Information Security Policy

Lightfoot is committed to preserving the confidentiality, integrity, and availability of all the physical, electronic and information assets throughout its organisation to preserve its competitive edge, cash-flow, profitability, legal, regulatory, and contractual compliance, and commercial image.

Confidentiality, integrity, and availability (CIA) is at the heart of Lightfoot. Assets including physical, information, people and services maintain the highest degree of **Confidentiality;** ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access. **Integrity;** safeguarding the accuracy and completeness of information and processing methods. **Availability:** ensuring that information and associated assets should be accessible to authorised users when required and therefore physically secure.

Lightfoot is committed to maintaining certification of ISO 27001:2022 Information Security Management System ("ISMS").

The ISMS of which this policy, other supporting policies, procedures, employee handbook, information security objectives, and related documentation are a framework which has been designed in accordance with the specification contained in ISO 27001:2022.

Lightfoot's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating, and controlling information related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability, information security objectives and Risk Treatment Plan identify how information-related risks are controlled.

As part of our commitment to ISO 27001:2022 (Information Security) Lightfoot have defined our Security Objectives, which can be provided upon request.

Lightfoot has implemented dedicated resource for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be conducted to determine appropriate controls for specific risks.

All employees of Lightfoot, external consultants, sub-contractors, and external parties will be made aware of their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All employees will receive appropriate training and awareness, including third party non-disclosure agreements and contracts.

Lightfoot is committed to continuous, systematic review and continual improvement to achieving certification to ISO 27001:2022 with the British Standards Institution. Lightfoot will make this Information Security Policy available to all interested parties on our website.

Signature: DocuSigned by: Neil Warman CD1CF03513734EC...

Neil Warman, Chief Financial Officer

Date: 22 May 2024