1.0 ISMS Policy Statement

1.1 Fundamentals Group (*We / Our / Us*) specialises in the design, manufacture, installation and servicing of specialist voltage control and monitoring equipment for the electrical power systems industry.

1.2 *Our* activities place emphasis upon the IT system being available to all employees, at all times, including via remote access.

1.3 *We* recognise the importance of an Information Security policy and management system as part of the overall Business Management System to protect *our* data and hardware assets and that of other stakeholders that *we* are responsible for.

1.4 *We* are committed to maintaining certification of the Business Management System to ISO27001 and to meet all other relevant regulatory and customer requirements. *We* recognise the importance of continually improving the system.

1.5 *We* train staff to recognise the importance of data security and ensure that they have adequate resources to meet the requirements of the system. IT policy and security forms part of the employment contract.

1.6 *Our* Management Team is responsible for setting the goals and objectives of the Information Security Management System and ensuring measurements are in place to gauge their effectiveness. The goals and objectives will be derived from risk assessments of *our* operations. Specific responsibilities within the ISMS are detailed in the BMS manual and individual job descriptions.

1.7 The system will be audited on a regular basis as part of the internal audit programme.

1.8 All deviations and exceptions from the ISMS will be handled through the non-conformance process.

1.9 *We* work closely with an external IT service provider to set-up, control, secure and maintain the IT system.

1.10 All users on the system will only have access to those parts of the system required to perform their jobs, some data such as accounts, personnel and customer accounts will be highly restricted. Control will be achieved by user profiles and passwords.

1.11 *Our* servers will be automatically backed-up to a separate device at least daily and copies stored off site. Where 'previous versions' is available on the server, this will be enabled twice daily.

1.12 The IT system is included in *our* disaster recovery plan.

1.13 If *our* data is hosted on any platform outside its premises, the host and all connecting networks must be compatible with this policy.

Approved By: _____ Date: 18/10/2021

Jon Hiscock (Managing Director)

Version Control

Date Reviewed	Next review date	Issue No.	Changes (most recent first)	Process owner	Approver
18/10/2021	18/10/2022	8	Logo changed	Operations	J Hiscock
29/09/2021	29/09/2022	7	Reviewed and signed, logo changed, Fundamentals Ltd changed to Fundamentals Group.	Operations	J Hiscock
04/08/2020	04/08/2021	6	Reviewed and signed. Clarification of backup statement, updates to increase 'plain English'	Operations	J Hiscock
05/07/2019	05/07/2020	5		Operations	J Hiscock