VISIVE®

POWERED BY SMART TECHNOLOGY

Data Protection Policy

Version 1.1 December, 2021

The aims of our data security and the retention of data proposals is primarily to protect the company's digitised information assets from all threats, whether they be internal or external, deliberate or accidental. It is also to ensure continuity of information services by preventing breaches in the security of the company's information systems.

Our main objectives in relation to data security include ensuring information is protected against un-authorised access and safeguarding confidentiality. This ensures the integrity of information is maintained (i.e. ensuring accuracy and completeness by protecting against un-authorised access or modification). Having these steps in place enables the company to meet all relevant legislative and regulatory requirements, as well as meeting in-house standards in respect of the management of information and systems. These goals mean that Visive's services are managed in such a way as to achieve maximum continuity and availability.

No un-authorised machine or person shall be permitted to gain access to the company network at any time and machines that are connected to the company network shall be used only by
persons authorised to do so for the purposes for which they are authorised. It is made clear to all employees that no un-authorised software should be run on machines connected to the company network. As a further precaution, data on machines connected to the company network are secured against un-authorised access.

Visive operates robust Contingency & Disaster Recovery Plans, which are regularly updated and tested. Upon completion of each contract, any secure data transferred is returned to the relevant client or stakeholders.