Cyber Security Analyst - Investigations

College/Division	Division of the Chief Operating Officer
School/Section	Information Technology Services
Location	Burnie / Launceston / Hobart / Sydney
Classification	Higher Education Officer Level 7
Reporting line	Reports to Associate Director, Cyber Security

Position Summary

The University of Tasmania is building a vision of a place-based University with a mission to enhance the intellectual, economic, social and cultural future of Tasmania, and from Tasmania, contribute to the world in areas of distinctive advantage. The University recognises that achieving this vision is dependent on the people we employ as well as creating a people-centred University that is values-based, relational, diverse, and development-focused.

We are seeking to appoint a Cyber Security Analyst – Investigations within IT Services as a part of the Division of the Chief Operating Officer.

The Security Analyst will be responsible for identifying, analysing, and influencing the management of information risks across the organisation

- Review logs and events and investigate anomalies
- Stay abreast of developments in the Information Technology industry specifically as they relate to Information Security
- Manage investigations of a highly sensitive nature where breaches in the Universities acceptable use policy, state or federal laws have occurred while adhering to privacy requirements
- Provides guidance to first responders for handling information security incidents
- Compiles and analyses data for management reporting and metrics
- Conducts computer forensic analysis, data recovery, eDiscovery, and other IT investigative work
- Determines the most appropriate methods of protecting original evidence and recovering deleted, erased, hidden and encrypted data.

The role includes the development and implementation of procedures and standards around a Cyber Security Framework, ongoing compliance assessment against the framework, and communication on ICT security matters to University members and ICT operational support staff.

We are an inclusive workplace committed to 'working from the strength that diversity brings' reflected in our Statement of Values. We are dedicated to attracting, retaining and developing our people and are committed to inclusive principles. We celebrate the range of diverse assets that gender identity, ethnicity, sexual orientation, disability, age and life course bring. Applications are encouraged from all sectors of the community. Tell us how we can make this job work for you.

What You'll Do

- Investigate and report on ICT security threats, incidents and breaches, conduct forensic analysis and design and implement mitigation strategies.

- Champion the ICT Security agenda influencing positive outcomes in the use of ICT in a secure, efficient and effective environment.
- Work collaboratively with other ICT Services teams and stakeholders across the University to effectively manage ICT Security compliance and ICT Security investigations.
- Develop and maintain effective reporting and communication methods to University Governance groups, University members and ICT operational staff and provide expert advice on contemporary ICT security issues
- Lead and contribute to compliance reviews across ICT infrastructure, business systems and business practices and ensure remediation work is undertaken effectively within an agreed timeframe.
- Liaise with ICT security experts from external organisations and groups to ensure comprehensive and expert knowledge on ICT security issues and trends is maintained.

What We're Looking For (success criteria)

- Experience in ICT security compliance and risk management including the ability to lead, investigate and report on ICT security threats, incidents and breaches
- Technical expertise in performing digital forensics on a variety of media, including hard drives, thumb drives, memory cards, and cellular devices
- Technical expertise in following industry best practices and standards in digital evidence acquisition, handling, and documentation
- Work collaboratively with other University members including IT Services, Key Stakeholders, students and external bodies to troubleshoot, resolve security issues and conduct forensic analysis to assist with investigations
- Tertiary qualifications in ICT or ICT security industry certifications or extensive relevant experience in ICT security

Other position requirements *(delete those not applicable)*

- Knowledge of University environment.
- Experience in establishing and implementing effective ICT security and Information Security framework including strategy, policy, practice and methodologies.

University of Tasmania

The University of Tasmania is an institution with an enduring commitment to our state and community, and a strong global outlook. We are committed to enhancing the intellectual, economic, social and cultural future of Tasmania. Our Strategic Direction strongly reflects the University community's voice that our University must be place based but globally connected as well as regionally networked and designed to deliver quality access to higher education for the whole State.

We believe that from our unique position here in Tasmania we can impact the world through the contributions of our staff, students and graduates. We recognise that achieving this vision is dependent on the people we employ, as well as creating a university that is values-based, relational, diverse, and development-focused.

Check out more here:

https://www.utas.edu.au/jobs

https://www.utas.edu.au/careers/our-people-values-and-behaviours

The intention of this position description is to highlight the most important aspects, rather than to limit the scope or accountabilities of this role. Duties above may be altered in accordance with the changing requirements of the position.