Information Security Policy

Intent

Assetlink Group ("Assetlink") incorporating Assetlink Services Pty Limited and AssetFuture Pty Limited ensures the security of documents and data under our control and is committed to the assessment and treatment of information security risks directly or indirectly related to our processes, products and services.

Principles

Accordingly, we will:

- Comply with relevant information security legislation and regulations, any relevant customer requirements.
- Educate, train and provide sufficient resources, including identifying clear roles, responsibilities and authorities, to our team members as well as, where appropriate, to sub-contractors and visitors, so that all relevant parties understand information security issues and the effect of their activities on information security
- Monitor, through operational and management review meetings, and systematic auditing, our information security performance towards established objectives.
- Develop and maintain operational procedures to minimise and handle any information security issues, should they occur.
- Identify information security requirements and results from risk assessment and risk treatment.
- Continually improve our information security processes and procedures.

To achieve our information security objectives, we have implemented an Integrated Management System, which includes information security management system requirements and maintains certification against ISO27001:2013.

RACI

Responsible	It is the responsibility of all team members to ensure the Policy is understood, implemented and maintained within all levels of their teams.
Accountable	The final authority for this policy lies with the Managing Director.
Consulted	When making changes to this policy a consultation should be carried out with those team members and teams who have responsibility for information security.
Informed	All changes to this policy should be communicated to all team members and relevant contractors.

Operation and Incidence

Asset Classification and Control

All Information Systems and Information Assets must be uniquely identified, assigned a classification and an Information Owner; and the Information Owner will decide who is authorised to access an Information System or Information Asset, the type of access (read, modify, delete, copy), where it can be accessed, when it can be accessed, and if and how it may be made public.

Personnel Security

Every individual who uses or has access to Assetlink's information, information systems or computer equipment must be made aware of the Information Security Policy, and be advised that they are responsible for maintaining information security, including, but not limited to:

- Complying with all information security policies, standards and procedures;
- Ensuring information is only used for the purpose it was collected as defined by the Information Owner;
- Maintaining confidentiality of passwords; and
- Promptly reporting evidence of attempts to compromise security or misuse of information or information systems to the Information Owner.

Physical and Environmental Security

All Information Systems or Information Assets classified as "critical" must be housed in a physically secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls. It must be physically protected from unauthorised access, damage and interference.

Communications and Operations Management

Communications of sensitive Information Assets, either within Assetlink facilities or involving third parties, must be secured in a proper manner commensurate with the value and sensitivity of the Information Assets; and appropriate processes be implemented and maintained in the general Assetlink operation to ensure that Information Systems and Information Assets are protected from electronic attacks, threats and vulnerabilities.

Access Control

Access to Information Assets and Information Systems will be granted in a controlled manner, by the Information Owner, driven by business requirements such as the user's role or the "need to know" principle; and ‘read only’ access to Information Assets classified as public does not require a formal authentication and authorisation process.

Systems Development and Maintenance

Appropriate security is to be designed and implemented into all stages of the Information System Life Cycle (design, implementation, operation, and disposal).

Business Continuity Management

All Critical Information Systems have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure the ability to recovery from failure or unexpected interruption; and the Information Owner is responsible for the implementation of a routine of risk assessment in order to refine the recovery requirements. The Business Continuity and Disaster Recovery Plans must be updated to reflect these refinements.

Compliance

All applicable legal, statutory, contractual or regulatory requirements for information security will be documented and defined by the Company's solicitor; and every individual who uses or has access to information, information systems or computer equipment will be made aware of their responsibilities to comply with all legal, statutory, contractual or regulatory requirements pertaining to the information or information systems.

Authorised by:

…………………………………………	…………………………………………
Frank Cipriani	Aurora Fonte
Chief Financial Officer	Managing Director