INFORMATION SECURITY POLICY

Document Control
Reference: ISMS POL 2.1
Issue No: 4.10
Issue Date: 02JUL2025
Classification: Controlled

1. Document Purpose & Scope 2
2. Policy Statement 2
3. Information Security Objectives 2
4. Responsibilities 3
5. Implementation 3
6. Document Owner & Approval 4
   6.1 Change History Record 4

1. DOCUMENT PURPOSE & SCOPE

a) This document sets out the Information Security Policy of Sota Solutions Ltd with respect to the activities undertaken by the company as described in its ISMS Scope Document.

b) This document has been approved by the Management Board and will be reviewed annually for continued suitability in accordance with the company's standard Management Review Procedure and will be communicated to all staff within the company and, where appropriate, made available to interested third parties.

2. POLICY STATEMENT

a) The company is committed to maintaining and continually improving an Information Security Management System (ISMS) that satisfies all applicable requirements and is certified to the international standard ISO/IEC 27001:2022.

b) This policy aims to prevent and minimise the impact of security incidents and business disruptions in order to ensure the company provides a service that meets or exceeds the expectations of our clients.

c) The company will conduct its operations in accordance with the demands of its ISMS and will comply with all relevant legal and statutory obligations required by the law of the countries in which we operate and the reasonable practice and relevant requirements of interested third parties, including client contractual obligations.

3. INFORMATION SECURITY OBJECTIVES

a) The objectives of this policy are to define the company's position in relation to its approach to information security, which it qualifies as the requirement to secure and maintain the AVAILABILITY, CONFIDENTIALITY and INTEGRITY of the physical and information assets employed in support of the company's SotaCloud, SotaProtect, SotaColo, SotaConnect and SotaDR service offerings.

b) The company's Information Security objectives are detailed as follows:

1. To manage, control and reduce information security risks to an acceptable level:

Measurement: Reviews will be conducted annually and risk assessments after any significant change to business operations or technology. The risk exposure will be calculated based on scoring of likelihood and impact with appropriate treatment to mitigate or reduce the risk where possible. This will be tracked within our risk register.

Responsibility: The Risk & Audit Committee will oversee the risk management program, with support from departmental heads and platform or asset owners.

Timeline: Quarterly reviews and ongoing risk mitigation activities. Risk treatment plans will be reviewed and updated as needed based on risk levels.

Evaluation: The effectiveness of risk management efforts will be assessed using metrics such as reduction in high-risk incidents, successful implementation of mitigating controls, and compliance with established risk tolerance levels. This will be reviewed annually by the Risk & Audit Committee.

2. Ensure information is appropriately protected and available in line with business requirements:

Measurement: Availability and confidentiality of critical business information will be measured through annual internal audits. Compliance with established access control policies, media handling and asset management to be verified by periodic review of appropriate registers.

Responsibility: The Risk and Audit Committee are responsible for ensuring compliance with data protection and availability standards.

Timeline: Protection and availability will be monitored continuously, with a formal review conducted annually to assess system performance and business alignment.

Evaluation: Evaluation will be based on confirmation that corresponding registers have been completed accurately in accordance with the relevant policy. Results will be reviewed by the Risk & Audit Committee.

3. To ensure that information shared with third parties is protected against unauthorised disclosure:

Measurement: Third-party risk and compliance will be monitored through auditing. Data protection agreements (DPAs) and non-disclosure agreements (NDAs) will be reviewed.

Responsibility: Internal teams will work collaboratively to ensure that third-party relationships comply with the company's information security policies.

Timeline: Third-party risk and compliance will be conducted annually or when entering into new third-party agreements. Compliance audits will be scheduled quarterly or following any breach or security incident.

Evaluation: The performance of third-party information security will be evaluated based on the outcomes of audits, assessment of contract compliance, and the absence of security incidents involving third parties. Results will be reviewed by the Risk & Audit Committee

4. To maintain employee awareness of information security:

Measurement: Employee awareness will be tracked and measured through mandatory training Completion rates, periodic phishing simulations, and surveys on information security understanding.

Additional assessments will be conducted following any significant information security updates or incidents.

Responsibility: Human Resources (HR) and department heads will jointly coordinate and track employee training and awareness programs.

Timeline: Awareness programs will be delivered during onboarding, with annual refresher courses and ad-hoc updates as needed. Awareness tests (e.g., phishing simulations) will occur periodically.
Evaluation: Evaluation will be based on training completion rates, test scores, and the frequency of successful phishing attempts or other security incidents resulting from employee negligence. Results will be reviewed by the Risk & Audit Committee

5. Ensure that all breaches of information security are reported and investigated:

Measurement: Incident management processes will be measured by tracking the number of reported incidents, response times, and resolution effectiveness. The root cause analysis and corrective actions taken will be documented and evaluated.

Responsibility: The Risk & Audit Committee will oversee the incident management process, ensuring all breaches are promptly reported, investigated, and mitigated.

Timeline: All incidents, whether suspected or confirmed, must be reported within 24 hours. Investigations will be initiated immediately. Reviews will be carried out quarterly.

Evaluation: The effectiveness of the breach handling process will be evaluated through post-incident reviews, incident resolution times, and lessons learned to prevent recurrence. Results will be reviewed by the Risk & Audit Committee.

