POSITION DESCRIPTION

Position Title:	(Senior) Information Security Analyst
Organisation Unit:	Information Technology Services
Position Number:	TBA
Type of Employment:	12 months Fixed Term, full-time
Classification:	Hew Level 6/7 + 15% cash (industry loading)

THE UNIVERSITY OF QUEENSLAND

The University of Queensland (UQ) contributes positively to society by engaging in the creation, preservation, transfer and application of knowledge. UQ helps shape the future by bringing together and developing leaders in their fields to inspire the next generation and to advance ideas that benefit the world. UQ strives for the personal and professional success of its students, staff and alumni. For more than a century, we have educated and worked with outstanding people to deliver **knowledge leadership for a better world**.

UQ ranks in the world's top universities, as measured by several key independent ranking, including the Performance Ranking of Scientific Papers for World Universities (45), the US News Best Global Universities Rankings (52), QS World University Rankings (51), Academic Ranking of World Universities (55), and the Times Higher Education World University Rankings (60). UQ again topped the nation in the prestigious Nature Index; and secured a greater share of Australian Research Council grants in 2016 ($24.5 million) than any other university nationally.

UQ has an outstanding reputation for the quality of its teachers, its educational programs and employment outcomes for its students. Our students remain at the heart of what we do. The UQ experience –the UQ Advantage – is distinguished by a research enriched curriculum, international collaborations, industry engagement and opportunities that nurture and develop future leaders. UQ has a strong focus on teaching excellence, winning more national teaching excellence awards than any other in the country and attracting the majority of Queensland's highest academic achievers, as well as top interstate and overseas students.

UQ is one of Australia's Group of Eight, a charter member of edX and a founding member of Universitas 21, an international consortium of leading research-intensive universities.

Our 50,000-plus strong student community includes more than 13,000 postgraduate scholars and more than 12,000 international students from 144 countries, adding to its proud 230,000-plus alumni. The University has about 7,000 academic and professional staff and a $1.7 billion annual operating budget. Its major campuses are at St Lucia, Gatton and Herston, in addition to teaching and research sites around Queensland and Brisbane city. The University has six Faculties and four University-level Institutes. The Institutes, funded by government and industry grants, philanthropy and commercialisation activities, have built scale and focus in research areas in neuroscience, biomolecular and biomedical sciences, sustainable minerals, bioengineering and nanotechnology, as well as social science research.

UQ has an outstanding track-record in commercialisation of our innovation with major technologies employed across the globe and integral to gross product sales of $11billion+ (see http://uniquest.com.au/our-track-record).

UQ has a rapidly growing record of attracting philanthropic support for its activities and will have further success in this area as an important strategic aim going forward.

Organisational Environment

The division of Information Technology Services (ITS) at The University of Queensland provides an information environment that supports the teaching, learning, research and engagement objectives of the University and contributes positively to the student experience and the University's reputation, in line with our values of Service, Team, Accountability and Results. It comprises three major sections located across the University's campuses: Academic Services, Enterprise Support and University Networks. Also located within ITS is the internationally recognised information security group, AusCERT, which provides services throughout Australia and New Zealand. ITS manages core networks not only for the whole of The University of Queensland but also, on behalf of the Queensland Regional Network Organisation (QRNO), works with Queensland universities to manage access to the national university network (AARNet). ITS also operates Supercomputers and many of the University's largest servers.

AusCERT is a leading Cyber Emergency Response Team for Australia. As a not-for-profit information security group based at The University of Queensland, AusCERT helps members prevent, detect, respond to and mitigate threats. Formed in 1993, AusCERT is one of the oldest CERTs in the world. AusCERT monitors and evaluates global cyber network threats and vulnerabilities, and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, threat intelligence and other relevant resources for information security and IT professionals.

For further information visit our website www.its.uq.edu.au and www.auscert.org.au.

Information for Prospective Staff

Information about life at UQ including staff benefits, relocation and UQ campuses is available at - http://www.uq.edu.au/current-staff/working-at-uq

DUTY STATEMENT

Primary Purpose of Position

This position is responsible for technical and operational support within the Australian Cyber Emergency Response Team (AusCERT).

Duties

Duties and responsibilities include, but are not limited to:

Information Security Analyst **HEW level 6**	**Senior Information Security Analyst** **HEW level 7**
• Carry out individual work or participate in group-based project assignments as required, with some freedom to propose own topics of interest where relevant to AusCERT's members. AusCERT's development environment is primarily Python based.	• Undertake design, development and project management of information technology projects, including ICT service development, and evaluation. AusCERT's development environment is primarily Python based.
• Development and evaluation of security tools and techniques.	• Provide advice regarding the security, design, implementation, installation and maintenance of AusCERT's information technology systems and infrastructure. Duties may include evaluation of open source security tools and techniques.
• Vulnerability analysis.	• Vulnerability analysis.
• Consult on the technical aspects of information technology to AusCERT members.	• Consult on the technical aspects of information technology and provide high level support for services delivered to AusCERT's members.
• Maintain a current knowledge of networking, computer and security standards, state-of-the-art developments and products. Maintain links with authorities, vendors, and relevant personnel within international peer groups, the Internet and the global university and research community.	• Maintain a current knowledge of networking, computer and security standards, state-of-the-art developments and products. Maintain links with authorities, vendors, and relevant personnel within international peer groups, the Internet and the global university and research community.
• Incident response and other related provision of services to members.	• Incident response and other related provision of services to members.
• Contribute to the activities of other groups within AusCERT as directed, under the supervision of the relevant manager	• Contribute to content development and delivery of services within AusCERT.
• Supply information and advice for the production of operational, budgeting and planning reports as required.	• Assist the team leader and unit manager in matters of budget preparation, management of the unit, planning and adherence to ICT procurement guidelines

	• Assist team members in developing their skill set through mentoring, providing senior support and expertise to other staff on information security and technology topics, as appropriate
• Travel (intrastate, interstate and/or overseas) on AusCERT business as required, including, but not limited to, Flying Squad engagements and other out of office activities.	• Travel (intrastate, interstate and/or overseas) on AusCERT business as required, including, but not limited to, Flying Squad engagements and other out of office activities.

