INFORMATION SECURITY POLICY

AUTHOR	Tiffany Duncan
APPROVER	Lyn Hodges
APPROVAL DATE	20/03/2024
CLASSIFICATION	PUBLIC

Document Control Box

Version	Author	Changes made	Approved by	Date
Draft		Created by CL		
1.0	LH	Final version	LH	2018-05
1.1	TD	Classification matrix added to document control page	LH	2020-03
2.0	LH	Revised document and addition of operational process flow.	LH	2020-07
2.1	TD	Removal of Document process flow, first paragraph text page 2 and reference to amendment form in control box	LH	2020-08
3.0Draft	TD	3.0Draft changes to wording around GDPR		Mar_21
3.0		Draft approved, final document	LH	Mar_21
4.0Draft	TD	Addition of sentence re: supplier compliance		Apr_21
4.0		4.0 draft approved	LH	Apr_21
4.1	TD	Amendment to text in Doc control box and review date replaced with approval date and addition of External Classification		August_20_21
4.2	TD	Removal of ASE 03 ref as no longer required see doc control procedure.		Nov_21
4.3	TD	Document reviewed.	LH	April_13_2022
5.0	TD	Amendment in line with NC legislation and ISO 27001 context.	LH	September, 20,2022
5.1	TD	Move document to new template otherwise no changes		13/04/2023
5.2	TD	Document reviewed – no changes	LH	19/09/2023
6.0	TD	Addition of title and content – ISMS Objectives	LH	20/03/2024

Table of Contents

Purpose and Scope

This information security policy, which is sponsored by our Information Security Committee (ISC), sets out the framework for how we set our information security objectives, how we translate these into our information security controls, and how we govern our information security objectives.

ASE Corporate Eyecare is committed to safeguarding the security of the information with which it is entrusted, to complying with relevant data protection legislation, to meeting the information security requirements of its customers and partners, and to embedding security consciousness and continuous improvement throughout its people, processes and technology.

Responsibility

ASE recognises its legal and financial obligations relating to its operations with all stakeholders. Our Information Security Committee (ISC) are committed to the continuous improvement of sustainability of its management systems throughout the organisation.

The ISC will be responsible for working with our technology partners to establish the individual security control objectives with reference to our overall risk treatment plan and relevant guidelines and standards.

Our ISC has responsibility for development, management and evaluation of our information security management system (ISMS).

Our ISC will ensure full legal compliance at all times including all statutory Acts, Regulations and associated Approved Codes of Practice. Including the Health & Safety at Work etc Act (1974) and Environment Protection Act (1990). The ISC will also ensure compliance is maintained against the ISO 27001:2013 Information Security Management Systems and the Data Protection Act 2018 as well as all other primary legislation for our activities. We will also ensure competency of those providing goods and services into ASE.

The ISC will also ensure adherence and compliance with agreed supplier and client commercial contracts.

This ISC shall report to the board on information security issues and will ensure that our information security objectives are in line with our overall business strategy.

Periodically, and at least once per year, the ISC will evaluate the context of our organisation, the issues we face both strategically and operationally, and conduct a risk assessment and treatment process to identify our information security objectives at a high level.

ASE will seek compliance with all stakeholders, customers, suppliers, 3rd party contractors.

Operational Controls

ISMS Objectives

The ISMS Objectives have been set to ensure the principles of confidentiality, integrity and availability are considered and measured. Therefore, our objectives are agreed and approved by the Information Security Committee (ISC) annually. Details of the objectives, measures, targets and review frequency including responsibilities for evaluation are logged and maintained in the Objectives Tracker which is reviewed at the quarterly management reviews by the ISC.

Compliance with the Data Protection Legislation

The ISC, in line with our commitment to conform to the DPA will be responsible for maintaining and reviewing the documentation and processes required under the legislation. This information will be communicated to staff and made available to our clients and data subjects as a published Statement of Compliance.

Communication

The ISC is responsible for overseeing the communication of this policy to staff and to interested parties, and shall nominate an appropriate member to be responsible for this day-to-day

Review

Periodically, and at least once per year, the ISC will review this policy to ensure that it continues to support our commitment to information security, and complies with relevant legislation.

Exceptions

All exceptions to this Document will have to be authorised by the Managing Director.