POSITION DESCRIPTION

SECTION A: Position Context

Position Title	IT Executive (Information Security)
Position Grade	E2 - Executive
Category	Executive
Campus / Unit	Sarawak Campus – Information Technology
Term of Appointment	Full-time Appointment
Effective Date	June 2024

Position Purpose

The position is a technical support position at the Branch Campus University in Sarawak. The position will be responsible for carrying duties involving various functions of Information Technology designated by the Manager, Information Technology - mainly to develop, deploy and support IT initiatives for the University, which include planning, governance, project management, security, technology review, processes improvement, issue management, technology presentation and training, risk management, incident management, infrastructure implementation and administration and any other activities across other sections of IT Unit as well as any other relevant tasks as assigned.

Participation on Committees

The position will be required to participate on relevant committees as is needed for the efficient performance of duties and as directed by the Assistant Manager; or Manager, Information Technology; or Director, Administration; or the Pro Vice-Chancellor and Chief Executive Officer - PVC & CEO (Sarawak); or by an authorised personnel.

Supervision Reporting Relationships

This positions' supervisor/manager	Assistant Manager (Infrastructure), Information Technology; or any other person as assigned by an authorised personnel
Other position reporting to this position	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**	• Establish a framework for risk management; which involves identifying particular events or circumstances (threats and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. • Perform analysis of technology risk metrics, then formulate and provide independent reporting on the University's technology and cyber risk posture. • Lead and drive the establishment of IT security activities and initiatives as part of the University's IT Security programme; inclusive of security awareness, training and incident response. • Develop and maintain appropriate security documentation for applications, infrastructure and systems. • Manage and monitor Cybersecurity incidents, logs, alerts and events to ensure the cybersecurity risk is mitigated.
2.	**POLICY AND PLANNING**	Assist and support the Manager and Assistant Manager, Information Technology 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 and Culture 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 Assistant Manager (Infrastructure); and/or IT Manager; or Director Administration; or PVC&CEO (Sarawak); 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 Computer Science or IT or a related discipline from a recognised institution with a minimum of three (3) years of relevant work experience; or A Diploma in Computer Science or IT or a related discipline from a recognised institution with a minimum of five (5) years of relevant work experience.	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, 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 and leadership.	Essential
2.	Experience in assisting or performing risk assessment or incident response and management.	Essential
3.	Experience in running small/medium size IT projects in a corporate environment.	Essential
4.	Familiar with current security technologies and keen interest in learning within security domain.	Essential
5.	Familiar with supporting and managing the Endpoint Detection and Responses (EDR/XDR), Email security gateway, Firewall, IPS,VPN,DLP,MFA, etc.	Essential
6.	Handle, Validate and Investigate Security Events (Intrusions/Malicious Activity/Security Events).	Essential
7.	Ability to perform the tasks assigned under pressure and short notice. Ready to work outside of normal office hours when required.	Essential
8.	Ability to handle confidential and sensitive information responsibly.	Essential
9.	Self-motivated, demonstrating a high level of initiative, assertiveness, versatility and flexibility.	Essential
10.	Experience in responding to all audit enquires pertaining to IT security matters.	Highly Desirable
11.	Demonstrates up-to-date knowledge of the current cyber security trends, threats, solutions and tools.	Highly Desirable
12.	Understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, and common security elements.	Highly Desirable