IT Security
Information Security Management System
ISMS Statement

Policy Classification: IG & IT	**Policy Issue No:** Issue 2.4
Last Review Date: December 2024	**Last Reviewed By:** IT Director/Governance and Risk Manager/Director of Transformation and SIRO
Initial Date Issued: December 2021	**Written By:** IT Director
Approved By: Operose Health Executive Team	**Status of Document:** Final - Controlled
Date of approval: 16 June 25	
Next Review Due Date: December 2026	**Page No:** 1 of 2

Document Control

This is a CONTROLLED document and updates or changes to this document are authorised and then advised by email to the relevant document holders.
It is UNCONTROLLED when printed.
You should verify that you have the most current issue.

INFORMATION SECURITY MANAGEMENT STATEMENT

Scope of the Statement

The scope of this Information Security Management System (ISMS) Statement relates to the use of databases and computer systems operated by **Operose Health** in pursuit of the organisation's business in working with complex health systems to provide the very best healthcare service to patients and services users, and to transform their quality of healthcare experience. It also relates where appropriate to external risk sources including functions which are outsourced.

Operose Health will maintain an information security management system designed to meet the requirements of ISO 27001 in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of **Operose Health** to:

- Make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the business management system.
- Comply with all legal requirements, codes of practice and all other requirements applicable to our activities; therefore, as a company, we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.
- Provide all the resources of equipment, trained and competent staff and any other requirements to enable these objectives to be met.
- Ensure that all employees are made aware of their individual obligations in respect of this information security policy.
- Maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on "risk".

This ISMS statement provides a framework for setting, monitoring, reviewing and achieving our objectives, programs and targets.

To ensure the organisation maintains its awareness for continuous improvement, the Business Management System (BMS) is regularly reviewed by the organisation's Executive Team to ensure it remains appropriate and suitable to the organisation's business. The BMS is subject to both internal and external annual audits.

The following policies relate to the management of information security systems and together underpin the organisation's information security assurance framework:

- CG-POL-Information Governance Policy
- CG-POL-Acceptable Use of Information Technology Policy
- CG-POL Information and Cyber Security Policy
- CG-POL-Data Management Policy
- CG-POL-Incident Management Policy
- CG-POL-Intellectual Property and Copyright Policy
- CG-POL-Media Policy
- CG-POL-Transportation of Records Policy
- CG-POL-Freedom Of Information Policy
