Information Security Policy

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this Manual.

When any part of this Manual is amended, a record is made in the Amendment Log shown below. The Manual can be fully revised and re-issued at the discretion of the Management Team.

Issue	Issue Date	Additions/Alterations	Initials
1.0	01/05/18	First Authorised Issue	BC
1.1	12/11/18	Reformatted doc, added Appendix with relevant legislation	BC

Introduction

essensys is committed to achieving and maintaining the trust of our customers. Integral to this mission is our commitment to preserve the confidentiality, integrity and availability of all the physical and electronic information assets throughout our organisation. essensys' integrated business management systems (IBMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

To safeguard the security of its data assets, as well as those of any third parties the company interacts with, essensys continually reviews the IBMS to ensure they are compliant with the ISO/IEC 27001 standard for information security management.

essensys has voluntarily chosen to comply with the internationally recognised ISO/IEC 27001 standard. It provides a stable framework to help the company balance efficiency with security as it increases in size. By adhering to the standard's rigorous set of requirements, essensys has been able to establish a highly organised, risk-based methods of managing personnel, IT systems and processes in a way that ensures sensitive data is protected.

Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all essensys information systems (including but not limited to all Cloud environments commissioned or run by essensys, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
    a. This explicitly includes any ISO27001-certified Information Security Management Systems the business may run.
    b. The resources required to manage such systems will be made available
    c. Continuous improvement of any IBMS will be undertaken in accordance with Plan Do Check Act principles
2. Make certain that users are aware of and comply with all current and relevant UK, EU and US legislation.
3. Provide the principles by which a safe and secure information systems working environment can be established for employees and any other authorised users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect essensys from liability or damage through the misuse of its IT facilities.
6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

Scope

The scope of this policy covers the following areas:

- All departments within the company and all of its assets
- The London and New York offices and the policies and procedures within the essensys IBMS that affect home and remote workers
- Interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations
- All interested parties including any contractual, business, legal or regulatory requirements for essensys, with the exception of any historical contracts that do not

fully take account of the essensys IBMS. In such cases the company will, on an ongoing basis, seek to update contracts as they renew (or earlier as decided by the business) so that they are in scope.

Information Security Principles

The following information security principles provide overarching governance for the security and management of information at essensys.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements.

2. Staff with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on the basis of *least privilege* and *need to know*.

5. Information will be protected against unauthorized access and processing in accordance with its classification level.

6. Breaches of this policy must be reported

7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.

8. Any explicit Information Security Management Systems (ISMS) run within the business will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001 clause 10.

Legal & Regulatory Obligations

essensys has a responsibility to abide by and adhere to all current UK, EU and US legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in *Appendix A*.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below.

Suppliers

All suppliers will abide by the Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing essensys assets, whether on site or remotely
- when subcontracting to other suppliers.

Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of essensys information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes essensys' Data Protection Policy, and may result in criminal or civil action against the business.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against essensys. Therefore, it is crucial that all users of the information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.

All current staff and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

Any security breach will be handled in accordance with the data breach policy.

Incident Handling

If a member of staff is aware of an information security incident, then they must report it to their department head. Additional information can be found within the Information Security Incident Management policy.

Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available on essensys' Sharepoint.

All staff and any third parties authorised to access essensys' network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

Review and Development

This policy, and its subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies. The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems

essensys' Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The CIO is responsible for the management and maintenance of the risk treatment plans. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks that would usually be identified on the risk register.

The COO (accountable) shall, with the Head of Infrastructure (responsible), execute and maintain business continuity and contingency plans.

For essensys data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this Information Security Policy. All of these areas are covered in the essensys IBMS and are supported by its policies and procedures.

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 are made aware of their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (as per the controls from section 16 of Annex A and the supporting policies, processes and procedures for them) and to act in accordance with the requirements of the IBMS. All Employees/Staff will receive information security awareness training and more specialised Employees/Staff will receive appropriately specialised information security training.

Availability
This means that information and associated assets should be accessible to authorised users when required and not available to unauthorised individuals and therefore physically secure. The computer network is resilient and essensys is able to respond to incidents according to agreed service levels (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There are appropriate business continuity plans in place for identified scenarios.

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 essensys' information and its systems (file servers, networks, data repositories, telephony systems and websites).

Integrity
This involves safeguarding the accuracy and completeness of information and processing methods and therefore, requires reasonably reducing the chance of deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data, taking account that the cost of implementing security controls should not outweigh the benefit of them to the business. There are appropriate contingency plans for all systems, data backup plans and security incident reporting. essensys complies with all relevant data-related legislation in those jurisdictions within which it operates.

Physical (assets)
The physical assets of essensys include, but are not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

Information assets
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), intranet(s), PCs, laptops, mobile phones, as well as on DVDs, USB sticks 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.).

Appendix A: Summary of relevant legislation

The Computer Misuse Act 1990
Defines offences in relation to the misuse of computers as:
1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

The Freedom of Information Act 2000
The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996
"Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm."

Obscene Publications Act 1959 and 1964
The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

Terrorism Act 2006
The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.
It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.
In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

General Data Protection Regulation
The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect implementation of the GDPR. The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover.
The GDPR requires essensys to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in and can also easily opt out. It requires data breaches to be reported to the Information Commissioner's Office within 72hrs of essensys becoming aware of their existence.