STEPHEN AUSTIN
EST 1768

BY APPOINTMENT TO HER MAJESTY THE QUEEN PRINTERS STEPHEN AUSTIN & SONS HERTFORD, ENGLAND

# Information Security Policy

Stephen Austin is committed to protecting the security, confidentiality and integrity of our clients' data and documentation throughout our organisation. Information security will continue to be aligned with Stephen Austin's objectives and our Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information security risks to acceptable levels.

Stephen Austin's current risk management framework provides the context for identifying, assessing, evaluating and controlling information related risks through the implementation of an ISMS, which is compliant with the requirements of ISO 27001: 2013. The risk assessments, statement of applicability and risk treatment plan within the ISMS identify how information related risks are controlled. The Systems and Compliance Manager is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data back-up procedures, anti-virus systems, access controls to systems and information security incident reporting are fundamental to this policy. Controls for each of these areas are contained within the ISMS, supported by specific documented procedures and policies.

Stephen Austin aims to achieve specific, defined security objectives, which are in line with the context of our organisation. We are committed to achieving and maintaining certification to ISO 27001: 2013.

All employees, subcontractors and certain external parties identified within the ISMS are expected to comply with this policy and with the ISMS itself, that implements this policy. All employees and subcontractors and certain external parties will receive the appropriate information security training.

The ISMS is subject to continued, systematic review and improvement. This policy will be reviewed at least annually, in line with any organisational changes, or changes to information security risk assessments.

David Cockram
Managing Director

Document ID : SACOMPLIANCE012
Approver: Managing Director
Author: Systems & Compliance Manager
Classification: Public
Revision: 3.0
Issue Date: 25.03.19