


# Cyber Security Specialist

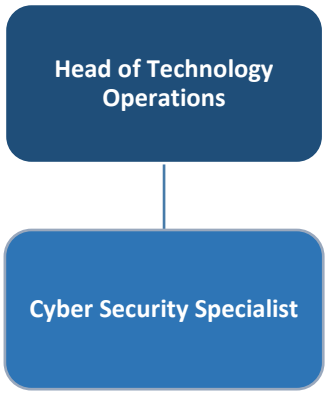
| | | | |
|---|---|---|---|
| **Reports to:** | Head of Technology Operations | | |
| **Group:** | Technology | **Financial Authority:** | As per DFA |
| **Direct Reports:** | 0 | **Revision (m/y):** | 9/2026 |

## Purpose

The role is responsible for configuring, implementing and testing security solutions within WEL's ICT and Operational Technology infrastructure. It maintains robust information security management practices to protect systems against security breaches and reduce the potential impact of cyber-attacks.

As part of WEL's cyber maturity uplift, the role translates security priorities into practical initiatives, operational improvements and assurance activities across IT and OT. This includes governance, risk visibility, vulnerability management, identity and access controls, network security, monitoring, incident preparedness and secure-by-design delivery, applied in ways that recognise safety, availability and operational requirements.

## Reporting Structure




## Key Accountabilities (Outcomes)

- Support delivery of WEL's cyber maturity uplift roadmap through practical security initiatives, operational improvements and evidence-based assurance activities.




- Configure, implement, test and continuously improve security solutions across enterprise IT and operational technology environments, including industrial control systems and SCADA-related networks and services.
- Contribute to cyber security governance, standards, procedures, risk reporting, control evidence, audit readiness and executive assurance, aligned with WEL's risk appetite and recognised frameworks.
- Strengthen vulnerability and threat management through scanning, monitoring, risk assessment, prioritisation, remediation tracking and reporting across IT and OT assets, using approaches appropriate to operational constraints.
- Support identity and access management controls, including privileged access, authentication, authorisation, access reviews, least privilege and the management of service and emergency access accounts.
- Improve network security and segmentation practices across enterprise and industrial environments, working with technology and engineering teams to protect critical services without compromising safety or availability.
- Improve monitoring, detection, incident response and recovery readiness through effective security tooling, alerting, workflows, playbooks, exercises and lessons learned across IT and OT.
- Apply secure-by-design principles to technology and operational change, advising on security requirements, architecture, implementation options, risk treatment and operational handover.
- Work collaboratively with IT, OT, engineering, project and vendor teams to ensure controls are practical, risk-based and aligned with operational, safety and reliability requirements.
- Support third-party and supplier security assurance through security reviews, control assessments, service oversight and risk-based recommendations.
- Maintain cyber security risks, issues and actions to support prioritisation, accountability and clear progress reporting.
- Promote a security-aware culture through practical guidance, coaching and awareness support for staff, leaders and specialist teams.

## Decision Authority and Scope

| Scope | Role expectation |
|---|---|
| **Owns** | Owns assigned cyber security analysis, technical configuration, testing, documentation and operational outputs, ensuring they are accurate, supportable and aligned with approved standards, procedures and change controls. |
| **Influences** | Influences cyber risk treatment, security architecture, operational readiness and technology change by providing practical advice and working with IT, OT, engineering, project, risk and vendor stakeholders. |




| | |
|---|---|
| **Recommends** | Recommends risk-based improvements to security controls, architecture, operating practices, incident readiness and supplier arrangements across enterprise IT and operational technology environments. |

## Ways of Working (Enterprise Expectations)

These expectations apply to all roles and should be demonstrated through day-to-day behaviour, decision-making and interactions across the business and with external stakeholders.

- Act consistently with WEL's values and contribute positively to organisational performance and development.
- Champion health, safety and wellbeing, and model safe behaviours in all aspects of the role.
- Maintain a strong customer and service focus, supporting reliable delivery and positive stakeholder outcomes.
- Build effective relationships across the business, with contractors, utilities, authorities and other stakeholders to support coordinated operational delivery.

## Capabilities That Matter Most

The role requires strong technical judgement, practical cyber security expertise and the ability to translate security risks into clear advice and effective solutions. Success depends on collaboration, attention to detail, sound stakeholder engagement and the ability to support secure, resilient ICT services.

- Strong cyber security engineering capability across security architecture, operations, network security, identity and access management and secure-by-design principles.
- Sound understanding of information security, IT risk management, security protocols, cryptography, authentication, authorisation and audit practices.
- Practical knowledge of endpoint protection, SIEM, vulnerability management, privileged access management, network security and Linux/Windows platforms.
- Knowledge of operational technology security concepts, including industrial control systems, SCADA, industrial networks, segmentation, remote access, asset visibility and the constraints associated with legacy or high-availability environments.
- Ability to balance cyber security objectives with operational safety, service continuity, reliability and engineering requirements in a critical-infrastructure environment.
- Strong communication, reporting and stakeholder engagement skills, including the ability to work effectively with internal teams and third-party vendors.
- High integrity, professionalism, quality orientation and customer focus, with a proactive approach to continuous improvement.




## Essential Qualifications & Experience

- Relevant tertiary qualification in IT or another relevant discipline, or comparable experience.
- Experience in professional services, cyber security and/or the technology industry.
- Solid experience in information security and IT risk management, including security protocols, cryptography, authentication, authorisation, audit and secure-by-design principles.
- Deep working knowledge of information security tools and techniques across multiple domains, such as security architecture and engineering, security operations, network security and IAM.
- Expert knowledge of endpoint protection, SIEM, identity and access management, vulnerability management, privileged access management and network security.
- Professional working experience on Linux and Windows platforms.
- Knowledge of security governance frameworks, particularly NIST and ISO 27001.

## Desirable Qualifications & Experience

- Experience or strong interest in operational technology, industrial control systems, SCADA, utilities, critical infrastructure or other complex networked environments.
- Understanding of OT security practices such as network segmentation, secure remote access, industrial asset visibility, vulnerability management and incident response in high-availability environments.
- Relevant certification from ISO, $(ISC)^2$, ISACA, GIAC or Microsoft, or training in cloud, networking, firewalls or industrial cyber security.
- Experience working with third-party technology or engineering vendors in regulated or safety-critical environments.

## Role Evolution

This role may evolve as strategy, structure and priorities change.

# Our Purpose

Enabling our
***communities to thrive***

# Our Vision

To create and support an
***innovative and sustainable energy future***

# Best in Service

So we have the
***trust of our community***



# Best in Safety

Every Day - ***Home Safe***



# Our Values

**A** **Agile**

We listen to ideas, we explore opportunities and we adapt to changing situations with an open mind. When change is needed we make sure we understand why and we make it work. We're flexible and we respond professionally to change.

**B** **Build the business**

We make sure our day to day activity is sound while exploring ways to improve the way we work or things we do. We often ask "is there a better way to do this?" and we investigate options.

**C** **Care for each other, the customer and our assets**

We work as a team across the business to do things the right way. We treat others with respect, listening to their needs so we can deliver a reliable and safe service to our communities.

**D** **Do the right thing**

We make decisions with integrity and when we can, we help others make the right decision for their situation. We're open, honest and trustworthy. We speak up if we feel we should and we listen to others.

**E** **Every Day - Home Safe**

We lead by example to keep ourselves, our workmates and our communities safe. We use the right equipment, we challenge unsafe acts and we say no if we think it's not safe.