Information Security Policy Statement

SP AusNet is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our securityholders, employees, customers, suppliers and for the communities in which we operate. Finding the right balance between information security risk and business benefit enhances our business performance and minimises potential future exposures.

It is the policy of SP AusNet to ensure:

- Information will be protected against unauthorised access.
- Confidentiality of information will be maintained.
- Information will not be disclosed to unauthorised persons through deliberate or careless action.
- Integrity of information through protection from unauthorised modification.
- Availability of information to authorised users when needed.
- Information security training must be completed by all staff.
- All suspected breaches on information security will be reported and investigated.

Any individual dealing with information at SP AusNet, no matter what their status (eg; employee, contractor, or consultant), must comply with the information security policies and related information security documents published on the SP AusNet intranet. This policy applies to all information, computer and network systems governed, owned by and/or administered by SP AusNet.

The objectives of these policies are to:

- Reduce the opportunity for mistakes and misunderstandings to occur when dealing with IT assets and information of SP AusNet.
- Educate staff to allow them to independently make informed decision with regards to the secure handling of IT assets and information which is owned by SP AusNet within the framework of the information security policies.
- Assist in the identification and investigation of fraudulent IS related activities and co-operate with relevant legal agencies.
- Defend IT assets and information that SP AusNet governs, owns, manages, maintains or controls which are both tangible and intangible and safeguard IT related records and documents that exist in all forms – paper and electronic.
- Comply with the needs of the Regulatory Authorities (internal or external) and relevant legislation.

The goals of information security management are to:

- Have information security controls in the framework of information security policies so as to provide a secure environment for the operation of SP AusNet's business.
- Identify through appropriate risk assessment, the value of information assets and to understand their vulnerabilities and the threats that may expose them to risk.
- Manage the risks to an acceptable level through the design, implementation and maintenance of appropriate security processes and controls
- Comply with legislation and industry best practices that apply to SP AusNet

All personnel have a responsibility to report perceived and actual information relating to information security breaches and or IT incidents either to the IT Service Desk or to their immediate managers.

Management and employees are responsible for embedding information security risk management in our core business activities, functions and processes. Information Security Risk awareness and our tolerance for risk are key considerations in our decision making.

Nino Ficca
Managing Director
28 January 2011

SP AusNet
A member of Singapore Power Group