Palladium
MAKE IT POSSIBLE

GBL IT01

Information Security Policy

Functional Group: Information Technology
Policy Owner: Global Director, ICT
Policy Approver: Chief Operating Officer
Version: 3.2
Last Updated: 06 August 2026
Last Reviewed: 06 August 2026

Contents

1. Purpose 1

2. Scope and Applicability 1

3. Definitions 1

4. Roles and Responsibilities 2

5. Policy Details and Requirements 2

5.1. Statement of Compliance 2

6. Policy Violations and Reporting Concerns 3

7. Version History 4

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.

2. Scope and Applicability

This Policy is applicable globally to the Company, and all Representatives of the Company, and to any joint venture where the Company has a controlling interest.

3. Definitions

Certain terms used in this Policy are defined in GBL CG01 GL01 Definitions of Standard Terms. In addition:

Availability: 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.

Confidentiality: 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.

Integrity: 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: 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: Regular meeting where senior management reviews the effectiveness of the ISMS.

Objectives: Goals which are set to ensure that the Information Security Policy requirements are met and continual improvement is achieved.

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

SWOT: Methodology for determining internal security issues that could impact Information Security by identifying Strengths, Weaknesses, Opportunities and Threats.

4. Roles and Responsibilities

The Policy Owner is responsible for maintaining and enforcing this Policy. The Company and all Representatives are responsible for complying with it.

5. Policy Details and Requirements

5.1. Statement of Compliance

a. 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.

b. 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.

c. 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.

d. 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.

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

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

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

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

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

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

6. Policy Violations and Reporting Concerns

Violations of this policy may result in disciplinary actions being taken, which may include termination of employment.

Employees have a responsibility to raise concerns about situations that they know, or appear to them in good faith, to violate this policy. Employees can raise questions or concerns directly to their managers, the Human Resources department, the Ethics, Risk and Compliance Department at ethics@thepalladiumgroup.com or anonymously on the Integrity Hotline. All concerns are managed in a confidential manner and Palladium has a strict policy towards non-retaliation for concerns raised in good faith.

7. Version History

Version	Effective Date	Approved By	Summary of Change
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
3.1	13 June 2024	COO	Change of ownership
3.2	06 August 2026	COO	Adoption of Company updated policy templates.