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 License: JTKSM014

VACANCY NOTICE

POSITION : **MANAGER - CYBERSECURITY AND RISK**
LOCATION : Kuching, Sarawak
INDUSTRY : Education
TYPE : Fixed-Term Contract
REF : C22102026/IT

JOB SUMMARY

The position reports to the Director, Information Technology and is responsible for managing the IT Cybersecurity & Risk team.

The primary purpose of this role is to drive the strategic cybersecurity posture, defend against evolving threat landscapes, and oversee governance, risk management, and compliance (GRC) frameworks across the University.

The position is responsible for ensuring the digital assets, systems, and security measures are robust, resilient, and fully aligned with national and international standards.

This role involves developing and overseeing the University's cybersecurity strategy and long-term roadmap, implementing security frameworks (such as ISO 27001, NIST, and COBIT), managing SIEM monitoring and endpoint protection frameworks, leading vulnerability management programs, and serving as Lead Incident Handlers during major security breaches.

Additionally, the Manager will support the Director of Information Technology in strategic decision-making, enterprise-wide IT risk assessments, maintaining the corporate risk register, enforcing security governance policies, and managing relationships with key security partners and auditors.

The University views its Cybersecurity and Risk Management posture as a critical strategic asset that safeguards its mission and stakeholders. The position will demonstrate a strong commitment to delivering secure, resilient, and compliant IT environments while embedding a University-wide culture of security awareness and data privacy.

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's activities.

1) **Leadership**
   - Provide strong leadership, supervise, encourage, and support the work of subordinates within the IT Cybersecurity & Risk unit, including setting professional security standards for staff.
   - Ensure staff within the Cybersecurity & Risk unit are properly trained and provide guidance for them to carry out their security monitoring, GRC, and incident response duties effectively.
   - Plan and set performance goals for the cybersecurity staff and monitor performance against established operational KPIs and security metrics.
   - Provide leadership in developing staff skill sets and professional certification competencies (e.g., CISSP, CRISC, CISA, CEH) aligning with University directions.
   - Develop IT Cybersecurity & Risk plans and operational roadmaps aligning to divisional and University targets.
   - Drive cultural change across the organisation to prioritize data privacy, cybersecurity vigilance, and security awareness at all levels.

2) Technical Skills & Security Governance

Strategic Security Leadership & Operations:

- Develop and oversee the University's cybersecurity strategy and long-term roadmap to ensure alignment with institutional goals.
- Manage and optimise the effectiveness of daily security operations, SIEM monitoring, log analysis, Next-Gen firewalls, Endpoint Detection & Response (EDR), and Data Loss Prevention (DLP) frameworks.
- Direct the University's vulnerability management program, ensuring timely vulnerability identification, risk prioritisation, remediation, and patching across enterprise assets.

Incident & Risk Governance:

- Serve as the Lead Incident Handlers for major security breaches, coordinating cross-departmental responses, forensic analysis, root-cause remedies, and legal/regulatory reporting.
- Lead enterprise-level IT risk assessments for ongoing and new digital initiatives, providing recommendations on risk mitigation and maintaining the corporate IT risk register.
- Establish and enforce standardised Security Operating Procedures (SOPs) and security baseline guidelines to maintain a resilient defense posture.

3) Policy and Planning

- Formulate, implement, and periodically update comprehensive IT security policies and procedures to ensure the unit meets management, staff, and institutional needs.
- Ensure institutional compliance with national and international security standards and governance frameworks (e.g., ISO 27001, NIST, COBIT, PDPA).
- Liaise with internal and external auditors to ensure SUTS satisfies all regulatory, government, and security audit requirements.
- Provide project management advice and cybersecurity expertise for enterprise projects across the University

4) Set Direction

- Provide expert advice on cybersecurity and risk management functions for the Director, Information Technology, PVC&CEO (Sarawak), Executive Group, Board Committees, Board of Directors, and University Council.
- Help strategically position the University as a resilient and secure digital university in Malaysia through effective cybersecurity defenses and GRC practices.
- Develop a long-term technology security roadmap aligned with evolving cyber threats and University objectives.

5) Resource and Budget Management

- Develop, justify, and manage annual and mid-to-long term cybersecurity operational and capital budgets, ensuring sustainable resource planning and software/tool license renewals.
- Ensure resources (both financial and human capital) are planned, managed, and prioritized effectively and strategically.
- Be proactive in finding solutions for any problems relating to IT cybersecurity and risk matters and improve on work processes.

6) Liaison and Vendor Management

- Liaise with relevant government authorities, statutory bodies, and regulatory agencies regarding cyber compliance and data protection laws.
- Negotiate high-level contracts and manage key relationships with security vendors, contractors, and service providers to ensure optimal service delivery and best value.
- Maintain good communication and interaction with internal parties and stakeholders to ensure security risks are actively managed and resolved.

