Unitalent
21-2 Jalan Putra Mahkota 7/7B
47650 Subang Jaya, Selangor, Malaysia
Tel: +6012-5227761
Website: www.unitalentcareer.com
Email: resume@unitalentcareer.com
JTK Licence : JTKSM014

VACANCY NOTICE

POSITION : MANAGER, INFRASTRUCTURE & CYBERSECURITY RISK
LOCATION : Kuching, Sarawak (Malaysia)
INDUSTRY : Education
TYPE : Fixed Term Contract
REF : C27032026/IT

JOB SUMMARY

The position reports to the Director and will be responsible for managing the IT infrastructure and Cybersecurity Risk team.

Responsible for ensuring the University's IT infrastructure and Cybersecurity Risk measures are hardy, secure, and aligned with industry standards to support smooth University's operations of the University. This role involves managing and optimising servers and network infrastructure, implementing cybersecurity frameworks, and leading the IT Infrastructure & Cybersecurity Risk team.

The position requires a proactive thought process and approach to maintain highly available, scalable, and secured University's IT assets. Additionally, this manager will support the Director of Information Technology in strategic decision-making, particularly in infrastructure planning, technology upgrades, and security protocol implementation.

- Design, implement, and maintain a sustainable IT infrastructure architecture to provide highly available IT hardware and services, including data centers, physical/virtual servers, networking equipment, storage systems, backup, recovery systems and so on. Ensure the infrastructure meets the operational demands of the organisation, and provide continuous support across IT unit.
- Regularly review, analyse, and enhance servers, networking systems, workstations, and other IT assets to ensure high performance, compatibility, and security standards as set out in the relevant IT policies and procedure, market/industry standards/requirements and/or institutional requirements. Oversee timely updates and upgrades to maintain optimal working condition and avoid technical obsolescence.
- Develop and enforce cybersecurity framework and protocols focusing on preventing and mitigating cyber threats and vulnerabilities. Lead and manage cybersecurity monitoring initiatives, including system and network log analysis, to detect, triage, isolate, and respond to suspicious activities proactively. Deep-dive and conduct root cause analysis and implement short-term and long-term remedies to protect University's assets.
- Establish or collaborate with the Director of Information Technology in establishing comprehensive IT policies on infrastructure and cybersecurity governance. Develop procedures and guidelines specific to IT infrastructure, digital asset management and protection, compliance with industry security standards and IT requirements.
- Establish and maintain Service Level Agreements (SLAs) for incident and request management and resolution. Continuously assess and improve/enhance the team's performance in responding to and resolving IT infrastructure-related issues and requests timely.
- Recommend and/or lead initiatives for hardware technology refreshes, upgrades, or replacements to prevent obsolescence and mitigate potential performance and security risks. Advise on and implement the latest updates and technology advancements to ensure that all infrastructure components are upto-date.
- Account for all the IT assets across the University. Oversee the inventory and life cycle of all hardware assets across the University, ensuring accurate records, efficient utilisation, traceability and proper disposal or repurposing as needed.
- Act as a liaison with other departments to facilitate the smooth execution of IT projects including but not limited to infrastructure and hardware and cybersecurity upgrades/refreshes. Communicate technical requirements to relevant stakeholders for coordinated infrastructure management, and IT governance.

- Build a cohesive and skilled infrastructure team, fostering a culture of continuous learning and improvement. Facilitate talent development through coaching, mentoring, and performance management, ensuring team members are equipped and knowledgeable to address emerging infrastructure and cybersecurity challenges.

The University views its IT Infrastructure and Cybersecurity Risk posture as critical strategic assets that safeguard its mission and stakeholders. The position will demonstrate a strong commitment to delivering secure, resilient, and high-performing IT services, while proactively managing infrastructure and cybersecurity risks to ensure continuity, compliance, and trust.

Key Responsibilities 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.

