Carne Data Governance and Security

Carne - General

Carne values the trust that our clients place in us by letting us act as custodians of their data.

We take our responsibility to protect and secure your information very seriously.

Further details on the ways we handle your data can be found in our <<Privacy Policy>>.

Data Governance and Security

Carne is committed to providing robust systems and infrastructure to protect our client and corporate information by continually developing our security policies and procedures.

Our Information and Cyber security policies and standards are overseen by the Group Chief Technology Officer.

These policies and standards are aligned with the ISO27001/27002 framework and are reviewed on an annual basis and approved by the senior management team.

Carne also has in place an IT Committee which monitors the Information and Cyber security policies and procedures for any industry or regulatory changes that may be required.

All employees and contractors are required to sign and adhere to documented terms imposing confidentiality obligations in respect of client data. In addition, all staff are required to undertake mandatory annual cyber security and information security training.

The importance of cyber security and information protection is reinforced by senior management to increase awareness of the potential risks and the need to comply with our cyber security policies and procedures.

Client data is classified as confidential data with strict access controls in place to manage this data.

Data loss prevention tools are also implemented to monitor and track data sharing and email traffic.

We have dedicated cyber security and data protection policies in place covering the following areas:

- Information security and access controls
- Protection of our systems
- Vendor management
- System availability and change management
- Incident management
- Business continuity plan
- Mandatory requirements of the GDPR