Information Security Policy

Document Control
Reference: Information Security Policy
Issue No: 1
Issue Date: 18/08/2017

The Board of Directors and Management of iSAMS Ltd located at 9 Talavara Court, Darnell Way, Northampton, NN3 6RW, which operates in the education sector in the business of software development, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation and services in order to maintain 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 iSAMS Ltd's goals and the ISMS (Information Security Management System) is intended to be an enabling mechanism for information sharing, electronic operations and for reducing information-related risks to acceptable levels.

iSAMS Ltd'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. The Data Protection Officer 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 manual and are supported by specific documented policies and procedures.

iSAMS Ltd 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 iSAMS Employees, contractors, consultants and any external parties or organisations that may be identified in the ISMS shall comply with this policy. The ISMS is subject to continuous, systematic review and improvement.

iSAMS Ltd has established a Management team with representatives from all relevant business units and includes the Data Protection Officer (DPO) to support the ISMS framework and to periodically review the security policy.

iSAMS Ltd is committed to achieving certification of its ISMS to ISO27001:2013.

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

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

Preserving

This means that management, all employees, contractors, 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 will receive information security awareness training and more specialised employees 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 iSAMS Ltd must be able to detect, 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.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it, therefore preventing both deliberate and accidental unauthorised access to iSAMS Ltd's information and client information and its systems.

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, data backup plans and security incident reporting. iSAMS Ltd must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of iSAMS Ltd including, but not limited to, computer hardware, data cabling, 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, 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 iSAMS Ltd

iSAMS Ltd 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, the Information Security Manual and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

The consequences of breaching the information security policy are set out in the Organisation's disciplinary policy and in contracts and agreements with third parties.

Document Owner and Approval

The Head of Service and Operations is the owner of this document and is responsible for ensuring that this policy document is reviewed.

A current version of this document is available to all members of staff on the corporate network and HR system. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board of Directors on 18/8/17 and is issued on a version controlled basis under the signature of the Managing Director.

Signature: Alastair Price Date: 18/8/17

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Alastair Price – MD	18/08/2017