INFORMATION SECURITY POLICY STATEMENT

Information Brokers Pty Ltd is committed to understanding and effectively managing risks related to Information Security, to provide a greater certainty and confidence for our customers, employees, suppliers and 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 Information Brokers Pty Ltd to ensure;

- Information will be protected against unauthorized access
- Confidentiality of information will be maintained
- Information will not be disclosed to unauthorized persons through deliberate or careless action
- Integrity of information through protection from unauthorized modification
- Availability of information to authorized 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, no matter what their status (eg; employee, contractor or owner), must comply with the information security policies and related information security documents published on our intranet. This policy applies to all information, computer and network systems governed, owned and/or administered by Information Brokers Pty Ltd.

The objective of these policies are to:

- Reduce the opportunity for mistake and misunderstandings to occur when dealing with IT assets, both physical and electronic
- Educate staff to allow them to independently make informed decisions with regards to the secure handling of IT assets and information which we own within the framework of the information security policies
- Assist in the identification and investigation of fraudulent Information Security related activities and cooperate with relevant legal agencies
- Defend IT assets and information that we govern, own, manage, maintain or control, which are both tangible and intangible, as well as 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, to provide a secure environment for the operation of our various business units
- Identify through appropriate risk assessment, the value of information assets, understanding 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 our business units

All personnel have a responsibility to report perceived and actual information relating to information security breaches and/or IT incidents to the CEO or their immediate manager. 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.

Rod Keys
Chief Executive Officer

Certified System
ISO27001

Version 1.1
Last Reviewed: March 2024