The University of Waikato
Te Whare Wānanga o Waikato

POSITION DESCRIPTION

Senior Cybersecurity Analyst

Vision

We will
- deliver a world-class education and research portfolio
- provide a full and dynamic university experience which is distinctive in character
- pursue strong international linkages to advance knowledge

The over-arching themes of this *Vision* are:
- Excellence
- Distinctiveness
- International Connectedness

Values

Ko te mana o Te Whare Wānanga o Waikato ka herea ki tō tātou:
- Tu ngātahi me te Māori
- Mahi pono
- Whakanui i ngā huarahi hou
- Whakarewa i te hiringa i te mahara

The University of Waikato places a high value on:
- Partnership with Māori
- Acting with integrity
- Celebrating diversity
- Promoting creativity

1. GENERAL

The Information Technology Services (ITS) Division is responsible for the coordination of information and communications technology (ICT) planning for the University, the delivery of robust, reliable core ICT infrastructure and enterprise systems, and the provision of professional ICT consultancy and customer focused support services.

The ICT vision is “To engage, enable, innovate and protect our ICT services, and empower the University of Waikato to leverage the value of ICT to achieve its strategic goals.”

2. POSITION PURPOSE

Within the ITS Network and Security group, the Cybersecurity team is responsible for identifying security risks, ensuring appropriate security protection is implemented, monitoring and detecting security issues, responding to security incidents and overseeing post-incident recovery. The Cybersecurity team includes internal staff and outsourced services provided by the University’s cybersecurity partner.

The Senior Cybersecurity Analyst position is responsible for monitoring and maintaining the compliance of information systems and associated infrastructure with security policies, standards and controls. The role

also has responsibility for the maintenance and communication of security standards and procedures; investigation, reporting and escalation of possible breaches of ICT security; coordination of regular security risk assessment of critical ICT systems and ICT Infrastructure; assistance in the development and evaluation of new strategies and plans to address potential and known security practices and procedures; providing advice and guidance on IT security practices; assisting with planning and coordinating the awareness and education on security policies; and maintenance of online security resources, standards and industry best practice information.

As part of information security, the position is responsible for ensuring the effectiveness of the cybersecurity systems including end-point protection systems; vulnerability management systems; incident and event monitoring systems; firewall and intrusion preventions systems; plus, any other information security systems that may be implemented in future.

3. ACCOUNTABILITY

The Senior Cybersecurity Analyst is responsible to the Associate Director Network, Security and Assurance.

4. FUNCTIONAL RELATIONSHIPS:

Internal: Network and Cybersecurity Teams
Chief Information Officer
ITS managers and teams
Vice Chancellors office, Pro Vice Chancellors and Directors
University staff and students

External: External customers utilising University ICT services
Cybersecurity vendors and support partners

5. KEY TASKS

5.1 Security Controls

- Provide input to and lead initiatives from the information security aspects of the University's ICT Strategy.
- Provide input for ongoing improvement of the University's security standards and best practices for the organization, including recommending security enhancements to management as needed.
- Develop strategies to respond to and recover from security breaches.
- Educate University staff and students on information security through coordinating and administering an ongoing security awareness programme.
- Oversee the implementation of security systems, such as firewalls, network access control, network and log monitoring, and data encryption programs, to protect sensitive information.
- Provide advice and guidance regarding the implementation or processing of new security products and procedures.
- Undertake regular security risks assessments, utilising the University's cybersecurity partner as required, and initiate and track appropriate pro-active actions when security risks are identified.
- Review the results of the cybersecurity partner's vulnerability scan reports and ensure vulnerabilities are mitigated. Arrange and coordinate penetration testing.
- Investigate new and emerging ICT technologies and assess effectiveness of their security controls.
- Ensure there is ongoing effective monitoring of networks and systems in order to detect security breaches or intrusions, including implementing and administering systems and software to help detect irregular system behaviour.
- Undertake incident response activities during security breaches to minimize the impact, participate in the technical and forensic investigation into how the breach happened and reporting findings to management.
- Provide feedback on the ITS Network and Security group standards and procedures for security administration and support.

5.2 Security Administration

- Develop and maintain a thorough understanding of the University's centrally supported applications, systems and technologies, especially the security administration of such.
- Monitor ICT environment security integrity and performance using monitoring systems and operational procedures to ensure environments are kept secure, including ensuring the effectiveness of the University's cybersecurity partner's services.
- Administer or peer review the administration of cybersecurity related systems and applications.
- Maintain security system and process operational documentation - keep up to date and accurate records.
- Ensure that ITS, Service Desk and Users are kept aware of current security threats and the status of situations arising from security related issues.
- Respond to information security service requests and incidents in a timely manner.

5.3 Team Contribution

- Actively participate in project and Cybersecurity team activities.
- Participate in peer review processes to ensure changes are implemented effectively.
- Provide security advice, guidance and assistance to other technical staff within ITS and external to the Network and Security teams.
- Undertake administration and support activities resulting from incident or change requests from within the Cybersecurity team, or when participating as a member of a project team.
- Participate in the maintenance of a safe and healthy work environment for self and others, including students. Comply with and undertake responsibilities set out in the University's Health and Safety Policy.