7) **Customer Service**
   - Demonstrate organsation Values and collaborate with internal and external customers to better understand, anticipate, and meet current and future security and compliance needs.
   - Implement high-quality processes that document, assess, improve, and deliver favorable service performance.
   - Ensure the cybersecurity team provides a friendly, responsive, and professional service, providing accurate security guidance to staff and students.

8) **Report**
   - Prepare and provide accurate board-level reports, risk metrics, and cybersecurity status updates as and when required by 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.

10) **Occupational Safety and Health (OHS)**
   - Support management in the implementation and improvement of OHSMS, and ensure Unit operations comply with relevant OHS legislation and rules.

11) **Organization Values and Culture**
   - Commit to the organizations values.
   - Conduct work professionally while demonstrating the organization's values at all time.
   - Assist management in implementing the organization culture and lead the team in embracing the organization Values.

12) **Other Duties**
   - Any other duties as and when is required by the Director, Information Technology; or PVC&CEO (Sarawak); or any other person as assigned by an authorised personnel.

JOB REQUIREMENTS

- A Bachelor's degree in Computer Science, IT, Cybersecurity, or relevant discipline from a recognised institution.
- Higher level qualification can be considered.
- Possess at least Two (2) relevant IT certification(s) in active status with minimum one at professional cybersecurity level (e.g. CISSP, CRISC, CISA, CISM, CEH, PMP, Prince2, ITIL, CompTIA Security+ or equivalent).
- Minimum of five (5) years of relevant work experience, and minimum of two (2) years of experience in a leadership role or management experience in Cybersecurity operations, Governance, Risk, and Compliance (GRC), or Information Security management in a small to medium enterprise.
- Strong knowledge of IT governance principles, regulatory requirements, risk management, and cybersecurity best practices. Proven experience with frameworks such as ISO 27001, NIST, and COBIT.
- Proven leadership in conducting enterprise-level IT risk assessments and maintaining a comprehensive corporate risk register.
- Extensive experience in managing cybersecurity incidents (Incident Response Lead/Commander) and conducting root cause analysis.
- Hands-on experience with security technologies including SIEM, Next-Gen Firewalls, Endpoint Detection & Response (EDR), DLP, and Vulnerability Scanners.

- Advanced organisational skills, with the ability to draft board-level reports, risk assessment recommendations, and University-wide security policies.
- Strong team leadership skills, with a track record of developing, managing, and motivating staff and managing vendors and contractors.
- Knowledge of local data protection laws (e.g., PDPA) and their practical application in an educational or enterprise setting.
- Some working experience in higher education institutions will be highly desirable.
- Familiarity with IT infrastructure, cloud computing, networking, and web technologies from a security defense perspective. Hands-on experience with ITSM tools is an advantage.

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 pdf file).

4. Email your application to resume@unitalentcareer.com or WhatsApp to +6012-5227761.

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, IT, Cybersecurity, or relevant discipline from a recognised institution. Higher level qualification can be considered.	Essential
2.	Possess at least Two (2) relevant IT certification(s) in active status with minimum one at professional cybersecurity level (e.g. CISSP, CRISC, CISA, CISM, CEH, PMP, Prince2, 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.	Minimum of five (5) years of relevant work experience, and minimum of two (2) years of experience in a leadership role or management experience in Cybersecurity operations, Governance, Risk, and Compliance (GRC), or Information Security management in a small to medium enterprise.	Essential
2.	Strong knowledge of IT governance principles, regulatory requirements, risk management, and cybersecurity best practices. Proven experience with frameworks such as ISO 27001, NIST, and COBIT.	Essential
3.	Proven leadership in conducting enterprise-level IT risk assessments and maintaining a comprehensive corporate risk register.	Essential
4.	Extensive experience in managing cybersecurity incidents (Incident Response Lead/Commander) and conducting root cause analysis.	Essential
5.	Hands-on experience with security technologies including SIEM, Next-Gen Firewalls, Endpoint Detection & Response (EDR), DLP, and Vulnerability Scanners.	Essential
6.	Advanced organisational skills, with the ability to draft board-level reports, risk assessment recommendations, and University-wide security policies.	Essential
7.	Strong team leadership skills, with a track record of developing, managing, and motivating staff and managing vendors and contractors.	Essential
8.	Knowledge of local data protection laws (e.g., PDPA) and their practical application in an educational or enterprise setting.	Highly Desirable
9.	Some working experience in higher education institutions will be highly desirable.	Highly Desirable
10.	Familiarity with IT infrastructure, cloud computing, networking, and web technologies from a security defense perspective. Hands-on experience with ITSM tools is an advantage.	Preferable