Security & Risk and exercises a high degree of autonomy to help ensure the availability, confidentiality and integrity of University systems, services and data. The position will also receive day-to-day directions from the Team Leader, ITS Security and will be required to work both as part of the security team and independently in a variety of security tasks.

The position provides specialist input into software selection and deployment and ensures appropriate security scans and assessments are conducted prior to go-live.

The Senior IT Security Specialist ideally possesses an understanding of multi-sector institutions and the information reporting requirements of relevant government bodies. This position must also develop and maintain an in-depth knowledge of the structure and functions of the Schools and Directorates/Sections within the University, an awareness of the ramifications of system unavailability, and a broad understanding of relevant policies, procedures and guidelines and their wider application across the University.

Position and organisational relationships

The Senior IT Security Specialist reports to the Head, IT Security & Risk, and works collaboratively across ITS to support access to the necessary resources, skills and knowledge for effective security outcomes.

The Senior IT Security Specialist provides authoritative technical expertise and strategic advice, guiding evidence-based decisions on the selection, implementation and optimisation of security tools, services and investments within delegated authority.

The Senior IT Security Specialist works in close liaison with ITS colleagues to foster strong relationships, in addition to collaborating with key internal and external stakeholders.

The Senior IT Security Specialist requires agile but sound analytical and problem-solving skills to analyse information and apply judgement and relevant experience to resolve issues promptly in a complex and diverse environment. The position is required to exercise judgement concerning the availability, confidentiality and integrity of systems, services and data while considering the interdependencies across systems.

The Senior IT Security Specialist is a subject matter expert responsible for the design and implementation of properly authorised security customisations and enhancements to end-to-end services.

The Senior IT Security Specialist is required to have expertise in the operation of commercial software, tools and frameworks relevant to ensuring the availability, confidentiality and integrity of systems, services and data.

Key selection criteria

Applicants must demonstrate they are able to undertake the inherent responsibilities of the position as contained in the position description and are able to meet the following key selection criteria:

Training and qualifications

1. Completion of:
   - a relevant postgraduate qualification or progress towards postgraduate qualifications and extensive relevant experience; or
   - extensive experience and advanced specialist expertise; or
   - an equivalent combination of relevant experience and/or education/training.

   Knowledge and expertise in cloud applications in a university context is highly desirable.
2. Must hold a valid *Employee* Working with Children (WWC) check.

Experience, knowledge and attributes

3. Demonstrated ability to provide authoritative technical advice, influence stakeholders and coordinate complex security activities in a customer-focused environment, while working within organisational and budgetary constraints.
4. Demonstrated experience in IT Security in a complex IT environment, including demonstrated experience in incident handling and response, vulnerability management and tools, techniques and frameworks relevant to IT Security activities.
5. Demonstrated understanding and application of the Information Technology Infrastructure Library (ITIL)
6. processes and procedures.
7. Demonstrated ability to coordinate and provide expert technical direction during responses to cyber incidents and investigations, while ensuring the highest levels of confidentiality and privacy.
8. Demonstrated ability to operate effectively in high-pressure and high-stress security scenarios, coordinate contributions from relevant stakeholders and deliver high-quality outcomes, including written reports as required.
9. Ideally, the demonstrated understanding of the operations of multi-sector institutions and their relationship to DEEWR, Skills Victoria, VTAC and other relevant government agencies.
10. Demonstrated communication, interpersonal and negotiation skills, including proven experience and ability to work effectively in a team and contribute to a positive and safe workplace culture.
11. Demonstrated alignment with the University's commitment to child safety.

The University reserves the right to invite applications and to make no appointment.

It is not the intention of the position description to limit the scope or accountabilities of the position but to highlight the most important aspects of the position. The aspects mentioned above may be altered in accordance with the changing requirements of the role.