sota

INFORMATION SECURITY POLICY

Document Control
Reference: ISMS POL 2.1
Issue No: 4.1
Issue Date: 07-Dec-2020
Classification: Controlled

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 27001:2013.

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.

2. To ensure that all information collected, held and used by the company in support of the in-scope services, is appropriately protected and available in line with business requirements.

3. To ensure that information shared with third parties is protected against unauthorised disclosure and is managed in accordance with the company's information security policies.

4. To maintain employee awareness of information security, thereby ensuring that all employees acknowledge its importance to the company and are aware of their own individual responsibilities for information security.

5. To ensure that all breaches of information security, actual or suspected, are reported to and investigated by the Chief Information Security Officer (CISO), who has direct

responsibility for maintaining this policy and providing advice and guidance on its implementation.

6. To provide documentary evidence, in the form of records, to show that information security policies and processes are being followed correctly and appropriately.

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

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 Senior Management Team members are responsible for taking measures to ensure all staff members, contractors, third parties and clients are aware of this policy.

c) 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.

d) 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
- Employment 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
- Removable Media Policy
- Secure Desk Policy
- Security Incident Reporting
- Teleworking & Remote Working Policy

6. DOCUMENT OWNER & APPROVAL

The Managing Director 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 Head of Technical Services (Information Security 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