Job Title	Security Culture Specialist
Department	Cyber Resilience
Reports to	Cyber Risk Management Manager
Grade	Graduate
Purpose & Overview	– The Security Culture Specialist (Security Awareness, Training and Exercising) in Wales & West Utilities (WWU)'s Cyber Resilience Team is responsible for developing and implementing programs to educate and train employees on cyber security best practice, focused on improving security behaviours, fostering a security first culture and reducing human cyber risk. – They will be responsible for managing the development and delivery of engaging content and activities to raise cyber awareness across all Departments within WWU. – This role will lead on developing the wider Cyber Culture to reduce and mitigate human cyber risk. – The role is also the lead for delivering appropriate crisis management exercising at bronze, silver and gold team level. – The primary goal is to enhance WWU's overall security posture by fostering a culture of awareness and accountability among staff members. – This role is instrumental in building a resilient cyber security culture within WWU, by developing effective training programs and developing enhanced awareness, employing innovative and novel technologies to support the mission. – This crucial role will lead in protecting WWU's most sensitive data through strong communication skills, creativity, originality and a commitment to continuous improvement.
Key Responsibilities	– Design, develop and implement a tailored, measurable cyber security awareness and training programme that addresses the specific needs of, and risks to, WWU. – Plan, research, and create high-quality cybersecurity awareness communications deliverables such as presentations, talking points, videos, emails, articles, compelling images/infographics, web content, and online training. – Lead the development and implementation of comprehensive data and analytics to assess the effectiveness of the Cyber Culture training and make recommendations for continuous improvement. – Communicate with leadership teams across WWU to gain support for cybersecurity awareness initiatives and develop communication strategies to foster a cybersecurity-aware culture. – Maintain awareness of changes in regulations and compliance and the impacts. Ensure campaigns and content comply with relevant compliance requirements. – Create M.I Reports to identify trends and concerns linked with Cyber Security and develop training materials based on this.

	– Deliver engaging and informative content that covers topics such as phishing awareness, password hygiene, data protection and social engineering within a CNI context. – Oversee learning modules employing innovative, engaging and original material wherever possible. – Organise and deliver annually, in house or via 3rd parties, crisis management exercising at bronze, silver and gold team level, ensuring scenarios are severe but plausible, to maximise the value gained by participants. – Ensure training content is tailored to different audience groups, customising material for technical and non-technical staff. – Plan and execute simulated phishing campaigns to assess WWU colleagues' susceptibility to phishing attacks, improving resilience over time. – Analyse results to identify trends, areas of improvement and potential risks. – Communicate cyber security policies and procedures to WWU colleagues in a clear and accessible manner. – Ensure that colleagues understand the rationale behind security policies and their role in maintaining a secure environment. – Establish key performance indicators (KPIs) to measure the effectiveness of the security awareness and training programme. – Generate regular reporting on training completion rates, phishing simulation results and overall improvements in behaviour and sentiment towards security awareness. – Work with the relevant IT and HR teams to integrate cyber security training into onboarding processes. – Be an advocate for a positive security culture throughout WWU. – Be WWU's subject matter expert on the latest cyber security threats, trends and best practices. – Ensure training material remains relevant to reflect the evolving cyber security landscape and emerging risks. – Establish feedback mechanisms from employees to continuously improve training content and delivery methods. – Record and implement lessons learned from security incidents where appropriate, to enhance training programmes.
Technical Skills	– Significant experience in a similar role, ideally some of which has been spent in a CNI environment. – Experience of working in a security awareness and training environment delivering solutions to large organisations.
Qualifications	<u>Essential</u>: – Proven experience in developing and delivering cyber security awareness and training programmes. – A strong awareness of innovative learning platforms. – Strong communication and presentation skills. – Understanding adult learning principles and instructional design. – Knowledge of phishing techniques and social engineering. <u>Desired</u>: – Bachelor's or Master's degree in Cybersecurity or related field. – Other relevant cyber security certifications

Additional Information	– Vetting