Job Title	Security Resilience (Identity, Data & Systems) Manager
Department	Cyber Resilience Team
Reports to	Head of Cyber Resilience and Physical Security
Grade	Personal Contract
Purpose & Overview	– The Security Resilience Manager in Wales & West Utilities (WWU)'s Cyber Resilience Team is a leadership role responsible for overseeing and managing protective security measures to safeguard WWU's data, information assets and critical systems. – The role holder will be fully accountable and responsible for all areas under the Cyber Assessment Framework (CAF) Principal B – Working alongside internal teams across WWU, this role plays a crucial part in establishing a comprehensive protective security program, implementing strategies to mitigate cyber threats and delivering strong cyber resilience in WWU. – Reporting to the Head of Cyber Resilience and operating in line with the WWU Cyber Security Strategy, the Security Resilience Manager is responsible for shaping and executing protective security strategies, implementing robust protective security measures and fostering a culture of security awareness. – Strong leadership skills, technical expertise and effective collaboration are essential attributes for this critical role.
Key Responsibilities	– Develop and execute a strategic vision for protective security aligned with the WWU's cyber security strategy. – Collaborate across WWU to integrate protective security into the overall business strategy. – Develop and implement protective security policies, procedures and guidelines related to WWU's role as an OES. – Maintain compliance with legislation, sector-specific regulations and industry standards. – Support the design and implementation of protective security measures relevant to WWU's IT and OT estate, across the domains of security policy and procedures, identity and access management, security architecture and resilient system design, data security, and ensuring enterprise wide security awareness and training plans are in place. – Deliver oversight of relevant security controls across WWU's network. – Develop and maintain incident response plans specific to protective security-related incidents. – Support, as appropriate, the response to incidents, working collaboratively across WWU in order to contain and mitigate security incidents. – Demonstrate leadership in the support and implementation of security awareness and training programmes. – Foster a culture of security awareness and accountability throughout the organisation. – Collaborate with the physical security team to integrate protective security measures within physical security controls. – Support the deployment of a holistic approach to security in WWU, that considers both cyber and physical threats. – Support the assessment and management of security risks associated with third-party vendors and partners. – Collaborate with internal teams (e.g. IT) to ensure vendors adhere to established security standards. – Establish and maintain a robust security governance framework. – Ensure that security initiatives align with the UK regulatory environment and with relevant industry standards.

	– Analyse security incidents, providing insights and recommendations for improvement as required. – Create regular reports for senior stakeholders as required. – Be prepared to collaborate with other teams within WWU's Cyber Resilience and IT Teams, including incident response, threat intelligence, disaster recovery and business continuity.
Technical Skills	– Certified Information Systems Security Professional © (CISSP) – Certified Global Industrial Cyber Security Professional © (GICSP) – A working knowledge and experience of cyber risk management standards including IEC62443 – Team management experience in a cyber security function. – Experience of matrix management in a complex and dynamic operating environment. – Strong technical skills across a broad range of security domains
Qualifications	<u>Essential</u>: – Significant cyber security experience ideally some of which has been spent in Critical National Infrastructure environments. – Proven experience in leadership roles within systems security, security operations, identity management and infrastructure and data protection within a cyber security environment. – In-depth knowledge of cyber threats, cyber incident management and risk management. – Strong communication and interpersonal skills. <u>Desired</u>: – Strong peer network, and involvement in Sector specific cyber security groups such as E3CC.
Additional Information	– The role holder will be required to be vetted to 'Security Cleared' Level and maintain this clearance. – The role holder will be required to deputise for the Head of Cyber Resilience when required.