Information Security

Policy, Objective & Procedure

Policy

Lucidity is committed to provide, manage, maintain and continuously improve an information security management system [ISMS] in compliance with ISO 27001 that enables:

- Confidentiality protection provisions of information held by Lucidity
- Integrity of the Lucidity systems structure affording protection from unauthorised access or intrusion
- Lucidity software platforms designed and developed to meet customer needs and expectations
- Availability, reliability and sustainability of Lucidity platforms and the data and information they hold
- Systems to ensure the protection of data and information from loss or corruption
- Lucidity business sustainability through subscriptions growth and retention
- Complimentary alignment of product offerings of Lucidity and SiteSoft products

The ISMS is enabled through a series of policies, second tier objectives against each policy with documented systems and technology solutions.

Responsibilities and authorities

Overall ownership is shared between the executive team and directly managed by the DoT & ISMS Rep in the case of an incident, issue or nonconformance.

Competent persons within Lucidity are assigned roles in owning and delivery processes. Individuals shall be accountable for following policies and procedures and for informing management of any likely or prospective breaches.

Forms, templates and records

Lucidity platforms

SiteSoft platforms integration with Lucidity

Lucidity source code

Lucidity policies and associated objectives for delivery of the policies

Objectives

The following ISMS objectives apply to all aspects of the ISMS and are measured for performance and improvement through executive review meetings.

OBJECTIVE	PERFORMANCE	MEASURE
Lucidity customer focused design and development	Lucidity software platforms designed and developed to meet client needs and expectations, including SiteSoft applications	Road Map development and improvement program Client driven product enhancements and continual product improvement and integration of product offerings across the organisation
Lucidity platform sustainability and reliability	Reliability and sustainability of Lucidity platforms including SiteSoft applications	Lucidity platform/site downtime rate
Lucidity confidentiality by data protection provisions	Confidentiality protection provisions of information held by Lucidity on all platforms	Breach of data protection laws
Lucidity data integrity imbedded in systems structure	Integrity of the Lucidity systems structure affording protection from unauthorised access or intrusion on all platforms	Breach through unauthorised access Platform robustness Malware effectiveness Virus event monitoring
Lucidity manage data availability by loss protection	Systems to ensure the availability of data and protection from loss or corruption	Data loss protection effectiveness Event monitoring Penetration testing outcomes
Lucidity as a sustainable business	Lucidity listing on ASX by Q3 2022	Exponential growth of product range, flexibility offered to existing customers and potential clients Refer Business Management OKRs

Lucidity

Lucidity Software is a product of more than a decade of software refinement, and a lifetime of working with organisations on training, compliance and risk management requirements. This has progressed in 2022 with the merger of Lucidity and SiteSoft.

Lucidity determines information security to be the protection against unauthorised use of information in any form including electronic data, and the measures taken to achieve an acceptable level of security.

To support and continuously improve Lucidity business development and the information security system, a set of policies are defined, approved by the executive team, published and communicated to employees and relevant external parties including subcontractors, suppliers, clients as appropriate and regulators upon request.

Policies are a result of strategic planning, regulator compliance contract obligations and the risk thinking associated with threats and opportunities.
The ISMS requires staff and involved parties to have a level of information security awareness. This is provided through Lucidity's e-learning system and other qualifications and training according to individual roles and ownership of the ISMS.

Rev No	Changes made	Who Reviewed & Approved	Training required ? (Y/N)
A - 5.0.1	Combination of several previous documents	Executive Team [ISO 27001]	Yes
A - 5.0.2	Minor updates	Wayn Wong	No
A - 5.0.3	Timelines updates	N.Cruse for ELT	No
A - 5.0.4	Integration of Lucidity & SiteSoft resulting in updated performance expectations	R. Cruse for ELT	No
Digital Signature Approval: