**JOB DESCRIPTION**

This form summarises the purpose of the job and lists its key tasks.

It may be varied from time to time at the discretion of the College in consultation with the postholder.

|  |  |
| --- | --- |
| **Job Title:** Head of Cyber Security and Governance | **Job ref no:** ISD-0342-24 |
| **Grade:** 8 | **Department:** Infrastructure Services Directorate |
| **Accountable to:** IT Director | **Responsible for:** Cyber Security Architect |

|  |
| --- |
| **Job summary:**  The Head of Cyber Security and Governance is responsible for developing and implementing RVC's cyber security strategy and governing IT policies, to ensure the protection of information assets whilst maintaining compliance with relevant regulations. This role involves leading the cyber security team, managing risks and IT policies and procedures, and fostering a culture of security awareness across the RVC. |

|  |
| --- |
| **Competency: Strategic Leadership**  **Key tasks:**   * + Develop and implement a comprehensive cyber security strategy aligned with RVC’s strategic objectives.   + Lead the cyber security team, providing direction, support, and professional development opportunities.   + Ensure RVC’s cyber security posture is robust and resilient. |
| **Competency: Risk Management**  **Key tasks:**   * + Identify, assess, and manage cyber security risks.   + Develop and maintain a risk management framework and ensure regular risk assessments are conducted.   + Implement measures to mitigate identified risks and monitor their effectiveness. |
| **Competency: Compliance and Governance**  **Key tasks:**   * + Ensure compliance with relevant legislation, regulations, and standards (e.g., GDPR, ISO 27001).   + Develop and maintain cyber security policies, procedures, and standards.   + Conduct regular audits and assessments to ensure compliance and identify areas for improvement. |
| **Competency: Incident Response**  **Key tasks:**   * + Develop and maintain an incident response plan.   + Lead the response to cyber security incidents, ensuring timely and effective resolution.   + Conduct post-incident reviews and implement lessons learned. |
| **Competency: Security Awareness and Training**  **Key tasks:**   * + Promote a culture of security awareness across the RVC.   + Develop and deliver cyber security training programs for staff and students.   + Provide guidance and support on cyber security best practices. |
| **Competency: Stakeholder Engagement**  **Key tasks:**   * + Build and maintain strong relationships with internal and external stakeholders.   + Communicate effectively with senior management, staff, and students regarding cyber security issues and initiatives.   + Collaborate with academic and administrative departments to address their cyber security needs. |
| **Competency: Innovation and Improvement**  **Key tasks:**   * + Stay abreast of emerging cyber security threats, technologies, and trends.   + Foster a culture of innovation and continuous improvement within the cyber security team.   + Implement new technologies and practices to enhance RVC’s cyber security posture. |
| Flexibility:  To deliver services effectively, a degree of flexibility is needed, and the post holder may be required to perform work not specifically referred to above. |