6. Provide documentary evidence of policy compliance:
Measurement: Documentation and audit trails will be maintained and reviewed through regular internal and external audits. Evidence such as logs and audit reports will be collected and stored securely.

Responsibility: The Risk & Audit Committee will be responsible for ensuring documentation is accurate and up to date and will oversee the audit process and final reporting.

Timeline: Documentation will be maintained continuously. Internal audits will be conducted annually, and external audits will occur every two years or as required by regulatory bodies.

Evaluation: The completeness and accuracy of the documentation will be evaluated during audits. Compliance with information security policies and regulatory requirements will be reviewed by the Risk & Audit committee.

7. Continually improve the company ISMS based on customer and employee feedback, incidents, key performance indicator results, audit findings and technologies:

Measurement: Improvement initiatives will be tracked using key performance indicators (KPIs), such as incident frequency, audit findings, and employee feedback. Regular reviews of audit reports, customer feedback, and incident data will drive continuous improvement.

Responsibility: The Risk & Audit Committee and department heads, will lead the process of continual improvement.

Timeline: Continuous improvement activities will occur throughout the year. Formal reviews and updates to the Information Security Management System (ISMS) will take place annually, with adjustments made as new information or feedback is received.

Evaluation: Evaluation will focus on progress against established KPIs, the effectiveness of improvements made, and the overall reduction in incidents or risks. Results will be reviewed during annual ISMS reviews by the Risk & Audit Committee.

c) The achievement of these security objectives will be supported by the application of security safeguarding controls & control objectives for the purpose of the management of risk to the CONFIDENTIALITY, AVAILABILITY, and INTEGRITY of the in-scope information assets. These safeguarding controls are detailed within the company's Statement of Applicability (SOA).

4. RESPONSIBILITIES

a) The Sota Solutions Executive Management Board is responsible for reviewing and approving the content and implementation of this policy.

b) The Sota Solutions Risk & Audit Committee are responsible for taking measures to ensure all staff members, contractors, third parties and clients are aware of this policy. All staff members, contractors, third parties and clients are required to comply with the policy requirements and share responsibility for its implementation when operating on behalf of the company or within its operating environment.

c) The Sota Solutions Executive Management Board, Senior Management Team and all staff members, clients, contractors and third parties, are expected to take responsibility for the security of company and customer information assets at all times.

5. IMPLEMENTATION

a) The company will maintain its ISMS as a documented system with defined policies, processes and procedures. All documentation that is in-scope of the ISMS will be subject to review under the company's standard Management Review Procedure and subject to version control. All ISMS policies, procedures and documents will be accessible by all staff via the company SharePoint site.

b) The company will operate a risk assessment and treatment methodology in accordance with the international standard ISO / IEC 27005: this methodology is documented in the company's Risk Management Process.

c) The company will ensure both adequate and appropriate resources are made available to establish, implement, maintain and improve the ISMS.

d) The company will conduct formal internal audits of its ISMS in accordance with its planned audit schedule.

e) The company will assess the continuing suitability, adequacy and effectiveness of its ISMS via its Management Review Procedure.

f) Policies relating to specific areas of the company ISMS are recorded in the following documents:
- Acceptable Use Policy - Corporate Mobile Device Acceptable Use Policy - Information Communications Systems
- Access Control Policy
- BYOD Policy
- Contact with Authorities & Suppliers
- Employmet Commencement Policy
- Employment Termination Policy
- Encryption & Cryptographic Controls Policy
- Information Backup and Restore Policy
- Information Classification & Media Handling Policy
- Information Security - Supplier Relationships Network Security Policy
- Password Policy
- Removal Media Policy
- Secure Desk Policy
- Secure Incident Reporting Policy
- Teleworking & Remote Working Policy

6. DOCUMENT OWNER & APPROVAL

The Chief Executive Officer is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the ISMS.

- The current version of this document is available to members of staff on the company SharePoint site.
- This document is approved by the Executive Management Board on the date shown and is issued on a version controlled basis.
- Any subject area mentioned in this policy for which you cannot find a supporting procedure should be brought to the attention of the Compliance Manager. The document is subject to on-going review and any changes will be notified to staff as and when they are made.

6.1 Change History Record

Issue	Description of Change	Author	Date of Issue
1.0	Updated for publishing	Head of Technical	17/06/2016
2.0	Minor update	Head of Technical	23/06/2016
2.0	Updated links	Head of Technical	19/09/2016
3.1	Review and Update	Head of Technical	02/05/2017
3.2	Changes to section 6	Head of Technical	30/11/2017
3.3	Minor amendments	Head of Technical	08/05/2018
4.0	Minor amendments	Head of Technical	26/07/2019
4.1	Publication	Kelly Sears	12/08/2019
4.2	Branding	Ben Smoker	07/12/2020
4.3	Add signature to policy	Ben Smoker	30/09/2021
4.4	Annual Review	Ben Smoker	03/01/2023
4.5	Minor Amendments	Kelly Sears	30/08/2023
4.6	Annual Review	Kelly Sears	03/01/2024

4.7	Minor Amendments	Kelly Sears	11/04/2025
4.8	Formatting	Kelly Sears	14/04/2025
4.9	Amendment to document owner	Kelly Sears	07/05/2025
4.10	Minor amendmens to objectives	Kelly Sears	02/07/2025