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
7.0	30 Apr 2026	Removed references to QMS policy and signed by the top management	SD

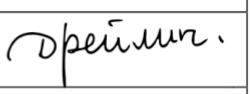
ISMS Policy

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:

Name	Michael Christian	Nigel Davies	Will Emmerson	Stas Dreiling
Job title	CTO	CEO	CIO	COO
Signature				
Date	30 Apr 2026	30 Apr 2026	30 Apr 2026	30 Apr 2026