Information Security Policy

Information Security Policy with IG Implications

1 Policy

The Directors and management of Aseptika Limited (Aseptika), located at St Ives, Cambridgeshire, United Kingdom, 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 Aseptika's goals and information security management arrangements are intended to be an enabling mechanism for information sharing in accordance with legal and regulatory requirements, for electronic operations, and for reducing information-related risks to acceptable levels.

Aseptika's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks. Risk assessment and risk treatment processes identify how information-related risks are controlled. The Managing Director is the Senior Information Risk Owner and responsible for the risk management framework.

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. Specific policies and procedures support this policy.

Aseptika 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 staff and contractors of Aseptika are expected to comply with this and supporting security policies. All staff, and certain external parties, will receive 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 security arrangements are subject to continuous, systematic review and improvement.

Aseptika has established a management meeting chaired by the Managing Director to support information security arrangements.

Aseptika is committed to achieving and maintaining compliance with NHS security and confidentiality requirements and compliance with the GDPR.

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

2 Definitions

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

Preserving

This means that management, all full time or part time 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 Aseptika. All staff will receive information security awareness training and more specialised 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 Aseptika 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.

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 Aseptika's information and proprietary knowledge 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 and data backup plans and security incident reporting. Aseptika must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Aseptika 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, 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 Aseptika Ltd.

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 Aseptika.

3 Document History

Document History

Version	Date released for approval	Contributors Initials	Reviewers Initials	Changes from Previous Version
v1.0	21/1/18	GL		First Draft
v1.1	21/1/18	KAA		Text corrections
v1.2	23/1/18	JMA		Aseptika Formatting corrections
V1.3	9/2/18	JMA		Added Document Control Page
V1.4	23.02.2018	JMA		Updated for signing
V1.5	28.02.2019	KAA		Revision as a PUBLIC document for website
V1.6	03.05.2018	ETRA		Updated to new template and new document number
V2.0	11/12/2018	ETRA	KAA, JAA, CB	Annual review and part of CC2018-0187