



Management Systems
Manual
**INFORMATION SECURITY &
PIMS POLICY**
Level 1 document

Reference	MSP 90
Revision	01
Date	20/02/2018
Page:	1 of 2

Stanmore Group Ltd
Information Security - BS ISO/IEC 27001:2013,
Personal information Management (GDPR)- BS10012-2017

The Company recognises that the disciplines of confidentiality, integrity and availability in Information Security and Personal information Management (GDPR requirements) are integral parts of its management function.

The Management of Stanmore Group Ltd views these as primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls, along the lines laid down in the BS ISO/IEC 27001:2013 and BS10012-2017 standards..

It is the Company's information security and Personal information Management (GDPR requirements) policy to seek to operate to the highest standards continuously and to implement and operate fully to BS ISO/IEC 27001:2013 and BS10012-2017 standards, including continual improvement, through registration and annual review.

The Company will:

- ✓ Comply with all applicable laws and regulations and contractual obligations;
- ✓ Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet information security requirements;
- ✓ Communicate its Information Security and Personal management objectives, and its performance in achieving these objectives, throughout the Company and to interested parties;
- ✓ Adopt an information security management and Personal information management system comprising a security manual and procedures which provide direction and guidance on information security and Personal information matters relating to employees, customers, suppliers and interested parties who come into contact with its work;
- ✓ Work closely with its Customers, Business Partners and Suppliers in seeking to establish appropriate information security and Personal information standards;
- ✓ Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security and Personal information management;
- ✓ Train all members of staff in the needs and responsibilities of Information Security and Personal information management;
- ✓ Constantly striving to meet, and where possible exceed, its customer's, staff and investors' expectations.
- ✓ Processing personal information only where this is strictly necessary for legal and regulatory purposes or for legitimate organizational purpose
- ✓ Processing only the minimum personal information required for these purposes
- ✓ Providing clear information to natural persons (including children) about how their personal information can be used and by whom
- ✓ Ensuring special safeguards when collecting information directly from children
- ✓ Only processing relevant and adequate personal information
- ✓ Processing personal information fairly and lawfully
- ✓ Maintaining a documented inventory of the categories of personal information processed by the organization
- ✓ Keeping personal information accurate and, where necessary, up-to-date
- ✓ Retaining personal information only for as long as is necessary for legal or regulatory reasons or



Management Systems

Manual

INFORMATION SECURITY & PIMS POLICY

Level 1 document

Reference	MSP 90
Revision	01
Date	20/02/2018
Page:	2 of 2

- for legitimate organizational purposes and ensuring timely and appropriate disposal
- ✓ Respecting natural persons' rights in relation to their personal information
- ✓ Keeping all personal information secure
- ✓ Only transferring personal information outside the UK in circumstances where it can be adequately protected
- ✓ Maintain a strategy for dealing with regulators across the EU, where goods and/or services are offered to natural persons who are resident in other EU countries
- ✓ Apply the various exemptions allowable by data protection legislation
- ✓ Where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance
- ✓ Identify workers with specific responsibility and accountability for the organization's PIMS
- ✓ Maintain records of processing of personal information

Responsibility for upholding this policy is truly Company-wide under the guidance and with the assistance of the head of quality assurance, which encourages the personal commitment of all staff to address Information Security and Personal information management as part of their skills.

Signed: 

Date: 18.5.18

Director