INFORMATION SECURITY POLICY

Integrity Print Ltd is committed to maintaining and improving information security within the Company and reducing its exposure to risk to ensure the confidentiality, integrity and availability of corporate and client information will be assured.

The purpose of this policy is to ensure that all staff, visitors and contractors to the Westfield site understand Integrity Print's information security requirements to comply with contractual and applicable regulatory and legislative requirements, through the appropriate level of training of our employees and contractors and communicated to interested parties.

Through the continuous improvement of our Information Security Management system (ISMS) we will strive to maintain certification to ISO 27001:2013 standard incorporating C&CCC Standard 55 and the legal requirements of EU GDPR, identifying, assessing, evaluating and controlling information assets to determine the risk and identify objectives to mitigate those threats.

Business Continuity plans for critical activities will be produced, maintained, and tested.

All responsibilities have been defined within the ISMS which will be reviewed annually to respond to any changes within the business. Compliance with Company policies & procedures will be monitored via the Information Security Forum, along with independent review by both internal and external audit on a periodic basis.

All breaches of Information Security will be reported to and investigated by the Information Security Forum.

Managing Director

Integrity define Information Security as follows

To preserve the availability, integrity, and confidentiality of our information assets.

This is achieved by ensuring that all employees, contractors, and third-party suppliers are made aware of their responsibilities to preserve information security, to report security breaches and to act at all times in accordance with the requirements of the ISMS. Responsibilities are detailed in job descriptions and contracts, and all employees receive specific Information Security awareness training.

The confidentiality of Information Assets is preserved by ensuring that they are only accessible to authorized members of staff and the Company's physical and network security controls.

Integrity's networks are tested for resilience and availability and incorporate a robust system of checks that allow us to detect and respond rapidly to incidents that may threaten the availability of assets or information. Servers are backed up on site for additional resilience to ensure appropriate business continuity levels can be maintained. There are appropriate contingency plans in place should a data breach occur, and Integrity will comply with all appropriate legislation for data protection

The integrity of our Information Assets involves safeguarding the accuracy of information and processing methods, preventing the deliberate or accidental modification or destruction of either physical systems or electronic data.

The Integrity ISMS covers the physical assets of the business, including but not limited to, buildings, people, equipment, hardware, networks, telephone systems, filing systems, and data files.

Information Assets include information written or printed on paper, transmitted by post, or shown in film or video, or in verbal communications, as well as information stored electronically on servers or web portals, PCs, laptops and mobile phones and all information transmitted electronically by whatever means.

Integrity have a risk management framework in place to provide the context for evaluating and controlling information related risks through the establishment and maintenance of certification to ISMS. The Risk Assessment, Risk Treatment Plan and Statement of Applicability identify and document how information risks are controlled. Specific documented policies and procedures are used to provide control objectives for each area that is identified as critical to the delivery of a robust ISMS.