GBL IT01 Information Security Policy

Approved by:	MD, Organisational Effectiveness	Policy type:	GBL
		Policy number:	GBL IT01
Responsible official:	Global Director, ICT	Version:	3.0
		Effective date:	17 February 2022
		Last review date:	30 January 2023

Revision history

Version	Effective date	Approved by	Summary of changes
1.0	01 December 2015	COO	N/A
2.0	01 October 2017	CFO	Updates and expands GBL IT01 of Dec 2015 and associated guidelines
2.1	01 April 2021	MD, OE	Updates and expands GBL IT01 of Oct 2017 and associated guidelines
3.0	17 February 2022	MD, OE	Major revision of ISMS in ISO 27001 project

Statement

This is a controlled document. The master document is posted on the Company intranet. Representatives may print off this document for training and reference purposes but are responsible for regularly checking the Company intranet for the current version.

Contents

1. Purpose

This Policy aims to be a ‘Statement of Compliance’ to Information Security within Palladium, as set by the Board of Directors and implemented through the Corporate Leadership Team and Regional Partners.

2. Applicability

This Policy is applicable globally to all Company operations and all Representatives of the Company. It applies to joint ventures where the Company has a controlling interest and to any project where the Company has responsibility for the functions of the Responsible Official. Any deviation from this Policy requires the approval of the Responsible Official.

The Company has in place Guidelines, SOPs, Business Processes and Tools to support implementation of this Policy.

The Responsible Official, with input from the business as appropriate, is responsible for preparing and implementing the related Guidelines, SOPs, Business Processes and Tools.

3. Definitions

“Availability” is one of the three principles of Information Security where assurance is given that information is available to the organisation and interested parties who are authorised to have access to it, when and where they need to use and process it. In practice ensuring that information is available for those who are authorised to use it based upon its security classification.

“Company” refers to Palladium Group Holdings Pty Ltd and all of its subsidiaries or related companies.

“Confidentiality” is one of the three principles of Information Security where information, in any form, while in storage, being processed or communicated, shall be protected to ensure it is only available to those that are authorised by the organisation and/or the information owners to have access to, and use of, the information.

“Employee” means any person who has a part-time, full-time, intermittent, continuous, or fixed-term employment relationship with the Company.

“Integrity” is one of the three principles of Information Security where assurance is given that information in storage, being processed or communicated is accurate and complete; that it is correctly processed and has not been modified in any unauthorised way. The integrity of the networks and information systems that they connect to are also important to ensure that these operate in ways that the organisation intends them to be operated.

“ISMS” or “Information Security Management System” is a framework of business processes, policies, procedures and various other security controls that defines an approach to information security and works to measure and continually improve it,

“Management Review” is a regular meeting where senior management review the effectiveness of the ISMS.

“Objectives” are goals which are set to ensure that the Information Security Policy requirements are met and continual improvement is achieved.

“PESTLE” or “STEEPLE” is a methodology for determining external security issues that could impact Information Security by identifying influences from Political; Economic; Social; Technological; Legal; Environmental and Ethical events.

“Representative” means an Employee or any person who has an independent individual contractual relationship with the Company, whether as a contractor, consultant or agent of the Company. This includes non-executive directors of the board.

“SWOT” is a methodology for determining internal security issues that could impact Information Security by identifying Strengths, Weaknesses, Opportunities and Threats.

4. Policy

4.1. Statement of Compliance

In this Information Security Policy, Palladium has defined its commitment to protecting information through the Information Security Management System (ISMS) which ensures:

- **Confidentiality**: ensuring that information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods; and
- **Availability**: ensuring that authorised users have access to information and associated assets.

The ISMS effectiveness is achieved through understanding the risks and opportunities that may impact information within the Company and by using several controls, including policies, processes, procedures, software, and hardware functions; and managing these issues in ways that are beneficial to the Company and its interested parties.

These controls are continually monitored, reviewed, and improved to ensure that specific security and business objectives are met. This is operated in conjunction with other business management processes and incorporates the applicable statutory and contractual requirements.

Objectives have been defined primarily through the SWOT and PESTLE, although some may come from the Risk Assessment and the Management Review. They are designed to drive the management system forward and bring about continual improvement. Objectives focus on improving confidentiality, integrity and availability.

The ISMS has been designed to address legislation as listed in the ISMS Legal Register.

Palladium operates a programme of information security awareness and compliance through company inductions, training, and internal audits.

All employees are empowered to identify any potential security weaknesses and/or events which could be Information Security Incidents and report through the appropriate management channels.

A robust system is in place to continually improve the security controls by:

- Taking account of changes to business requirements and priorities;
- Considering new threat and vulnerabilities which may impact the business;
- Reviewing the effectiveness of the ISMS through internal audits and the Management Review process.

The overall intent of this management system is to give customers and other interested parties confidence in Palladium’s ability to protect all information held or processed by the Company.

5. Duty to comply

It is the responsibility of all Representatives of the Company to fully comply with this Policy. Failure to comply may result in disciplinary action including contract termination, contract non-renewal or other appropriate action.

6. Reporting

Representatives are required to report suspected violations of this Policy to their IT Support team, to their manager or through the Company's Whistle-blower mechanism.