1. Purpose

The purpose of this policy is to establish Apollo Property Group's commitment to protecting information assets and ensuring the confidentiality, integrity, and availability of information and systems that support our business operations, clients, partners, and Defence-related activities. This policy provides the foundation for Apollo's Information Security Management System (ISMS) and outlines the responsibilities and principles required to maintain a secure and resilient information environment.

2. Scope

This policy is approved by the Board of Apollo Property Group Pty Ltd and applies to all Apollo Property Group personnel, including employees, contractors, directors, offshore resources, temporary personnel, and third parties who access or manage Apollo information, systems, networks, or facilities.

Apollo Group Services Pty Ltd (AGS), as the employing entity, adopts and is bound by the governance and compliance framework of Apollo Property Group.

This policy covers all information formats, including digital, verbal, and physical records, and applies to all technologies, services, and devices used in the conduct of Apollo activities, whether company-issued, cloud-managed, hosted, or otherwise authorised for business use.

3. Policy Statement

Apollo Property Group is committed to maintaining a secure information environment and to operating an Information Security Management System aligned with ISO/IEC 27001:2022, the Defence Industry Security Program (DISP) requirements, and AS 4811 Workforce Screening standards.

Apollo recognises that information security is a shared responsibility and that maintaining trust, protecting data, and ensuring service continuity are essential to business operations and organisational resilience. Apollo will apply appropriate governance, risk management, personnel security, and cyber security controls to safeguard information throughout its lifecycle and ensure compliance with all legal, regulatory, contractual, and Defence-security obligations.

4. Information Security Management

Apollo will implement, maintain, and continuously improve an Information Security Management System that incorporates secure processes for risk assessment, access control, threat detection, change and configuration management, security monitoring, incident response, and business continuity. This includes the use of modern identity and access controls, device security, email protection, and monitoring systems such as Microsoft Entra ID, Microsoft Intune, and Avanan, as well as mechanisms to support phishing reporting, insider-threat awareness, and cyber event detection and response.

Apollo will monitor changes in technology, business operations, Defence security requirements, and the threat landscape, and will take proactive steps to maintain a security posture that reflects best practice and Defence expectations.

To support this commitment, Apollo will:

- Comply with all applicable laws, regulations and contractual obligations.
- Implement continual improvement initiatives including risk assessment and risk treatment strategies,
- Communicate information security objectives and performance to relevant internal and external stakeholders
- Maintain an Information Security management system comprising a security manual and procedures
- Work closely with customers, business partners and suppliers to establish appropriate Information Security standards.
- Review risk evaluation criteria in response to business and threat changes
- Train all workforce members in Information Security responsibilities
- Strive to meet, and exceed customer, staff, and supplier expectations.
- Provide education, training, and awareness for information security and the continued operation of the Information Security Management System.

5. Personnel Security and Suitability

Apollo will apply workforce screening, suitability, and ongoing monitoring requirements consistent with AS 4811 and DISP personnel security obligations. Screening and suitability requirements apply to all individuals accessing Apollo information and systems, including offshore resources. Enhanced screening and monitoring will apply to roles with privileged access, financial responsibilities, access to Defence-related information, or elevated security risk.

All workforce members must participate in security awareness activities and understand their role in identifying and reporting suspicious activity or security concerns.

6. Security Governance, Roles and Responsibilities

Ultimate accountability for information security rests with the Board of Directors.

Apollo Property Group assigns specific Defence security responsibilities in accordance with DISP requirements. The Director – Operations is appointed as the Company Security Officer (CSO) and has overall accountability for DISP security, including personnel security, physical security, information security, and governance obligations.

The Systems & Compliance Manager is appointed as the Security Officer (SO) and is responsible for managing day-to-day DISP activities, information security operations, personnel screening and suitability processes, contractor and third-party compliance, and security incident reporting in accordance with Apollo's policies and Defence security obligations.

Both the CSO and SO are responsible for maintaining evidence of compliance, ensuring Defence security requirements are embedded into Apollo's systems and processes, and reporting on security performance and risks to the Board.

Managers and Supervisors are responsible for ensuring workforce compliance with information security requirements and promoting secure work practices.

All workforce members must comply with this policy and its supporting procedures, protect information in their care, complete security training, and report actual or suspected security incidents or concerns.

7. Continuous Improvement and Assurance

Apollo will maintain a program of continuous improvement supported by internal assurance, external audit, DISP self-assessment and evidence collection, system monitoring, review of incidents and near misses, and lessons learned. This policy and associated controls will be reviewed at least annually or in response to significant organisational, regulatory, or technological changes.

Authorised by

Leon Bowes
CEO & Chairman