SH PROFESSIONAL SERVICES

Ref: SHPRCO015

Information Security Policy Statement

Approved by: Board & RCO Committee | Version: 1.1 | Effective date: 1 October 2026 | Next review: 1 October 2027

SH Professional Services Ltd (we, us, our) recognises that the information we hold — our own and that entrusted to us by our clients — is a valuable asset that must be protected. We are committed to preserving the confidentiality, integrity and availability of that information, and to managing information security risk as part of how we run our business.

1. Scope

This statement applies to all information we hold and process, in any form, and to everyone who works for or on our behalf, across all our systems, devices and premises and those of our service providers.

2. Our commitments

- We identify and assess information security risks and apply controls that are proportionate to them.
- We protect personal and confidential information through appropriate technical and organisational measures, including access controls, encryption, and secure handling, storage and disposal.
- We grant access to information on a need-to-know basis and keep access under review.
- We assess the security of the third-party tools and service providers we rely on, and hold them to appropriate standards. Their own terms and limitations apply to their services.
- We maintain arrangements to detect, respond to and recover from security incidents, and to maintain continuity of our services.
- We provide our people with training and clear expectations on acceptable use and secure working.
- We comply with our legal and regulatory obligations, including those under the UK GDPR and the Data Protection Act 2018.

3. Incident and breach management

We maintain procedures to manage information security incidents. Where an incident involves personal data and is likely to result in a risk to individuals, we will assess and, where required, report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours, and notify affected individuals where the law requires. Where an incident affects a client, we will inform the client in accordance with our obligations to them.

4. Governance and review

Responsibility for information security rests with our directors, who ensure that appropriate measures are in place and resourced. We align our approach with recognised good practice, working to standards set by ISO 27001 and Cyber Essentials, and we review this policy and our controls regularly and after any significant change or incident.

How we handle personal data is explained further in our Privacy Notice for Clients.