5.4 On-call

- There is no on-call requirement for this role.
- However, for critical incidents the Senior Cybersecurity Analyst may be called out, if available, to provide appropriate security incidence response (tier-3 response) to after-hours incidents escalated from other ITS on-call (tier-2) staff, or the University's cybersecurity partner's 24x7 operations centre (SOC).

Any other duties as required that are consistent with the position held, other than in exceptional circumstances such as rehabilitation after injury or sickness.

NOTE: Staff have an annual Objectives, Development and Reflection (ODR) meeting with their manager. New staff attend such a meeting approximately three months after taking up their appointment.

6. PERFORMANCE STANDARDS

The Senior Cybersecurity Analyst will be performing satisfactorily when:

- ITS, Service Desk and Users are kept aware of current security threats and the status of situations arising from security issues.
- Procedures which ensure reliable and professional operation of the security administration environment are always followed.
- Optimum security of the University's data and ICT applications and infrastructure is maintained and complies with service levels defined in the Service Level Agreements.
- Staff and students are routinely provided with updated information security awareness information and kept aware of the latest cybersecurity threats and associated best practice.
- Identity and end-point protection, intrusion prevention and other information security systems are kept up to date and security breaches and incidents are promptly responded to.
- Security monitoring and administration systems maintenance, support and operations run efficiently and effectively.
- Systems and data are protected from unauthorised access and denial of service attacks, with security incidents promptly dealt with, including logging and auditing information being captured to retrace unauthorised and attempted access.
- Problem analysis methods, tools and techniques are successfully applied to a variety of security problem/incident situations.

- Regular security risk assessment and audits are undertaken and identified risks are appropriately managed.
- Security patches and updates are completed within agreed timeframes.
- Systems and networks are routinely vulnerability tested, and issues are identified and remedied in a timely manner.
- Best practice ICT security is promoted and fostered, with advice and assistance provided to ensure systems and data security is consistently maintained.
- Server and storage equipment is configured and physically installed in line with current systems infrastructure hardening guidelines.
- Technical and procedural documentation and security records are up to date and available when required, and security standards and guidelines are maintained.
- Operational security documentation is produced and delivered to operation teams at a level which is understandable.
- All IT changes are managed via the change management process.
- Knowledge of administrative tasks is shared amongst other Cybersecurity staff and partner resources.
- The ability to recognise critical issues and think strategically is demonstrated consistently and in a broad range of project types (including complex situation assessment/strategy projects/tactical work on system security health).
- Proactive cybersecurity support/assistance is routinely provided to the other team members where appropriate.
- Positive feedback is received from business and customer stakeholders, and from colleagues with ITS.
- Safe and healthy work practices are followed that comply with University policies and procedures, relevant work standards and statutory obligations.

PERSON SPECIFICATION

EDUCATIONAL QUALIFICATIONS

Essential

- Bachelor's degree or higher in Computer Science or related field, be studying for such qualification, or equivalent relevant work experience.
- Certification in an industry standard framework such as CompTIA Security+, SSCP, CISM or CISSP, or be studying for such.

Preferred

- Higher education or industry recognised senior qualification or certification in ICT Security.

TRAINING, SKILLS AND KNOWLEDGE

Essential

- At least 5 years of experience in information security / cybersecurity administration, operation and incident response.
- Demonstrated experience and technical fluency with various security architectures, systems and industry security best practice.
- Experience with the use of ISO/IEC 2700x, NIST CSF, NZISM, CIS or other standards and frameworks.
- Good understanding of specialised security technologies and monitoring tools.
- Awareness of the security issues related to cloud technologies and services.
- Willingness to work helpfully with others and to be involved and share activities.
- Effectiveness in presenting a message in a meaningful form to persuade and influence others.
- Ability to understand organisational priorities and political sensitivities.
- Excellent analytical and problem-solving skills.
- Effective verbal communication and proven documentation skills.

Preferred

- Knowledge of security administration and operation of Microsoft 365 security products (e.g. Defender, Sentinel, Purview, Intune, etc) and Fortinet security products (e.g. Fortigate Firewalls, FortiAnalyzer, ZTNA, etc).
- Knowledge of penetration testing, attack surface monitoring and dark web monitoring.
- Knowledge of the security hardening requirements for virtual server technologies, Windows and Linux systems and applications, and large campus network environments.
- Knowledge of cybersecurity forensics.
- Experience of working in a Tertiary Institution would be helpful.

PERSONAL QUALITIES

- Good communication skills, oral and written; ability to communicate with end users as well as technical staff.
- Client focussed and user centred approach to development.
- Strong problem identification and solving skills.
- Ability to identify improvements, innovate, and implement change.
- Ability to work independently and with the minimum supervision and equally well in a team/project environment.
- Attention to detail and thoroughness.
- The capacity to show initiative and judgment.
- Discretion and respect for confidentiality.
- A commitment to a culture of openness, flexibility and co-operation to achieve excellence.
- A commitment to equal opportunity and to the University's partnership with Māori as intended by the Treaty of Waitangi.

July 2025