Thermogroup Ltd recognises that information is a valuable asset that needs to be protected. The company has a duty to ensure that the information it holds conforms to the principles of confidentiality, integrity, and availability as well as protection of personal data. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure; is accurate, up to date and is available to those who should be able to access it. This policy has been written to provide a mechanism to establish procedures and objectives to protect information against security threats and minimise the impact of security incidents. Thermogroup Ltd operates an Information Security Management System that strives to meet the requirements of ISO 27001:2013 as extended by ISO 27701:2019.

Responsibility for the creation and resources required for the Company's Security and Privacy Policy rests with the Managing Director who has appointed a Security Team and a Data Protection Officer to implement the policy. Thermogroup is committed to protect the information assets and personal data belonging to the company, its employees, customers and suppliers against all threats, whether internal or external, deliberate or accidental. Our policy enables us to comply with business requirements, customer and other third-party contract conditions relating to information security and protection of personal data, legislative and regulatory requirements, and to identify and manage related risks.

Objective

The objective of Thermogroup Ltd.'s information security and privacy strategy is to provide management direction and support for information security and privacy within the company. To achieve this, we will ensure that:

- Information will be protected against unauthorised access, loss or misuse
- Confidentiality of information is assured and not disclosed
- Integrity of information is maintained by protection from unauthorised modification
- Regulatory legislative and contractual requirements regarding intellectual property rights, data protection and privacy of personal information are met.
- Business Continuity plans will be produced, maintained, and tested as far as practicable.
- Staff receive sufficient Information Security and privacy training.
- All breaches of information security, actual or suspected are reported and investigated by the Security Team.

All managers are responsible for implementing the policy and ensuring staff compliance in their respective departments. Compliance with the Information Security Policy is mandatory. This policy statement forms part of our Information Security Management process and is reviewed at least annually. It is available to all staff and other interested parties. We constantly monitor our security and privacy performance and implement corrective action when required as part of our drive for continual improvement.

Alistair Bell
Managing Director
3rd August 2022