ZUDOMANZI GROUP PROPRIETARY LIMITED

DATA PROTECTION AND PRIVACY POLICY

1. Introduction

Zudomanzi Group Proprietary Limited, registration number 2014/000959/07, ("**Company**", "**we**", "**our**" or "**us**") is the provider of the Edgepoint Software and is committed to protecting the privacy and security of your Personal Information. This Data Protection and Privacy Policy ("**Policy**") sets out the principles and procedures that we follow in relation to the handling of Personal Information in compliance with the Protection of Personal Information Act ("**POPIA**") and other relevant data protection laws.

This Policy must be read together with any other documents or agreements that describe the manner in which we will in specific circumstances, collect or process your Personal Information. This Policy supplements such other documents and agreements but does not supersede them and in the event of any conflict, ambiguity or inconsistency between this Policy and such other documents and agreements, the terms of the particular document or agreement will prevail.

2. Scope

2.1 Part A of this Policy applies to all users of the Edgepoint Software and customers of Zudomanzi ("**Customers**", "**you**" or "**your**").

2.2 Part B of this Policy applies to all Zudomanzi employees and third-party service providers that have access to or Process Customers' Personal Information on behalf of Zudomanzi or within the scope of their employment, as the case may be.

3. Definitions

3.1 Personal Information: Any information relating to an identified or identifiable natural or juristic person; including information such as the name, identification number, location data, an online identifier, biometric information, financial or cultural identity of that person. Personal Information does not include information that does not identify a person (including in instances where that information has been anonymised).

3.2 Processing: Any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.3 Data Subject: The natural or juristic person to whom Personal Information relates.

3.4 Responsible Party: The entity that determines the purposes and means of Processing Personal Information. In this Policy, Zudomanzi Group Proprietary Limited is the responsible party.

3.5 Operator: An entity that processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party.

3.6 Consent: Any freely given, specific, informed and unambiguous expression by the Data Subject, by way of a statement or clear affirmative action, which signifies agreement to the Processing of its Personal Information.

PART A

4. Consent to Processing of Personal Information

4.1.1 By agreeing to the terms of this Policy, you provide us with your express Consent and agreement that we may Process your Personal Information as set out in this Policy.

4.1.2 If you do not agree with this Policy or are concerned about any aspect as it relates to your Personal Information, please do not continue to use our website, the Edgepoint Software or our services.

5. Personal Information we Process

5.1 We may Process various types of Personal Information, as follows:

5.1.1 Identity Information: includes information concerning your name, date of birth and identification (or registration) number;

5.1.2 Contact Information: includes your physical and postal addresses, email addresses and telephone numbers, as well as company secretarial information that has been disclosed in relation to you; and

5.1.3 Financial Information: includes bank account and payment card details (and tax registration numbers, as applicable).

5.2 We may also Process, collect, store and/or use aggregated data, which may include historical or statistical data for any purpose. Aggregated data may be derived from the Data Subject's Personal Information but is not considered Personal Information, as this data does not directly or indirectly reveal the Data Subject's identity. However, if we combine or connect aggregated data with the Data Subject's Personal Information in a manner that has the result that it can directly or indirectly identify the Data Subject, we will treat the combined data as Personal Information, which will be managed in accordance with this Policy.

6. Lawful basis for Processing

6.1 We Process your Personal Information lawfully, fairly, and in a transparent manner. We Process your Personal Information to facilitate the sale of our products, the provision of our services and to fulfil our statutory and regulatory obligations.

6.2 We may also use your Personal Information to:

6.2.1 maintain and update our customer, or potential customer, databases;

6.2.2 provide you with marketing material that is relevant to you;

6.2.3 diagnose and deal with issues and queries;

6.2.4 protect our rights in any litigation that may involve you;

6.2.5 for security, administrative and legal purposes;

6.2.6 comply with our statutory obligations and engagements with regulatory authorities;

6.2.7 be used for customer relations purposes;

6.2.8 fulfil any contractual obligations that we may have to you or any third party;

6.2.9 communicate with you and retain a record of our communications with you and your communications with us; and

6.2.10 for other lawful purposes that are relevant to our business activities.

6.3 We will limit Processing of your Personal Information to the specific and legitimate purposes listed in this clause 6, unless we reasonably consider that it is necessary to Process your Personal Information for another purpose that is compatible with the original purpose.

