ISMS POLICY STATEMENT

Top Management at bluesource (the" **Company**") understands the Information Security needs and expectations of its interested parties both within the organisation and from external parties including clients, suppliers, regulatory and Governmental departments.

Our Information Security policy is aligned to the requirements of ISO/IEC 27001: 2022, Cyber Essentials and Cyber Essentials Plus, with the Company committed to:

- Comply to all applicable laws and regulations and contractual obligations
- Implement Information Security objectives ("**Objectives**") that consider information security requirements following results of applicable risk assessments
- Communicate these Objectives and performance against them to interested parties
- Adopt an Information Security Management System ("**ISMS**") comprising an overarching policy document/manual, policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and other interested parties who encounter its work
- Confidentiality, Integrity and Availability of information
- Work closely with customers, business partners and suppliers to establish appropriate information security standards
- Adopt a forward-thinking approach on future business decisions, including the continual review of the ISMS and risk evaluation criteria, which may impact on Information Security
- Ensure that our information system and the information contained meet the needs of our business operations
- Provide appropriate resources (equipment, training, competent staff, and any other requirements) to operate the ISMS
- Ensure that all information, including internal, third party, personal and electronic data, is treated with complete confidentiality and appropriately protected
- Safeguard security of our information assets through effective business continuity management and disaster recovery
- Instruct all members of staff in the needs and responsibilities of Information Security Management, including that required of GDPR and DPA, and increasing staff awareness through education and training
- Reporting all actual or suspected information security incidents, breaches, and weaknesses so they can be investigated
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies
- Review controls forming the basis of the Statement of Applicability and ISMS through an annual programme of internal audit
- Constantly strive to meet its customer's expectations
- Maintaining a complaints process

The information security policy provides a framework for setting, monitoring, reviewing, and achieving our objectives, programmes, and targets.

The policy has been approved by the Directors and is reviewed annually or sooner should a significant change occur to ensure its continuing suitability, adequacy, and effectiveness. The Business Management System is subject to both internal and external annual audits.

Responsibility for upholding the policy is company-wide under the authority of the Managing Director who encourages the personal commitment of all staff to address information security as part of their skills and appoints the Head of Operations to manage the ISMS and its compliance.

Signed by:
John Forde
B2B1403BE597461...
John Forde
Managing Director