1) LEADERSHIP

- Provide strong leadership, supervise, encourage and support the work of subordinates within the IT Infrastructure and Cybersecurity Risk, including setting professional standard for the staff.
- Ensure that staff within the IT Infrastructure and Cybersecurity Risk are properly trained and provide guidance for them to carry out their duties effectively and efficiently.
- Plan and set performance goals for the staff within the IT Infrastructure and Cybersecurity Risk and monitor performance of the staff within the IT Infrastructure and Cybersecurity Risk.
- Provide leadership in the support of developing staff skill sets and certification competencies in relevant areas, aligning with the University direction.
- Develop IT Infrastructure and Cybersecurity Risk plans, aligning to divisional and University targets and plans

2) IT MANAGEMENT

- Provide strong technical and management leadership, direction, and expertise in the area of IT Infrastructure and Cybersecurity Risk and the University to ensure that its goals, policies and operations are supported effectively and efficiently.
- Manage and carry out digital transformation projects for the University including project planning, execution, progress reporting and etc. Ensure operation excellence in IT infrastructure and Cybersecurity Risk.
- Develop and maintain enterprise architecture, Cybersecurity and risk programs/framework/measures/tools, periodically review and implement in supporting the University objectives.
- Ensure the effective management of the IT assets for the University including effective security and backup, software licensing compliance, effective maintenance and support and compliance with relevant policies and regulations.
- Evaluate performance and effectiveness of the areas directly under the control of the Manager, Infrastructure and Cybersecurity Risk and ensure improvements are implemented whenever possible.
- Provide leadership and advice in the selection and implementation of enterprise mission critical applications.
- Develop annual and mid to long term IT Infrastructure & Cybersecurity Risk budgets for operational and capital expenditures, ensuring a sustainable resource planning

3) MANAGEMENT AND PLANNINGOF IT SERVICES & ACTIVITIES

- Develop and update the policies and procedures pertaining to the IT Infrastructure & Cybersecurity Risk to ensure the department meets the needs of management and staff of the University.
- Plan, organise, lead, and monitor the implementation and effective operation of the department's activities and services.

- Ensure that the services and activities planned are in accordance with government rules and regulations.
- Provide project management advice and expertise as required.

4) SET DIRECTION

- Provide advice on the development of the department functions for the Director, Information Technology, PVC&CEO (Sarawak), Executive Group, Board Committees, Board of Directors, and University Council.
- Help to strategically position the University as a major university in Malaysia through the development of adequate IT Infrastructure and Cybersecurity Risk.
- Develop a technology roadmap and direction, align to the University objectives.

5) RESOURCE MANAGEMENT

- Ensure that accurate information is available for use by the Executive Group, Board Committees, Board of Directors and University Council.
- Be proactive in finding solutions for any problems relating to IT Infrastructure and Cybersecurity Risk matters and improve on work processes.
- Ensure resources, both financial and human capital, are planned, managed, and prioritise effectively, and strategically.

6) LIAISON AND INTERACTION

- Liaise with relevant government authorities and statutory bodies in complying with the rules and regulations.
- Liaise, and interact with other external parties such as contractors and vendors, on relevant matters.
- Ensure able to negotiate with external parties such as contractors and vendors, so as to obtain the best value in services and products.
- Ensure good communication interaction with internal parties, and stakeholders to ensure issues are actively managed and resolved, including within own department.

7) CUSTOMER SERVICE

- Collaborate with internal and external customers to better understand, anticipate and meet the current and future needs of the branch campus university and its students in accordance with organisational expectations.
- Implement high quality processes that document, assess, improve and deliver favourable service performance.
- Be accessible for client enquiries; and respond to clients in a timely manner.
- Ensure the staff provide a friendly, helpful and responsive service to internal and external customers
- Provide accurate information, educate and advise the staff on the department policies and procedures.
- Respond to any queries in a timely and polite manner.

8) REPORTS

- Prepare and provide accurate reports on the relevant information as and when needed by the Management.

