Information Security Policy

Intent

Assetlink Group ("Assetlink") incorporating Assetlink Services Pty Limited, AssetFuture Pty Limited and AssetProjects Pty Ltd 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.

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

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.

Secure 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).

Processes for development of new systems and enhancements to existing systems must contain security requirements. Changes must be tracked within a formal change tracking environment. Authority for making changes will be restricted to authorised people. Changes must undergo a review/testing to eliminate negative impacts prior to their release.

When establishing new or implementing upgrades to existing systems, including off-the- shelf or out-sourced software development:

- Address security in the early stages of the development, including the concept and planning, needs analysis and design stages,
- Include data validity checks, audit trails and activity logging to ensure accuracy and integrity of data,
- Use change control, acceptance and system testing, planning and migration control when upgrading or installing software in the operational environment,
- Control access to system files to maintain integrity of the application and data,
- Implement access controls including restrictions, segregation/isolation of systems in all infrastructure and applications.

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.

End of Policy