

The Board of Directors and management of SAS International, located at 31 Sutton Business Park, Reading, Berkshire RG6 1AZ, and all manufacturing subsidiaries, which operates in the manufacturing sector, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with SAS International's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

SAS International's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Head of Risk 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 backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Business Management System and are supported by specific documented policies and procedures.

SAS International aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of SAS International and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive or are required to provide appropriate training. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

SAS International has established an Information Security Committee, chaired by Chief Information Security Officer (CISO) and including the Information Security Manager and other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

SAS International is committed to achieving compliance of its ISMS to ISO27001:2013 and the GDPR.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

## Preserving

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security



# INFORMATION SECURITY POLICY

awareness training and more specialised Employees/Staff will receive appropriately specialised information security training.

**the availability,**

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and SAS International must be able to [detect and] respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans. [Add any other specific control/compliance requirements.]

**confidentiality**

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to SAS International's information [and proprietary knowledge] and its systems [including its network(s), website(s), extranet(s), and e-commerce systems]. [Add any other specific control/compliance requirements.]

**and integrity**

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency [including for network(s), , website(s), extranet(s)], intranet(s) and data backup plans and security incident reporting. SAS International must comply with all relevant data-related legislation in those jurisdictions within which it operates. [Add any other specific control/compliance requirements.]

**of the physical (assets)**

The physical assets of SAS International including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

**and information assets**

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

**of SAS International.**

SAS International and [such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS].

**The ISMS** is the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO 27001:2013.

**A SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of SAS International.

	<p>SAS INTERNATIONAL 31 Sutton Business Park, Reading, Berkshire, RG6 1AZ <a href="http://www.sasintgroup.com">www.sasintgroup.com</a> Comments to <a href="mailto:DPO@sasint.co.uk">DPO@sasint.co.uk</a></p>	<p><b>Document Control</b> Reference: GD5.011 Issue No: 1 Issue Date: 18/05/18 Page: 2 of 3</p>
--	---	---

## 1 Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the GDPR.

A current version of this document is available to all data subjects and staff on the website, company intranet and is published [        ].

This policy was approved by the Board of Directors and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

Signature: 

Date: 22<sup>nd</sup> May 2018.

## 2 Change History Record

ISSUE:	DESCRIPTION OF CHANGE:	DATE:	APPROVAL: