ML Doctors

Information Security Management System (ISMS) Policy

Document Ref:	ISMS12
Version:	1.2
Date of version:	17/10/2019
Author:	S Densley
Approved by:	M Zia
Confidentiality level:	Public

We have chosen to adopt the principles defined in ISO27001 (2013) Information Security Management Systems, as a demonstration of our commitment to maintaining data and information security.

The nature of our business necessitates the transfer, use and storage of confidential information about individuals. Taking into account legal, regulatory and contractual security requirements, our objectives areto ensure that the information we use is accessed, communicated, stored and used in such a way so as to prevent its inadvertent use, loss, theft or corruption by any parties outside of our normal operations. The objective of ISMS are to;

- Maximise ML Doctors information confidentiality
    - Reduce Security Events and Weaknesses; Our aim is 0 security incidents as described in later sections of this manual. When an event or incident occurs we report, investigate and learn
    - Log all security events, prevent them turning into an incident; When an event is logged (where a potential for information breach is discovered but information confidentiality, availability and integrity has not been altered).
- Increase operational availability
    - The availability of our IT systems is crucial to our success. We strive for 100% system up time. We do this by recording incidents and continually improving our IT systems.
- Improve commercial contracts
    - Win larger contacts with suppliers by demonstrating our commitment to information security.

These objectives are measured and reviewed at management review. To achieve our objectives ML analys and measured the risks associated with our operations and processes and the impact these may have on our clients and suppliers. We have implemented methods, safeguards and procedures to mitigatethoserisks. These are defined in our ISMS Manual, and all staff have been trained to understand and utilise the security measures as part of their day-to-day activities.

Any incident which may compromise the ISMS will be fully recorded on our NC Log and corrective actions taken to prevent further repetition. If necessary these will be notified to the appropriate regulatory body should this be deemed necessary. Non-Conformance statistics will be discussed at monthly board meetings and any additional requirements (such as training or briefings) will be agreed and actioned.

Our ISMS arrangements will be regularly tested and measured by way internal and external audits. Results of which will be reviewed by the Directors to strive to continually improve our security arrangements and make available appropriate resources to ensure this is a continual process.

M Zia

Director

17/10/2019