

Information Security Policy Statement

Document number:	1.1
Owner	The Board of Platform One
Approver	Global CEO

1. OVERVIEW

Platform One Pty Ltd ("Platform One") is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our clients, employees, suppliers and for the communities in which we operate. Finding the right balance between information security risk and business benefit enhances business performance and minimise potential future exposures.

2. OVERALL OBJECTIVES

It is the policy of Platform One to:

- Ensure confidentiality, integrity and availability of Platform One's Information Security ("IS") systems
- Identify, communicate and manage the responsibilities of users and their obligations to help protect corporate information and systems
- Protect Platform One from business damage or legal liability and the inappropriate use of IS systems and information.
- Comply with the needs of the regulatory bodies and relevant legislation.

3. ASSOCIATED TARGETS**Ensure confidentiality, integrity and availability of Platform One's IS systems**

- Information shall be protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or careless action.
- Integrity of information through protection from unauthorised modification.
- Availability of information to authorised users when needed.
- Business continuity plans are developed, maintained and tested

Identify, communicate and manage the responsibilities of users

- Information security training is available and mandatory for all employees and where applicable tailored for individual roles

- Human Resources policies define and assign information security roles and responsibilities throughout the organization.
- Educate staff to allow them to independently make informed decision with regards to the secure handling of IT assets and information which is owned by Platform One within the framework of the information security policies.

Protect Platform One from business damage or legal liability and the inappropriate use of IS systems and information.

- Ensure the ability to identify and investigate fraudulent IS related activities and co-operate with relevant legal agencies.
- Contractual arrangements or formal agreements with clients, third party service providers, contractors and consultants include all relevant information security requirements

Comply with the needs of the regulatory bodies and relevant legislation.

- Relevant legislative, regulatory and business requirements are met
- Any individual dealing with information at Platform One, no matter what their status (e.g.; employee, contractor, or consultant), must comply with the information security policies and related information security documents. The policy applies to all information, computer and network systems governed, owned by and/or administered by Platform One.

4. COMPLIANCE AND CERTIFICATION

Platform Ones manages its systems via security controls. IT operational controls address certain aspects of Information Security specifically and in addition non-IT information assets are included and protected under the Information Security Management System ("ISMS").

- As part of the overall technical and security measures Platform One is certified with ISO 27001 requiring that management:
- Adopt an overarching management process to ensure that the information security controls are designed and continue to meet the organization's information security objectives and needs on an ongoing basis.
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable;
- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;

An independent external auditor tests Platform One controls as part of the ISO 27001 certification annually. This includes all controls that the organization deemed to be within the scope of the ISMS which was inclusive of physical security, HR and assets control. The regular audit schedule ensures that these controls have been implemented and are operating effectively. Management has determined the exhausted scope of the ISMS for certification purposes.

Platform One Australia achieved initial ISO 27001 Certification in 2017

Current Certificate Number 830-I-4

Certificate Issue Date: 18/12/2025

Certificate Expiry Date: 16/02/2029

Scope Of Current Certification: Platform One's jurisdiction expands to Australia, Sri Lanka, Malaysia, France & USA.



5. HISTORY TABLE

Date	Version No	Changes	Reviewed By	Approved By	Communications
5/01/2026	G 4.0	Updated for Recertification across all global locations	ISMS Manager	Global CEO	Published via Website
8/10/2025	G 3.2	Updated with new Certification Marks	ISMS Manager	Global CEO	Published via Website
17/12/2024	G 3.1	Updated with Certificate issue	ISMS Manager	Global CEO	published via Website
26/10/2024	G 3.0	Updated to include Malaysia and the upgrade to ISO27002:2022	ISMS Manager	Global CEO	published via Website
18/10/2023	G 2.0	Updated to reflect Merged ISMS (Australia & Sri Lanka)	ISMS Manager	Global CEO	published via Website
10/12/2022	G 1.2	Updated with Certificate details	ISMS Manager	ISMS Committee	published via Website
6/11/2022	G 1.1	New Auditor Certification mark	ISMS Manager	ISMS Committee	published via Website
7/8/2022	G 1.0	Updated to new Trading Name	ISMS Manager	Management Review	via Employment Hero