Job Title	Cyber Security Architect
Department	Cyber
Reports to	Senior Cyber Security Architect
Grade	Technical Tier 2
Purpose & Overview	To design and implement a robust enterprise-wide cyber security architecture function within WWU and assisting with the formation and planning of a multi-year Cyber Security Strategy.
Key Accountabilities	• Define, document, and embed a set of Security Architecture Principles that will guide all WWU Projects, Programmes and Changes • Define, document, and embed a complete set of ISO27001 compliant Security Policies, and associated ISMS • Develop Reference Architecture and all associated architecture models for Identity Management and Privileged Account Management • Consult on and input into the redevelopment and regular testing of WWU's Security Incident Response Plan (for both Cyber IT and Cyber OT) • Inputs to the strategic planning and oversight of a rolling five-year Enterprise Security Strategy that takes into account changing threat landscapes, evolutionary attack methodologies and evolving technological obsolescence of WWU's digital estate Develop, in conjunction with the Head of Cyber Resilience and the Senior Security Manager, a set of KPI's linked to WWU Enterprise Strategy and production of a Monthly KPI Report • Provide Security Architecture consultancy into other WWU projects and ongoing programmes of work, on both a planned and ad-hoc basis • Put in place a process that ensures all new systems (and architecturally significant changes to existing systems) have Security Architecture Reviews • Work closely with the Strategy and Architecture Team to ensure alignment with EA • Work with the Cyber Security Team to set up the team's processes and frameworks • Lead on a number of Cyber IT and OT defined projects.
Technical Know-How & Skills	• Experience with AppSec • Experience with Azure cloud and Microsoft security stack • On-premises architecture and Virtualization • Experience of use-case analysis • Experience of systems modelling and design using UML

	• Experience of modelling security architecture using Archimate or similar tools • Experience of using architecture modelling software (e.g., Enterprise Architect) • Familiarity with User Behavioural Analysis • Hands on experience of driving an enterprise security maturity improvement program • Skilled in reviewing and analysing whether security controls for any given system are suitable, using relevant attack modelling methodologies. • Develop repeatable, re-usable security architecture components, models and patterns • Experience of drafting Security Solutions Design documentation sets • Strong experience in Identity Management and the evaluation of access models (inc. SSO, MFA, RBAC, ABAC, eIDV etc) • Strong knowledge of and the ability to put into practice global Information Security Standards including ISO27002, CIS and NIST CSF
Qualifications	• CISSP Security Architectural qualifications, such as: • SABSA SCF or SCP, • CISSP-ISSAP, • GDSA • General (non-Security) Architectural and IT Governance Qualifications, EG, within TOGAF, COBIT, etc.
Additional Information	Vetting required – We require candidates to hold SC Clearance for this role. WWU will sponsor candidates who do not already hold SC Clearance through the process. Please note, however, that failure to attain or maintain SC Clearance during your tenure within this role, will be grounds for termination. Typically, this requires that candidates are either UK Nationals, or, have been resident in the UK for a minimum of five years and hold indefinite Right to Remain. Further details of what SC Clearance entails can be found at: https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels