the
typing
works

Information Security Incident Management Policy

We fully recognise the importance of the security of information within our company amongst all our stake-holders, but especially in relation to our clients and customers. As such, we are fully engaged with operating, maintaining and continually improving a relevant Information Security Management System with the long term aim to conform to the current version of ISO 27001.

Top level objectives are established to monitor and measure the efficiency of our Company and to promote the ongoing security of all our information assets, such that:

- Risks associated with the confidentiality, integrity and availability of our own assets and information and that of our interested parties are all comprehensively assessed for any associated information security risks.
- Appropriate controls have been identified and applied to mitigate any loss or damage arising.

All our processes and support functions are routinely audited and reviewed by Senior Management; There is a business continuity plan detailing options to maintain services in the event of a system failure or other occurrence.

We are committed to comply with relevant legislation, regulations and other requirements; All staff understand their obligations in this respect, and have awareness of the potential for breaches of information security and know to report any suspicious activity or error however caused. Any incidents are fully investigated by a Company Director.

Additionally, we welcome every opportunity suggested from any source to develop and improve our management system so that we can enhance our effectiveness through the IMS, and ensure that we remain recognised as a valued and trusted supplier that satisfies the total confidence of our customers.

We believe that it is essential that our Information Security Policy is communicated, understood and applied throughout the company.

This Policy is regularly reviewed and is available to all interested parties.