Direct Life Accredited with ISO 27001

What is ISO 27001?

ISO 27001 is an international standard that provides the specification for an Information Security Management System (ISMS).

We've all talked at management meetings about data security and cyber threats, but how many of us have tried to logically identify and assess all these risks, including human errors, and then try and create procedures to mitigate and remove these risks?

How we achieved ISC accreditation

Initially we assessed how we would protect and manage all our data using a risk management methodology, as we could see the value of the ISMS helping us conform to recent legislation, including GDPR and NIS Regulations. Following the rigours of the ISO framework we identified that we should protect 3 key aspects of the information we held, in a way that all staff could understand; the Confidentially, Integrity and Availability of our data.

From a Confidentiality perspective, the client needs to know why we are requesting the information, and that it won't be disclosed to wrong people or processes.

The Integrity of the data needs to ensure that the data collected is complete and accurate and is then protected from corruption so that the whole file can be accessed.

Availability means that we have systems that allow us access to the information when an authorised user needs it.

In our business, we deal with 1,000s of customers' application data, which includes sensitive medical data, and other application and bank details. We collect, record, transfer and store this data securely for a suitable amount of time that is relevant to the reason we are holding it.

To give you an idea of the range of requirements these are some of the areas that were reviewed, updated and documented; Information security policies, risk assessment and risk treatment policies, definition of security roles and responsibilities, inventories of applicable assets, access control policies, operating procedures for IT management, supplier security policies, employment screening, business continuity procedures, internal audit procedures, document control, password policy, clear desk and clear screen policy and also network diagrams.

What does this mean to the business, its customers, advisers and staff?

In doing this we have enhanced and improved current areas, reinforcing the good work we have done such as the changes introduced to meet GDPR.

We have created and updated documents, operations manuals, risk registers, asset logs, T&C handbooks to name a just a few. Key to all this was demonstrating that the entire organisation was aware of the importance of the security of data, and understood the procedures that were in place across the business, as well as demonstrating our commitment to ongoing improvement of InfoSec.

We received our certification for ISO 27001 and as a business, we have benefitted enormously from the work done to achieve this, but importantly it reinforces how important it is to keep customer data secure.

Original press release, May 2019, written by Neil McCarthy, Chief Commercial Officer
Neil.McCarthy@DirectLife.co.uk 07957175758

Read more information on the Approachable Certification.

Read more about the ISO 27001 accreditation.