Job Title	Industrial Control Systems (ICS) Security Officer
Department	Cyber Resilience Team
Reports to	Industrial Control System Security Manager
Grade	Technical Tier 1
Purpose & Overview	– The Industrial Control Systems (ICS) Security Officer in Wales & West Utilities (WWU)'s Cyber Resilience Team is a specialised role focused on ensuring the security and resilience of industrial control systems, including supervisory control and data acquisition (SCADA) systems and other critical infrastructure. – This role involves developing and implementing security measures to protect industrial environments from cyber threats and overseeing the reliability and safety of operational technology (OT) assets. The ICS Security Officer plays a crucial role in maintaining the cyber resilience of critical industrial processes. – Reporting to the Industrial Control System Security Manager, this is a critical role within the Cyber Resilience Team, dedicated to ensuring the security and resilience of industrial control systems. By implementing robust security measures, collaborating across the IT and OT domains, the ICS Security Officer contributes to the safety, reliability and cyber resilience of critical industrial processes. – Strong technical expertise, knowledge of ICS security principles and effective communication are essential for success in this role.
Key Responsibilities	– Develop and execute the ICS security strategy, aligning it with overall cyber security and business objectives. – Collaborate with key stakeholders to understand operational requirements and constraints. – Conduct risk assessments for ICS environments to identify and prioritise potential security vulnerabilities. – Implement measures to mitigate identified risks, ensuring the safety and reliability of industrial processes. – Design and implement security architectures for industrial control systems, incorporating robust security controls and access management. – Ensure the integration of security measures without compromising operational efficiency. – Develop and maintain incident response plans specific to ICS environments. – Lead incident response efforts in collaboration with IT and OT teams to minimise downtime and ensure the integrity of industrial processes. – Implement and manage security controls for SCADA systems and other critical components of ICS environments. – Monitor and analyse SCADA communications for anomalies and potential security incidents. – Assess and manage the cyber security risks associated with third-party vendors providing ICS components and services. – Collaborate with procurement and IT teams to ensure secure integration of third-party ICS solutions.

	– Ensure compliance with relevant regulations and standards specific to ICS security, such as NIST Cyber Security Framework, IEC 62443 and other industry-specific guidelines. – Stay informed about evolving regulatory requirements. – Implement network segmentation and isolation strategies to limit the impact of security incidents on critical ICS components. – Design secure network architectures that prioritise operational requirements. – Be prepared to develop and deliver security training programs for personnel working with ICS components. – Promote a culture of security awareness and best practice within the OT environment. – Implement continuous monitoring solutions for ICS environments, leveraging available threat intelligence to detect and respond to emerging threats. – Stay abreast of ICS-specific threats and vulnerabilities. – Collaborate with both operational technology (OT) and information technology (IT) teams to ensure a holistic and integrated approach to cyber security. – Facilitate communication, collaboration and cooperation between OT and IT environments. – Maintain comprehensive documentation of ICS security measures, configurations and incident response procedures. – Generate regular reports for senior leaders as required.
Technical Skills	– Significant experience in a similar role, ideally some of which has been spent in a CNI environment.
Qualifications	<u>Essential</u>: – Extensive experience in cyber security roles with a focus on industrial control systems and OT environments. – In-depth knowledge of ICS security principles, standards and protocols. – Strong communication and interpersonal skills for collaboration with cross-functional teams <u>Desired</u>: – Bachelor's or Master's degree in Cyber Security, Industrial Engineering or related field. – Other relevant cyber security certifications
Additional Information	– Vetting