- An employee may be required to carry out other duties within the scope of the classification and within the limits of their skill, competence and training

Other
Ensure you are aware of and comply with legislation and University policy relevant to the duties undertaken, including:

- the University's Code of Conduct
- requirements of the Queensland occupational health and safety (OH&S) legislation and related OH&S responsibilities and procedures developed by the University or Institute/School
- the adoption sustainable practices in all work activities and compliance with associated legislation and related University sustainability responsibilities and procedures
- requirements of the Education Services for Overseas Students Act 2000, the National Code 2007 and associated legislation, and related responsibilities and procedures developed by the University

Some positions may require the incumbents to work rotating shifts with appropriate allowances, or on a rotating roster not involving shift work as such. Some positions may require the incumbent to be available on-call outside of working hours, subject to payment of the prescribed allowance and overtime penalties if necessary. While staff will have a campus nominated as their principal campus, they may be required to work at any University Campus subject to the Travel and Transfer Policy (http://ppl.app.uq.edu.au/content/5.43.09-transfer-and-travel-between-university-locations).

Organisational Relationships

The position reports to the Team Leader, Coordination Centre. At HEW 7, the position may be required to direct other professional or technical staff on work relating to specific tasks or projects.

SELECTION CRITERIA

Please indicate in your selection criteria response for which HEW level you are applying:

Information Security Analyst **HEW level 6**	**Senior Information Security Analyst** **HEW level 7**

Essential • EITHER: ○ Bachelor's Degree, or equivalent, ideally with significant information technology component; Industry certification in one or more of the following areas: computer security, training, systems administration, programming or networking OR ○ An equivalent combination of relevant experience and/or education/training. • At least two years' experience in the IT industry, with at least one year of experience relevant to IT security. Some variation may be considered for applicants with a strong match to the other selection criteria. A demonstrable interest in information security is expected. • Knowledge of: ○ Ability to at least read/troubleshoot Python or an equivalent high level language ○ Shell scripting or equivalent system administration toolset. ○ The architecture and services of the TCP/IP protocol suite; ○ Linux operating systems (preferably RHEL and/or Debian). • Strong communication and interpersonal skills, with a demonstrable ability to work effectively with others to achieve positive outcomes. *Desirable* • Formal training in one or more of the following areas: ○ An IT security related discipline. ○ CSSLP (https://www.isc2.org/csslp/default.aspx) or CISSP	*Essential* • EITHER: ○ Bachelor's Degree, or equivalent, ideally with significant information technology component; Industry certification in one or more of the following areas: computer security, training, systems administration, programming or networking OR ○ An equivalent combination of relevant experience and/or education/training. • Formal training in one or more of the following areas: ○ IT security related discipline ○ SANS certification in an IT security related area ○ CSSLP, CISSP, or CISM certification • At least four years' experience in the IT industry, with at least two years of experience relevant to IT security including IT security incident resolution and/or a CSIRT team. Experience in computer/network forensics, or consulting in information security will be highly regarded. Some variation may be considered for applicants with a strong match to the other selection criteria. A demonstrable interest in information security is expected. • Experience applying information security management standards in a workplace, as well as ability to produce comprehensive policy and procedure documents, business proposals, content for publication and other forms of written communications in a high quality and accurate manner. • A willingness and ability to work with other staff including in a mentorship and support role.

https://www.isc2.org/cissp/default.aspx

- Experience in one or more of the following:
    - Computer/ network forensics.
    - IT security incident resolution.
    - A CSIRT team, particularly a coordination centre area.
    - Consulting or customer service experience in information technology, preferably in information security.
    - Windows operating systems (including Active Directory and administration).
    - Use of the RT (or RTIR) ticketing system
    - ISAC or similar models for information sharing groups
- Knowledge and/or experience in one or more of the following areas:
    - Networking/firewalls.
    - Big data analysis systems such as ELK and/or Splunk

- Programming including the ability to read/troubleshoot Python or a similar high level language
- Knowledge and experience in at least four of the following:
    - Shell scripting or equivalent system administration toolset.
    - The architecture and services of the TCP/IP protocol suite;
    - Linux operating systems (preferably RHEL and/or Debian).
    - Networking/firewalls
    - Big data analysis systems such as ELK and/or Splunk
- Strong communication and interpersonal skills, with a demonstrable ability to work effectively with others to achieve positive outcomes.

Desirable

- Experience in the supervision of staff.
- Experience in program management and/or project leadership for small projects

Australian Citizen or Permanent Residence required. The successful applicant will be required to submit to background checks.

The University of Queensland values diversity and social inclusion.

Employment opportunities are not limited by race, ethnicity, religion, disability, age, sexuality, gender or other protected attributes. Applications are encouraged from Aboriginal and Torres Strait Islander peoples. For further information please contact our Indigenous Employment Coordinator at: atsi_recruitment@uq.edu.au