9) AUTHORITY

- Plan, manage, and approve department expenses in accordance with the budget.
- Approve annual leave, overtime claims, travelling claims, and other claims within the department.
- Recommend travelling, training and development, and promotion of the staff within the department as appropriate.
- Ensure proper authorisation is obtained in accordance with University policies and procedures.
- Authority as mandated in University policies and procedures

JOB REQUIREMENTS

- A Bachelor's degree in Computer Science, IT or other relevant discipline from a recognised institution.
- Recognised certifications in any of these areas: security, Cisco professional, CISSP, CISM, CompTIA), Microsoft, project management, and any other relevant domains
- At least five (5) years of relevant working experience in the areas of network operations, support, systems and infrastructures, cybersecurity, technical services domain or extensive experience as a manager of a substantial technical services units in a medium to large enterprise with a proven record of providing quality service and at least two (2) years of experience in a leadership role.
- Knowledge of current rules and regulations governing IT (including privacy, security and software licensing) and its current trends.
- Have hands-on experience and knowledge of the operations and maintenance of IT infrastructure including systems, networks, cloud, storage, disaster recovery and facilities.
- Substantial experience in the management of Active Directory, VMware/Hyper-V, Azure AD, Office 365, RedHat and etc.
- Substantial experience in networking using CISCO systems including implementation of router, switches, WiFi, firewall, identity access management and etc.
- Experience in the set-up and maintenance of IT infrastructure including servers, PC hardware and other IT related hardware.
- Experience in the management of disaster recovery including development of backup and recovery policies, procedures and processes.
- Experience in executing IT infrastructure or enterprise information system projects on enterprise level.

TO APPLY

1. Applications should include with their application **a detailed CV** indicating qualifications, experience and other matters considered relevant to the application.

2. The application must also include a separate document addressing each applicable element of the Key Selection Criteria ***(As per attached below)***

3. Copy of all your academic certificates (compile all in one file)

4. Email your application to resume@unitalentcareer.com or whatsapp to +012-5227761

Key Selection Criteria
The application should include a separate document addressing each applicable element of the Key Selection Criteria, describing with evidence, how the applicant fulfils the essential and desirable criteria appropriate to the position being targeted.

	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, IT or other relevant discipline from a recognised institution.	Essential
2.	Recognised certifications in any of these areas: security, Cisco professional, CISSP, CISM, CompTIA), Microsoft, project management, and any other relevant domains.	Essential

	Experience / Knowledge / Attributes: Required by the appointee to successfully perform the positions key responsibilities.	**Essential/ Highly Desirable / Preferable**
1.	At least five (5) years of relevant working experience in the areas of network operations, support, systems and infrastructures, cybersecurity, technical services domain or extensive experience as a manager of a substantial technical services units in a medium to large enterprise with a proven record of providing quality service and at least two (2) years of experience in a leadership role.	Essential
2.	Knowledge of current rules and regulations governing IT (including privacy, security and software licensing) and its current trends.	Essential
3.	Have hands-on experience and knowledge of the operations and maintenance of IT infrastructure including systems, networks, cloud, storage, disaster recovery and facilities.	Essential
4.	Substantial experience in the management of Active Directory, VMware/Hyper-V, Azure AD, Office 365, RedHat and etc.	Essential
5.	Substantial experience in networking using CISCO systems including implementation of router, switches, WiFi, firewall, identity access management and etc.	Essential
6.	Experience in the set-up and maintenance of IT infrastructure including servers, PC hardware and other IT related hardware.	Essential
7.	Experience in the management of disaster recovery including development of backup and recovery policies, procedures and processes.	Essential
8.	Experience in executing IT infrastructure or enterprise information system projects on enterprise level.	Essential
9.	Have excellent interpersonal and organisational skills, pleasant personality, and a good team player.	Essential
10.	Experience in developing and managing financial and human resources to ensure sustainability, aligning to university objectives.	Essential
11.	Have experience in developing, managing and motivating staff and managing vendors and contractors.	Essential
12.	Experience in good report writing skills, business analysis, risk assessment, and able to make sensible and logical recommendations.	Essential
13.	Some working experience in higher education institutions will be highly desirable.	Highly Desirable
14.	Experience in the management of enterprise applications, or some experience in the use of and management of a learning management system (LMS) and student information system (SIS).	Highly Desirable
15.	Have experience in formulating the policies and procedures of information technology usage, and providing for its internal controls and security.	Highly Desirable