Top-level Information Security Policy

1 Purpose

Solidatus takes information security seriously and will at all times ensure that its operations comply with the highest prevailing industry best practices, applicable laws and regulations, and other security requirements. Solidatus also recognises the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, employees and other stakeholders. This document defines the information security policy of Solidatus.

1.1 Definition of information security

Information security is Solidatus' ability to ensure business success by upholding the following principles:

Confidentiality: information is not made available or disclosed to unauthorised individuals, entities or processes

Integrity: protection of accuracy and completeness of information

Availability: Information and associated information assets are accessible and useable when demanded by authorised individuals, entities or processes

Operational resilience: Continuity of operations and services at predefined acceptable levels after occurrence of disruptive incidents

Continual improvement: sustained enhancement and improvement in the effectiveness of Solidatus' information security capabilities

2 Scope

This policy applies to:

- everyone working for Solidatus, meaning permanent, fixed term, or temporary staff, and any third-party representatives, subcontractors, agency workers, volunteers, interns, or agents engaged with Solidatus who have access to Solidatus information systems (referred to as 'personnel', 'interested party' or 'user' in this document)
- all Solidatus systems, hardware, data, databases, cloud-based systems, computer systems, equipment, and software used by personnel working for Solidatus for storing, processing or transmitting Solidatus information
- Solidatus information, information of its employees and everyone working for Solidatus, and information of Solidatus customers and third parties that is processed, stored, or transmitted by Solidatus. The terms 'data' and 'information' are used interchangeably in this document as the context requires

3 Information security requirements and objectives

A clear definition of the requirements for information security within Solidatus will be agreed upon and maintained in connection with the customers and other stakeholders we work with so that all information security management activities fulfil such requirements. These include legal, regulatory, and contractual as well as project specific security requirements.

A security risk assessment will be carried out to identify the level of protection required. The security and control procedures will take into account the sensitivity and value of information. Success against these targets will be evaluated as part of the management review process.

4 Framework for Setting Objectives

Information security objectives will be set out in accordance with the ISMS Governance, Risks and Compliance Framework.

Information security objectives will be documented for an agreed duration together with necessary details for proper implementation. The objectives will be evaluated and monitored as part of management reviews.

5 Board commitment

This information security policy is approved and sponsored by the Board of Threadneedle Software Holdings Ltd and is applicable to all group entities as defined within the ISMS Information Security Governance Framework. The Board is committed to the success of our information security management system. It will allocate adequate resources, including personnel, technology, and financial resources, to establish and maintain an effective information security management system. Our commitment to information security extends to all levels of the organization. We will ensure that all employees, contractors, and third-party vendors are aware of and comply with our information security policies and procedures. We will continually review and improve our information security policies and practices to ensure they remain relevant and effective in light of evolving risks and threats.

This policy shall be reviewed at least annually and when there are significant changes to the internal and external operating environment of Threadneedle Software Holdings Ltd to ensure it remains fit for purpose. Any changes to, exceptions to or deviations from this policy shall be in writing and authorised by the Board. Where applicable, a risk assessment shall be performed and documented before an approval is granted.

Further topic-specific policies, standards, procedures, and processes to implement information security controls and to address specific functional areas/target groups within the organisation shall be published. All these documents shall support this top-level information security policy and the information security principles defined herein.

6 Revision History

VERSION NO.	DATE ISSUED	BRIEF SUMMARY OF CHANGE	APPROVED BY
V1.0	28/05/2018	Document approved and issued	Board
V2.0	05/10/2020	Pre CE+ Audit	Board
V3.0	25/01/2023	Changes in line with ISO27001 & CCM implementation	Board
V3.1	24/04/2023	Minor changes	Daniel Waddington