Information security policy

Melbourne Market Authority is dedicated to protecting the confidentiality, integrity, and availability of information relevant to its operations. To achieve this, we are committed to developing, implementing and maintaining processes which meet the requirements of ISO 27001:2022 Information Security Management Systems (ISMS) actively managing exceptions that may exist.

Melbourne Market

Information Security Management System

1	**Leadership**	Our leaders will promote a security-focused culture, ensuring responsibility and resources are dedicated to meeting security goals, and assuring stakeholders that information is properly protected, managed, and disposed of.
2	**Legal Compliance**	We are committed to adhering to all relevant laws, regulations, and contractual obligations to maintain high standards of security and privacy.
3	**Risk Based Decision Making**	We will take a risk-based approach to our operations ensuring foreseeable information security threats and vulnerabilities are identified, assessed and necessary controls are implemented to effectively mitigate the potential impact.
4	**Asset Management and Control**	We will implement processes to facilitate secure handling, maintenance, and disposal of assets and data to mitigate risks and maintain compliance.
5	**Training and Awareness**	A training and awareness program will be developed and implemented for all employees to promote a culture of security, including awareness of policies, procedures and controls relevant to their roles and responsibilities.
6	**Incident Management and Response**	A formal incident management process will be created to support prompt and effective response to security incidents, root cause analysis; applying lessons learnt to mitigate future events.
7	**Inspection and Monitoring**	We will implement an inspection, monitoring and evaluation program to validate the implementation and effectiveness of our ISMS.
8	**Continual Improvement**	We are committed to regularly reviewing and enhancing our information security management system to adapt to evolving threats and business needs.

To support this Policy Statement, we will create, maintain and periodically review measurable information security objectives and targets that align with our strategic direction. This Policy Statement will be communicated to all employees, contractors and made available to relevant stakeholders. It will be reviewed periodically to ensure its continued suitability.

Keith Louie
Chief Executive Officer