

Job Title	Information Security Officer
Reports To	Security Resilience (Identity, Data and Systems) Manager
Grade	Grade 4

Purpose	<p>The primary functions of the Information Security Officer will be to assist with the coordination of undertaking security support duties for IT projects and other Cyber project initiatives. The role will ensure IT projects adhere to security policies, secure architecture principals and conform to and regulatory cyber assessment framework. The suitable candidate will provide relevant, timely, credible information and sound professional advice to their immediate team and other Cyber Resilience representatives concerning IT's information security risk profile.</p>
Key Accountabilities	<ul style="list-style-type: none"> • Support the activities associated with Information Security on all non-CAF based IT projects. • Deliver the relevant security artifact requirements for each IT Project quality gate. • Document and log security assessments and penetration testing where required. This will also include arranging penetration test engagements and code reviews for in flight and new projects. • Report on all security incidents and risks identified within IT projects. • Evaluate and co-ordinate tickets assigned by IT / WWU employees to the security team within WWU IT's ticketing system. • Log and manage any control defects or failures identified via the SecOps ticket tracking system. • Provide security support into other WWU projects and ongoing programmes of work, on both a planned and adhoc basis • Support the review of existing systems security operations capabilities, and drive improvements for all technical and administrative controls. • Work closely with Security Operations to ensure the SecOps team are made aware of any defects, failed controls or risks identified. • Assist where required in any unplanned adhoc information security duties.

Technical Know-How & Skills	<ul style="list-style-type: none"> • Passionate about information security with energy and drive to improve WWU’s information security posture. • A good understanding of cloud concepts, particularly hybrid cloud. Experience with private cloud technology, particularly VMWare and public cloud technology Microsoft Azure is essential. • Understanding of project management methodologies (Waterfall, Agile, PRINCE2) is necessary. • Knowledge of cyber attack modelling techniques used to investigate and analyse breaches and IoA’s • Strong knowledge of leading endpoint detection and threat management products. • Knowledge of network security particularly around networking behaviour analytics and NAC. • Strong commercial acumen and vendor management. Ability to understand and translate between technical and business language where necessary. • Willing to continuously improve and ensure an ‘excellent’ service is always provided to the Cyber Resilience team customers. • Strong knowledge of information security control and compliance standards such as the NCSC CAF, ISO27002, IEC17789, CIS CSC and NIST CSF • A good understanding of CSIRT and incident response process and procedures. Experience working with recognised incident response providers would be an advantage. • A good understand of Microsoft Defender products and Microsoft Sentinel would be advantageous.
Qualifications	<ul style="list-style-type: none"> • CISM (Essential) • SC-900, AZ-900 (Essential) • CISM (Advantageous but not essential) • SC-200, SC-300, SC-400 and AZ-500 (Advantageous but not essential)
Job Dimensions	<p>People Management – The role holder will not have any direct reports, however will be expected to update all relevant stakeholders on the Information Security BAU activities and liaise with other Cyber Resilience team members. Reports officially to the Security Resilience (Identity, Data and Systems) Manager.</p> <p>Vendor Management – No direct vendor management. The role holder will liaise with multiple high value vendors within the Cyber and IT divisions.</p> <p>Budget Management – No budget management requirements. Knowledge of Opex, Capex, Regex and general procurement processes would be beneficial.</p>