An ETS Company

Information Security Public Policy Statement

Version:	Date:	Classification:	Owning team:
2.0	May 23, 2024	Public	ISCO

Contents

> **When displaying in Offices and Test Centres please only print page 2**

Information Security Policy Statement

PSI offers a comprehensive solutions approach from test development to delivery to results processing, including pre-hire employment selection, managerial assessments, licensing and certification tests, distance learning testing, license management services and professional services. We are committed to providing secure services to our clients in the public and private sectors, in order to consistently satisfy their needs and expectations.

We achieve this by operating, maintaining, and continually improving our information security arrangements as part of our Integrated Management System (IMS) in accordance with the international standard ISO27001:2022.

Information Security is controlled through the preservation of:

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

Our information security policy is achieved through understanding the risks and opportunities that may impact information within the business and by using a number of controls, including policies, processes, procedures, software, and hardware functions, to manage these issues in ways that are beneficial to the business.

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.

We have set SMART information security objectives and performance against these is monitored, measured, and regularly reported to Top Management. Objectives will be focused on improving confidentiality, integrity and availability.

We realize that information security is the responsibility of all personnel, and we actively promote a culture of continual improvement within the information security management functions, e.g. IMS system maintenance to suitably skilled and competent people. We operates a programme of information security awareness and compliance through company inductions, training and internal audits.

The IMS is maintained and is subject to internal and external audit. All employees are empowered to identify any nonconformities or identify any potential security weaknesses and/or events which could be information security incidents and report these through the appropriate management channels. The IMS has the full commitment of management.

To ensure that this commitment is delivered, we will:

- Comply with applicable legislation, regulation, and obligations
- Understand and meet the information security requirements of our clients
- Understand and meet the needs and expectations of other stakeholders
- Consider information security as a factor when making business decisions
- Set SMART information security objectives and monitor progress
- Incorporate our IMS within the business operations
- Ensure that staff and suppliers are aware of our information security Policy
- Ensure that our staff are competent to undertake their assigned roles
- Identify and implement opportunities to improve our Integrated Management System
- Monitor the performance of the IMS in achieving its objective
- Make this policy available to external parties upon request.

Owned by: Kathryn Walker, Director Information Security, Governance, Risk & Compliance

Date: 23/05/2024 **Next review date:** 23/05/2025

Revision history

Version	Date	Comments
0.1	October 17, 2023	Document creation.
0.2	November 23, 2023	Final draft ready for review
0.3	January 02, 2024	Final Review before IMS Management Committee
1.0	January 09, 2024	Amended Scope Statement and ratified by IMS Management Committee.
1.1	January 23, 2024	Published
2.0	May 23, 2024	Amended to PSI branding and removed all reference to LLH and Talogy

Approval Section

Name	Position	Date
Kathryn Walker	Director Information Security, Governance, Risk & Compliance	May 23, 2024