**ROOTS RESEARCH AND INFORMATION SECURITY STATEMENT**

Given that Roots Research’s key business focus is on the recruitment of research participants and this naturally involves processing of the personal data of research participants as well as the data of our clients and others, then it is wholly appropriate that information security and data protection is a key objective of the organisation. This objective is fully recognised and supported across the Roots Research team, whose personal commitment to information security and data protection is whole-hearted.

Core to the delivery of information security and data protection is our Information Security Management System (ISMS). Our ISMS was developed to be compliant with the ISO 27001, 2013 standard for Information Security Management Systems, and we are proud to have attained certification to that standard in 2015 and since then have been subject to rigorous annual audit to maintain accreditation.

The purpose of our ISMS is to maintain the availability, confidentiality and integrity of data; and enshrined within our ISMS, in line with the ISO 27001 standard, is a commitment to continuous improvement. We see the introduction of the General Data Protection Regulations and the work we are undertaking to meet the requirement of those Regulations, as part of our ethos of continuous improvement, as well as an obligation to maintain legislative compliance. At the centre of our ISMS and core to our compliance are our Policy for Information Security Management and our Policy for Data Protection, supported by a suite of policies, protocols and subordinate documents that constitute our ISMS framework. Below are our Information Security Management Policy and the Policy Statement taken from our Policy for Data Protection.

# 

# Information Security Management Policy

*It is the policy of Roots Research Limited to be fully committed to the achievement of high standards of performance in the management of information security, and protection of that information which is categorised as an information asset by the Company; to be held and handled by the Company in relation to its business activities.*

*The aim of this policy is to implement an Information Security Management System through the existence of a robust framework with appropriate arrangements and adequate preventative measures that serve to prevent information security failure, commensurate with identified risks to the security of that information.*

*The scope of this policy includes:*

* *information held about our clients and their projects;*
* *information held that is gathered about, and from, research participants on behalf of our clients; and*
* *information that enables Roots Research to operate as a business entity, including information held about our employees, partnership organisations, contractors and suppliers.*

*We recognise that information security failure can result from electronic and and/or document system error, human factors and from failings in management controls, therefore we undertake to implement robust and tested electronic and hard copy documented information systems, provide suitable system support arrangements, maintain a secure physical infrastructure and have proper provisions in place to guide and support employees in the holding and handling of information, and also any third party who as part of its business activities are entrusted by the Company with such information assets.*

*Our policy is underpinned by 12 high-level objectives.*

1. *Adopt and apply an effective information security management system, allocating clear accountabilities and responsibilities to support its implementation.*
2. *Ensure that information security management objectives carry sufficient weight in comparison with other business objectives.*
3. *Provide suitable resources to meet information security commitments.*
4. *Develop and implement action plans to maintain compliance and to support the pursuit of continuous improvement in the management of information security; and particularly the adequacy, suitability and effectiveness of the Information Security Management System.*
5. *Establish clear performance standards, and clear criteria and processes for undertaking risk assessment of information security.*
6. *Assess information that is to be held and handled, to determine the appropriate level and means of security to be applied on a risk-assessed basis that weighs the potential for breaches of security and/or loss of information.*
7. *Comply, as a minimum, with all applicable legal requirements and other appropriate requirements including those determined by the influential bodies to which the organisation subscribes, including industry standards, codes of practice and customer requirements.*
8. *Determine arrangements for the selection and management of contractors and service providers that recognises their ability and commitment to the effective management of information security, and following selection, help them to commit to our information security standards.*
9. *Maintain consultation and dialogue with and amongst colleagues, clients and other stakeholders to support our commitment to information security, and liaise with external stakeholders to ensure that we understand how we need to manage information security in relation to our business interaction with them, and they understand what we are doing with their information.*
10. *Ensure employees, contractors and other stakeholders who will have access to our information assets in the due course of business operations, are aware of, and trained on, our information security requirements, and abide by them.*
11. *Prevent or limit the consequence of any information security failure or information loss through effective contingency planning, including response arrangements.*
12. *Take all necessary steps, including regular monitoring and audit of compliance, effective investigation of information security failures, periodic management review, and implementation of appropriate corrective actions, to ensure that the information security arrangements continue to be effective.*

## *Policy for Data Protection - Policy Statement*

*Roots Research implements its Data Protection Policy as part of its compliance measures in relation to the General Data Protection Regulations 2018, and it is part of our ongoing demonstration of compliance with the principles of data protection.*

*Roots Research Limited (the Company) is registered as a Data Controller with the Information Commissioners Office (ICO) and complies with the obligations for data protection as described by the General Data Protection Regulations 2018 relating to the collection, usage and handling of personal information, and our processes.*

*Compliance with the policy is a foundation of the effective management of information security in line with our ISO 27001:2013 certification.*

*During the course of our activities we will collect, store and process personal data and we recognise the need to treat it in an appropriate and lawful manner. The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, clients and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Regulations. The Regulations impose restrictions on how we may use that information.*

*This policy sets out our rules on data protection and our approach to meeting the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.*

*We recognise that an act of non-compliance may lead to legal prosecution, as well as damage to the reputation of the Company. Data protection is also a matter of good business and social responsibility. To ensure that an appropriate level of data protection is maintained, this policy must be observed in relation to the collection, holding, use and disclosure of personal data.*

*Regular monitoring and review the effectiveness of this policy will take place to ensure that it continues to achieve its stated objectives.*

*Any breach or suspected breach will be investigated and may lead to disciplinary action being taken where that breach arises from the negligent or wilful action of an employee. In some cases, a breach of the terms of this policy may be treated as gross misconduct leading to summary dismissal of those responsible.*