Position Description

Title	Information Security Analyst		
Group	Finance and Corporate Services	Reports to	Information and Data Manager
Date Prepared	May 2024		

EWON is the industry-based Ombudsman scheme which provides all NSW energy and some water customers with independent, free, informal dispute resolution services. We work towards achieving fair and reasonable complaint outcomes for all parties, provide leading customer service and influence energy and water public policy. We are not a consumer advocate, nor do we represent industry.

Our Purpose

1. Provide high quality, independent advice, information and dispute resolution to NSW energy and water consumers.
2. Use our unique complaints data to enable energy and water providers to improve their customer service, systemically reduce the drivers of complaints and to inform the development of regulations, codes and policy.
3. Engage effectively with NSW consumers, promote our service and the complaints processes of energy and water providers through our community outreach and stakeholder engagement program.

Role Purpose

The Information Security Analyst is responsible for the protection of data, information security engineering and the implementation and monitoring of compliance with EWON's IT policies, cybersecurity framework, standard and procedures. The role also advises the leadership on risk levels and security posture, and provides guidelines on information security for the organisation, working effectively with internal stakeholders as well as cybersecurity partner, IT vendors and managed service providers.

Key Accountabilities

1. Operational Effectiveness	• Monitor, identify and assess cyber security issues and threats including breaches and potential intrusion incidents • Ensure the security of EWON's data and backup data of information systems and networks • Troubleshoot network and connectivity issues and provide solutions to minimise disruptions to the business
2. Threat Monitoring, Analysis & Reporting	• Investigate threats and vulnerability reports, coordinate remedial activities with IT vendors and managed service providers when a security risk or vulnerability is approaching • Review IT assets and information systems to ensure any new system changes are compliant with the organization's cybersecurity policies
3. Incident response planning and management	• Maintain and periodically test EWON's Business Continuity and Disaster Recovery Plans • Maintain EWON's Incident Response Plans as well as Cybersecurity Emergency Contacts, Risk Register and Incidents & Events Register • Report and troubleshoot on security breaches and incidents, and co-ordinate investigations & recovery activities with internal and external stakeholders

	• Perform Incident Response Simulations and Training to protect EWON's digital assets against cyber threats, security breaches and unauthorised accounts
4. Compliance management	• Participate in information security risk assessments & audits, and coordinate compliance reviews & penetration testings to ensure adherence to EWON's cybersecurity policies and adopted security standards such as ACSC Essential Eight Maturity Level, Microsoft 365 and Azure Security Baselines • Ensure that security improvement actions are evaluated, validated, and implemented as required, and coordinate the implementation of security remediation and improvements with IT vendors and managed service providers
5. Cybersecurity Framework and Awareness	• Identify security control requirements for IT assets and business applications, and provide input on cybersecurity requirements • Develop and implement cybersecurity policies and processes in accordance with established security framework and architecture • Establish and implement practices for the monitoring of information systems' logical and physical security to minimise the risk of un-authorized access, data loss, and tampering • Maintain up to date knowledge of information security standards and strategies • Educate and communicate the value of information security throughout all levels of the organisation's stakeholders, and promote an active culture of security awareness within the organisation • Improve user knowledge through attack simulations and security awareness training programs
6. Support IDT operations	• Support the Information & Data Manager in the execution of Operational Plans, IT Roadmap initiatives and technology projects • In collaboration with IT vendors and managed service providers, provide administrative support for IT infrastructure, networks and business applications • Ensures appropriate documentation is created and maintained for core IT assets and operational processes
7. Work Health and Safety	Demonstrates an active commitment to WHS and compliance with legislation: • Takes reasonable care for their own health and safety • Takes reasonable care for the health and safety of others • Attends WHS training as required by EWON • Complies with any reasonable instructions, policies and procedures given by EWON
8. Team Contribution	**Displays EWON Values and Behaviours**

Independence Integrity	One Team Service Excellence	Respect Social Justice

Planning and Reporting

• Actively contributes to the development and delivery of the team's annual operational plan.
• Contributes to the team's monthly dashboard and reports.
• Ensures delivery of KPI targets and achievement plan commitments.

Teamwork

	• Actively contributes to effective teamwork within own team and across EWON. • Displays the EWON values and supporting behaviours. • Ensures service excellence processes with a focus on continuous improvement. **Organisation Relationships** • Fosters good communication and cooperative relationships within EWON.
Additional Duties	Undertake other tasks as reasonably required and/or requested.

Key Behavioural Capabilities

The key behavioural capabilities below are important for effective performance of the role. These capabilities will be assessed at recruitment.

Capability	Indicators
Planning and Organising	• Understand and apply effective planning, coordination and control methods • Understand all components of the project management process, including the need to consider change management to realise business benefits
Communication	• Communicate clearly, actively listen to others, and respond with understanding and respect • Translate technical and complex information clearly and concisely for diverse audiences • Explore creative ways to engage diverse audiences and communicate information
Problem Solving	• Work through issues, weigh up alternatives and identify the most effective solutions in collaboration with others • Think, analyse and consider the broader context to develop practical solutions
Collaboration	• Collaborate with others and value their contribution
Innovation	• Champion the use of innovative technologies to maximise efficiencies and effectiveness • Keep up to date with emerging technologies and technology trends to understand how their application can support business outcomes
Accountability	• Commitment to EWON's vision and operational plans, and deliver quality outcomes • Responsible for own actions
Resilience	• Show commitment to achieving challenging goals and demonstrate high level of motivation • Demonstrate resilience and courage in the face of challenges
Integrity	• Be ethical and professional, and adhere to legislation, policy and guidelines • Uphold and promote EWON values

Key Relationships

	Information and Data Manager
	Leadership and Management Team

Internal Stakeholders	Project work teams
	IT Champions
	All staff members
External Stakeholders	Cybersecurity Partners
	Managed service providers for core IT infrastructure and business applications
	IT suppliers/vendors
	Cyber legal experts

Required Qualification/Accreditations

- Degree in computer science, software engineering, IT or related area
- Cybersecurity certifications such as CompTIA, ISC2 CC / CISSP, or equivalent are highly desirable

Selection Criteria

- 5+ years IT experience, with a background in professional/managed services preferred
- Minimum 3+ years' experience in information security field
- Extensive experience across a broad range of technologies, including:
    - Azure Cloud Platform and Microsoft 365 services
    - Microsoft Security and Compliance stack such as Microsoft Defender for Endpoint, Microsoft Defender XDR, Microsoft Sentinel, Microsoft Purview
    - Windows Desktops and Server operating systems
    - Network Security, Firewall and Intrusion Prevention Systems (Fortinet)
- Strong knowledge of the ISO27001, SecOps and Governance, Risk & Compliance (GRC) framework
- Proven experience in Essential Eight Maturity Model and requirements for implementing Essential Eight guidelines
- Excellent analytical and problem-solving skills, with the ability to understand the problem, conceptualise complex information and manage outcomes within agreed timeframes
- Excellent communication and interpersonal skills, including the ability to present to a wide audience, articulate messages to non-IT stakeholder and build and maintain relationships with internal and external stakeholders at all levels

About Our Workplace

EWON is strongly committed to maintaining a constructive workplace where people are openly encouraged to express their views and feel safe to speak up if they experience or witness discrimination, bullying or harassment at work.

EWON staff are bound by confidentiality requirements and must sign a confidentiality agreement on commencement of employment, and are to advise of any conflicts of interest in carrying out the role.

EWON is an equal opportunity employer and promotes a safe and healthy, harassment free work place.