



Case study



The development of an Information Security Policy and supporting onsite education and awareness presentation helps position cyber security as a priority at EISS Super.

THE CLIENT

Established in 1997, with origins dating back to 1919, Energy Industries Superannuation Scheme (EISS) provides superannuation, retirement and financial planning services to its members and employers.

Historically, EISS was exclusively available to the energy industry in NSW. In 2013, the fund was opened to all Australians and is now responsible for managing over \$5 billion on behalf of approximately 22,000 members.

EISS remains committed to working hard for its members so they can enjoy the retirement lifestyle they desire.

THE BUSINESS CHALLENGE

Following an Information Security Assessment, EISS was keen to further mature its information security posture with the development of a formal Information Security

Policy and the delivery of an onsite cyber security education presentation.

THE SOLUTION

Asterisk Information Security was selected to assist EISS with developing an Information Security Policy that would directly support EISS's strategy through the clarification of security requirements and relevant responsibilities.

Asterisk worked with EISS to define pragmatic principles that drive the management of security within the risk appetite of the business.

"A lack of clear direction for information security requirements may lead to poorly informed decision making that could result in the exposure of critical information and assets," said Jarrod Burns, Senior Security Consultant at Asterisk Information Security. "Defining mandatory principles is vital to the protection of information systems from unauthorised access, modification, and destruction. Developing and embedding a practical policy, in alignment with applicable standards and legislation, helps an organisation to preserve its reputation."

Information classification and handling guidelines were also developed for the policy, articulating how to identify if a certain piece or collection of information is critical to EISS and what the impact(s) would be in the event



MANAGEMENT



ARCHITECTURE



ASSESSMENT



INFRASTRUCTURE

of unauthorised disclosure, loss or destruction.

These handling guidelines expand on the existing approach to records management and covers the disposal of information in both digital and hard copy form.

In close consultation with EISS, Asterisk worked to ensure that the policy addressed key areas such as authorisation, authentication and accounting for both logical and physical access. “Formalising access management principles allows users and service providers to be given a clear statement of the business requirements to be met by access controls,” said Jarrod. “The policy aligns with, and supports, onboarding and offboarding procedures, and any user moves within the organisation.”

Following development of the policy, Asterisk delivered an education and awareness presentation to all EISS staff that covered the developed Information Security Policy and supporting content. Additionally, the presentation focused on demystifying online threats whilst educating users on security controls (both technical and non-technical) that they can apply easily at home and in the office.

“Jarrod from Asterisk delivered an excellent presentation which touched on all of the relevant areas of recent cyber threats and remediation,” said Stephanie Lyons, Chief Risk Officer at EISS. “Overall feedback was positive internally. Our people were engaged and there were post session questions around

topics such as phishing and password security.”

THE BENEFITS

An Information Security Policy, that is endorsed by Executive Management, communicated to personnel, and aligned with relevant standards and legislation is crucial to EISS’s ongoing cyber strategy.

“The direction set in the policy document will continue to support our business requirements and ensure that all processes and procedures are considered practical and enforceable,” said Stephanie. “We will regularly review the policy document to ensure it aligns with our cyber strategy and that best practices continue to be addressed.”

WE ARE ALL ABOUT INFORMATION SECURITY

Asterisk Information Security is a specialist consultancy providing actionable advice and solutions to enhance information security and reduce business risk. The team at Asterisk has been involved in the information security industry for over 18 years. Our clients range from SME to large enterprises across a variety of sectors including government, mining and resources, critical infrastructure, finance, retail, healthcare and not-for-profit.



For further information on how Asterisk can improve your information security, please contact **1800 651 420**

✉ contact@asteriskinfosec.com.au  [@asteriskinfosec](https://twitter.com/asteriskinfosec)  [linkedin.com/company/asterisk-information-security](https://www.linkedin.com/company/asterisk-information-security)