Avantgarde tiling
Quality Through Passion

INFORMATION SECURITY POLICY

Avantgarde Tiling Ltd recognises information as a vital asset to any organisation and therefore regards data security as a high priority for our business and understands its obligation to protect information, ensure it is kept securely and used appropriately. The Information Security (IS) policy and its supporting policies sets out the framework for the protection of confidentiality, integrity and availability of its data assets to help make sure that data held and processed by the company is managed with the appropriate standards to keep it safe.

The policies comply with legal requirements including the Data Protection Act and the General Data Protection Regulation (GDPR). The policies are concerned with the management and security of the company's information assets and the use of these by employees and others who may have been granted permission to process, store or otherwise handle information on behalf of the company. The policy relates to information systems, networks, digital storage and physical documents.

Information security management is an ongoing cycle aimed at continuous assessment of risk and response to emerging threats or vulnerabilities to protect information from unauthorised access, disclosure, modification or destruction. The approach is based on implementation guidance contained within ISO 27002 and where required separate procedural documents will provide detailed descriptions of policy implementation.

This IS policy relates to all IT systems and voice or data networks under the control of Avantgarde Tiling Ltd and information in transit through these systems as well as data in hard copy physical form. The policy applies to all parties who have access to, or use these IT systems, and information belonging to, or under the control of Avantgarde Tiling Ltd, including employees, temporary staff, agency workers, partner organisations, clients and 4th party agencies.
The aims of the IS policy are:

- to raise awareness of the controls and procedures within the organisation
- ensure security of data by implementing suitable controls
- to comply with relevant laws and legislation
- to avoid causing reputational and financial damage to the company

All Avantgarde employees should ensure that:

- Only those who need access to data have that access
- Information is not stored where it can be accidentally exposed or lost
- When data is sent, it is shared or transported securely using encrypted devices or channels.

The company directors will carry out a risk assessment in relation to the business processes that handle information assets and identify and implement appropriate security measures necessary to protect against possible breaches of confidentiality, integrity and availability of business-critical information.

Day to day responsibility for security management will be delegated to designated information or system owners within departments.

Users will be trained on the procedures needed to protect information to ensure compliance with the Data Protection Laws and be made aware of their responsibilities for data security.

An internal Data Protection Officer is appointed who will monitor data protection compliance, provide advice and guidance to employees, investigate any reported or suspected incidents or breaches of security. The Data Protection Officer will also review any changes in legislation or process which may have an impact on the security of information.

All policies will be communicated across the company to ensure good working practices.

Barbara Zanasi

Avantgarde Tiling Ltd

Managing Director

20 January 2024

Related policies and procedures

GDPR Data Protection Policy
Outsourcing and 3rd party compliance procedure
Mobile access and remote working procedure
HR employee handbook
Information security management procedure