

POSITION DESCRIPTION



SECTION A: Position Context

Position Title	Security Analyst
Position Grade	E2 – Executive
Category	Executive
Campus / Unit	Sarawak Campus – Information Technology (IT)
Term of Appointment	Fixed-Term Appointment
Effective Date	September 2026

Position Purpose

The position is a technical support position at the Sarawak Campus. The position will be responsible for carrying duties involving various functions of Information Technology designated by the Manager, Infrastructure and Cybersecurity Risk; or Director, Information Technology – mainly responsible for monitoring, analysing, and responding to security threats and incidents to protect our organisation's digital assets. The position will work closely with IT Infrastructure, Customer Support and Application teams to ensure the integrity, confidentiality, and availability of information systems.

Participation on Committees

The appointee will be required to participate on relevant committees as is needed for the efficient performance of duties and as directed by the Manager, Infrastructure and Cybersecurity Risk; or Director, Information Technology; or by an authorised personnel.

Supervision Reporting Relationships

<u>This positions'</u> supervisor/manager	Manager, Infrastructure and Cybersecurity Risk; or any other person as assigned by an authorised personnel.
Other position reporting to <u>this position</u>	None.

Location

This position is located at the Swinburne University of Technology Sarawak Campus.

SECTION B: Key Responsibility Areas

The key responsibility areas (KRAs) are the major outputs for which the position is responsible and are not a comprehensive statement of the position activities.

KEY RESPONSIBILITY AREAS		
1.	TECHNICAL SKILLS AND KNOWLEDGE	- Act as the organisation's early warning system by continuously observing network traffic, analysing system logs, and managing Security Information and Event Management (SIEM) tools to spot suspicious activities and filter out false alarms before a potential threat escalates. - Bridge the gap between technical systems and human behaviour by ensuring the organisation's adherence to legal frameworks and industry standards (such as NIST CFS), documenting the security posture for leadership, and conducting ongoing training to help employees recognise and avoid common threats such as phishing. - Proactively hunt for systemic weaknesses by conducting regular network scanning, coordinating simulated penetration tests, and enforcing rigorous patch management to identify, assess, and prioritise technical risks before malicious actors can exploit them. - Build and maintain robust technical defences installing, configuring, and managing essential security infrastructure – including firewalls, endpoint protection (EDR), and strict identity access controls, while ensuring all new IT projects are designed securely from the ground up.
2.	POLICY AND PLANNING	Assist and support the Manager, Infrastructure and Cybersecurity Risk to implement and to ensure compliance with all the policies relating to Information Technology.
3.	RESOURCE MANAGEMENT	- Establish and maintain materials and equipment storage. - Ensure system compatibility, maintenance of Swinburne Standard Operating Environment.
4.	VENDOR RELATIONSHIP MANAGEMENT	- Specify items required and obtain quotations as necessary. - Maintain good relationship with vendors.
5.	REPORTS	Prepare reports and provide accurate information as and when required by the Management.
6.	OCCUPATIONAL HEALTH AND SAFETY (OHS)	Assist management in ensuring compliance of all OHS legal and procedural requirements by various stakeholders, including through the following: - Execute OHS requirements in respective work areas; - Maintain cleanliness, good housekeeping and overall safe work environment; and - Undertake immediate correction and improvement action on any non-compliance practices, and report all OHS related injuries, ill health or incidents to the OHS section.
7.	SWINBURNE VALUES AND CULTURE	- Commit to the Swinburne Values. - Conduct work professionally while demonstrating the Swinburne Values at all time.
8.	CUSTOMER SERVICE	Demonstrate Swinburne Values including: - Provide IT related services; - Perform general equipment troubleshooting; and - Work effectively and with flexibility as a member of the technical team, providing prompt input, advice and assistance as required.
9.	OTHER DUTIES	Any other duties as and when required and directed by the Manager, Infrastructure and Cybersecurity Risk; and/or Director, Information Technology; or by an authorised personnel.

SECTION C: Key Selection Criteria

Application letters and/or resumes must address the Qualifications and Knowledge/Experience/Attributes sections under the key selection criteria.

Qualifications: Include all educational and training qualifications, licences, and professional registration or accreditation, criminal record checks etc. required for the position.		Essential / Highly Desirable / Preferable
1.	A Bachelor's degree in Information Technology (IT), Computer Science or other related discipline from a recognised institution with at least three (3) years relevant work experience. Master's degree holder can be considered.	Essential
2.	Possess at least one (1) relevant IT certification(s) with active status in either system, network, project management, information security, operations, or equivalent. (e.g; CCNA, ITIL, CompTIA Security+, or equivalent)	Highly Desirable

Experience / Knowledge / Attributes: Required by the appointee to successfully perform the positions key responsibilities.		Essential / Highly Desirable / Preferable
1.	At least three (3) years of relevant working experience in two of the following domains: deployment, configuration, support, cybersecurity, network security, project management in a medium to large enterprise with a proven record of providing quality service.	Essential
2.	Experience in assisting or performing risk assessment or incident response and management.	Essential
3.	Familiar with current security technologies and keen interest in learning within security domain.	Essential
4.	Familiar with support and manage the Endpoint Detection and Responses (EDR/XDR), email security gateway, Firewall, IPS,VPN,DLP,MFA, etc.	Essential
5.	Handle, validate and investigate Security Events (Intrusions/Malicious Activity/Security Events).	Essential
6.	Ability to perform the tasks assigned under pressure and short notice. Ready to work outside of normal office hours when required.	Essential
7.	Ability to handle confidential and sensitive information responsibly.	Essential
8.	Self-motivated, demonstrating a high level of initiative, assertiveness, versatility and flexibility.	Essential
9.	Experience in responding to all audit enquires pertaining to IT security matters.	Highly Desirable
10.	Demonstrates up-to-date knowledge of the current cyber security trends, threats, solutions and tools.	Highly Desirable
11.	Understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, and common security elements.	Highly Desirable