QMS and ISMS POLICY

Issue	Issue Date	Additions/Alterations	Initials
1.0	21 Dec 2017	Taken from the latest version of QMS manual	SD
2.0	30 Jun 2023	Taken from the latest version of integrated QMS and ISMS manual	SD
3.0	29th April 2024	Updated ISMS policy	WE
4.0	30th Apr 2024	Updated Quality policy	SD
5.0	1 May 2024	Signed by the top management	SD
6.0	2 May 2025	Reviewed and signed by the top management	SD

QMS Policy

It is the policy of Claromentis Ltd. to maintain a quality system designed to meet the requirements of ISO9001:2015 & ISO 27001 (or any other standard in line with Annex SL Structure)in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of Claromentis Ltd. to:

- strive to satisfy the requirements of all of our customers, stakeholders and interested parties whenever possible, meeting and exceeding their expectations;
- 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. These include but not limited to customers and clients and their requirements are documented in contracts, purchase order and specifications etc;
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities;

- 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 quality and 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 quality and information security policy provides a framework for setting, monitoring, reviewing and achieving our objectives, programmes and targets.

Customer service is an essential part of the quality process and to ensure this is fulfilled, all employees receive training to ensure awareness and understanding of quality and information security and its impact on customer service.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by “Top Management” to ensure it remains appropriate and suitable to our business. The Business Management System is subject to both internal and external annual audits.

ISMS Policy

The Senior managers of Claromentis are committed to the following core ISMS policy:

- The implementation and maintenance of an ISMS that is independently certified as compliant with ISO 27001:2022;
- Commitment to remain ISO 27001:2022 compliant by submitting to external audits, which should be verified by a UKAS accredited assessor.
- The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures;

- Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures;
- The maintenance of a risk treatment plan that is focused on eliminating or reducing security threats;
- The maintenance and regular testing of a Business Continuity Plan for the business and individual Disaster Recovery plans for key infrastructure.
- The clear definition of responsibilities for implementing the ISMS;
- The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties, and can support the implementation of the ISMS;
- The implementation and maintenance of the sub-policies detailed in the ISMS.
- The appropriateness and effectiveness of this policy, and the means identified within it, for delivering the organisation's commitments will be regularly reviewed by Top Management.
- The implementation of this policy and the supporting sub-policies and procedures is fundamental to the success of the organisation's business and must be supported by all employees and contractors who have an impact on information security as an integral part of their daily work.
- All information security incidents must be reported via 'Incident Report' form. Violations of this policy may be subject to the organisation's Disciplinary and Appeals Policy and Procedure.

Top Management

Michael Christian	Nigel Davies	Stas Dreiling	Will Emmerson
			
06/05/2025	02/05/2025	02/05/2025	06/05/2025