5.0.1 Quality Policy

The Quality Policy of CLS Data is as follows:

- Satisfy the requirements of all customers, stakeholders and interested parties whenever possible meeting and exceeding their expectations;
- Comply with all legal requirements, codes of practice and all other requirements applicable to our activities;
- To reduce hazards, prevention of injury, ill health and pollution;
- Provide trained and competent staff alongside all the resources of equipment to enable these objectives to be met;
- Ensure that all employees are made aware of their individual obligations in respect of this quality policy;
- Maintain a management system that will achieve these objectives and seek continuing improvement in the effectiveness and performance of our management system based on "risk".

Adam Harmer
Director and Quality Manager
03/10/2022

5.1.1 Information Security Policy

The ISMS Policy of CLS Data is as follows:

The implementation and maintenance of an ISMS that is independently certified as compliant with ISO 27001:2013;

- 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**;
- 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 this policy;
- 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 to top management. Violations of this policy may be subject to the organisation's **Termination Procedure.**
- Ensure that all employees are made aware of their individual obligations in respect of this information security policy.

Adam Harmer
Director and Quality Manager
03/10/2022