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 the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory, contractual compliance and commercial reputation.

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 provides the context for identifying, assessing, evaluating and controlling information-related risks. Risk assessment and risk treatment processes identify how information-related risks are controlled by Aseptika. The Managing Director is the Senior Information Risk Owner (SIRO) 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 and clinical risk assessments and the risk treatment plan.

All staff and contractors of Aseptika are expected to comply with this and support 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.

Aseptika's security arrangements are subject to continuous, systematic review and improvement.

Aseptika has established an IG Improvement management meeting, chaired by the Managing Director, to support information security arrangements.

Aseptika is committed to achieving and maintaining compliance with NHS Data Security & Protection Toolkit (DSPT), NHS Digital Technology Assessment Criteria (DTAC), Cyber Essentials Plus and other NHS security and confidentiality requirements and compliance with the UK GDPR, where appropriate EU GDPR.

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

2 Definitions

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

Preserving means that management, all full-time or part-time staff, sub-contractors, project consultants and any external parties have and are 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.

Availability 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 is 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 is an appropriate business continuity plan in place.

Confidentiality involves ensuring that information is only accessible to those authorised to access it and, therefore, to prevent both deliberate and accidental unauthorised access to Aseptika's information and proprietary knowledge and its systems.

Integrity 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 are appropriate contingency and data backup plans and security incident reporting. Aseptika complies with all relevant data-related legislation in those jurisdictions within which it operates.

Physical (assets) is the physical assets of Aseptika including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

Information assets are the information assets, including information printed or written on paper, transmitted by post, 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, 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).

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 References

ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems
BS EN ISO/IEC 27701:2021	Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
ISO 27033-6 IEC/EN 2016	Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems
BS EN ISO/IEC 27701:2021	Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
WCAG 2.1	Web Content Accessibility Guidelines 5 June 2018
NHSx DTAC	Digital Technology Assessment Criteria
NHS	The Information Security Management: NHS Code of Practice April 2007
NHS DSPT	NHS Data Security & Protection Toolkit
Cyber Essential	Cyber Essentials & Cyber Essentials Plus
ICO.org	Personal data breaches: Information Commissioners Office
ICO.org	The Information Commissioner's Office (ICO) Guide to Data Protection
MDCG 2019-16 Rev.1	Guidance on Cybersecurity for medical devices

4 Document History

Version	Date	Authors Initials	Reviewers Initials	Changes from Previous Version	Authorised by & date
1.0	21/1/18	GL		First Draft	
1.1	21/1/18	KAA		Text corrections	
1.2	23/1/18	JMA		Aseptika Formatting corrections	
1.3	9/2/18	JMA		Added Document Control Page	
1.4	23.02.2018	JMA		Updated for signing	
1.5	28.02.2019	KAA		Revision as a PUBLIC document for website	
1.6	03.05.2018	ETRA	MP	Updated to new template and new document number	KAA
2.0	11/12/2018	ETRA	KAA, JAA, CB	Annual review and part of CC2018-0187	
3.0	02.12.2019	JA	MP	MDR Transition update, part of CC2019-057	Kevin Auton
4.0	29.10.2020	JA	MP	Update as per CC2020-059	KAA
5.0	22.11.2021	JA	GE	Annual review CC2021-075	Kevin A Auton 23.12.2021
6.0	07.03.2022	JA	GE	Update language CC2022-018	Kevin Auton 18.03.2022
7.0	01.07.2022	JA	GE	Update CC2022-041	KAA 04.07.2022
8.0	27.10.2022	JA	GE	Migrate to AWS CC2022-063	KAA authorise JA 02.11.2022