Position Description – Information Security/Cyber Security Specialist

We are here to	Our work will
Enable people to make and act on the best decisions about medicines, health technologies and other options for better health and economic outcomes.	Ensure people can access the best care and achieve the best value, considering individual circumstances.

Courage **Customer Centricity** **Collaboration** **Integrity** **Accountability**

About the role – Based in Sydney

NPS MedicineWise has established an excellent reputation for our work in programs, products and services to improve the quality use of medicines and medical tests in Australia. We are an information rich organisation and we are the custodians of national health data sets provide health insights to our customers. This role is responsible for providing expert information and cyber security advice to the business, managing and mitigating risk and ensuring the relevant controls are in place in accordance with industry standards.

Key responsibilities

- Understand and communicate IT Security implications to IT and business stakeholders.
- Provide specialist advice in the definition, application and communication of IT Security policies and standards.
- Utilise technical and business experience in guiding security control design and remediation efforts, consulting and collaborating with technical subject matter specialists where required.
- Select and manage IT security services (pen-testing, risk assessments, audits)
- Assess the compliance of key IT Security controls established to protect the organisation's information assets, including controls relevant to third party, outsourced services, and cloud-based technologies.
- Identify vulnerabilities in systems and software and ensure remediated plans are established and tracked to completion.
- Lead Incident Response activities.
- Oversee security vulnerability, threat, risk and compliance assessments against industry standards (e.g. ISO27000 series).
- Provide guidance and maintain compliance against Australian Federal Government security standards such as PSPF and ASD ISM.
- Provide training to staff within the organisation on cyber security and related matters
- Assist the Health Data Governance Specialist as delegated with broader team projects and activities and with corporate responsibilities such as reporting, compliance and/or risk management.

General corporate responsibilities

- Carry out responsibilities in the role in a manner that is consistent with NPS MedicineWise competencies and values.
- Proactively work towards and meet agreed annual and interim performance indicators.
- Take responsibility for WHS in accordance with policy and relevant legislation.
- Be aware of responsibilities to identify, reduce and report risks to our business in accordance with the NPS MedicineWise Risk Management Policy.

Accountabilities

- Monitor endpoint security, detect non-compliance and work with stakeholder to remediate.
- Develop and maintain Information Security scorecard (Threats, Vulnerabilities, Incidents, CMM)
- Maintain and report on Information Asset Register, Threat Model, Business Impact Assessments
- Develop and maintain IT Security requirements all NPS projects
- Work with teams in project design and delivery, to ensure security controls are integrated into toolsets and processes to deliver secure operation
- Monitor operational security posture and identify compliance issues and risks for escalation with systems owners or risk management function
- Undertake and report on audits of third party users of data to ensure compliance.

Challenges you'll encounter

- Maintaining solution-focussed approach in an environment of continuous change
- Broad variety of systems and technologies
- Positively influencing internal stakeholders to develop information security aware culture
- Managing conflicting priorities and time effectively
- Delivering project deadlines within tight timeframes.

You will report to

- Health Data Governance Specialist

Role Requirements

- CISM or CISSP certification (or working towards)
- Experience in implementing security control in AWS / Azure
- Exposure to ISO 27001 and ISO 31000
- Knowledge of Australian Privacy Principles and Data Breach Notification Scheme
- Exposure to vendor/supply chain risk assessments
- Broad knowledge of Information/Cyber Security including operational processes, technology and threats landscape.
- Understanding of and experience in design, development, testing and information/cyber security controls.
- Sound written and verbal communication skills
- Experience developing and implementing policies and processes to support Information Security in a complex organisation
- Influencing skills

Role Desirables

- Exposure to PSPF/ISM/IRAP framework and processes
- Experience in working with Australian Federal Government PSPF and ASD ISM.
- Experience of ITIL change and configuration management.

Last Updated: Sep 2018