6.4 We may, where permitted or required to do so by applicable legislation, Process your Personal Information without your knowledge or Consent, and will do so in accordance with the further provisions of this Policy.

7. Data collection

7.1 We collect your Personal Information in three ways, namely:

7.1.1 through direct or active interactions with you;

7.1.2 through automated or passive interactions with you; and

7.1.3 from third-parties, including third-party service providers.

7.2 Direct or active collection from you:

7.2.1 We may require that you submit certain information to enable you to make use of our products and services, to facilitate the conclusion of an agreement with us or that is necessary for our fulfilment of our statutory or regulatory obligations. We also collect Personal Information directly from you when you communicate directly with us, for example via e-mail, telephone calls, feedback forms or forums.

7.2.2 If you contact us, we reserve the right to retain a record of that correspondence, which may include Personal Information.

7.3 Personal Information collected from third parties:

7.3.1 We receive Personal Information about you from our third-party service providers, such as our technical support services suppliers.

8. Compulsory Personal Information and consequences of not sharing with us

Where we are required to Process certain Personal Information by law, or in terms of a contract that we have with you, and you fail to provide such Personal Information when

requested to do so, we may be unable to perform in terms of the contract we have in place or are trying to enter into with you. In this case, we may be required to terminate the contract and/or relationship, upon notification to you, which termination will be done in accordance with the terms of the contract and all applicable legislation.

9. **Data Accuracy and Quality**

We take all appropriate and reasonable steps to ensure that your Personal Information is accurate, complete, and kept up-to-date. It is your responsibility to advise us or the persons responsible for the maintenance of your Personal Information should any of the Personal Information we have about you be incorrect, incomplete, misleading or out of date, by notifying us by using the contact details set out in clause 16 below.

10. **Data Security**

10.1 We have implemented appropriate, reasonable technical and organisational measures to secure the integrity of your Personal Information and to ensure the security of your Personal Information, including protection against unauthorised or unlawful Processing/misuse, accidental loss or damage as well as alteration and destruction.

10.2 We also create a back-up of your Personal Information for operational and safety purposes.

10.3 We review our information collection, storage and Processing practices, including physical security measures periodically, to ensure that we keep abreast of good practice.

10.4 Despite the above measures being taken when Processing Personal Information, we do not guarantee that your Personal Information is 100% secure.

10.5 You hereby acknowledge that you know and you accept that technology is not absolutely secure and there is a risk that your Personal Information will not be secure when Processed by means of technology. You will not be able to take action against us if you suffer losses or damages in these circumstances.

11. **Data retention and deletion**

11.1 We may retain and Process your Personal Information if and for as long as:

11.1.1 we are required or permitted by law, a code of conduct or a contract with you to do so;

11.1.2 we reasonably need it for lawful purposes related to the performance of our business activities;

11.1.3 we reasonably require it for evidentiary purposes; or

11.1.4 you agree to us retaining it for a specified further period.

11.2 To determine the appropriate retention period for Personal Information, we will consider, among other things, the nature and sensitivity of the Personal Information, potential risks or harm that may result from its unauthorised use or disclosure, the purposes for which we Process it and whether those purposes may be achieved through other means. We will always comply with applicable legal, regulatory, tax, accounting or other requirements as they pertain to the retention of Personal Information.

11.3 Personal Information is securely deleted or anonymised once it is no longer needed.

12. Storage and transfer of Personal Information

12.1 We store your Personal Information on our servers or those of our service providers and in hard copy format at our offices and/or at the storage facilities of our third-party record storage and management providers.

12.2 We reserve the right to transfer to and/or store your Personal Information on servers in a jurisdiction other than where it was collected, or otherwise in a jurisdiction that may not have comparable data protection legislation.

12.3 We ensure that international transfers of your Personal Information comply with applicable data protection laws and that appropriate measures are in place to ensure an adequate level protection of your Personal Information. If the location to which Personal Information is transferred and/or is stored does not have substantially similar laws to those of South Africa, which provide for the protection of Personal Information, we will take reasonably practicable steps, including the imposition of appropriate contractual terms to ensure that your Personal Information is adequately protected in that jurisdiction.

12.4 Please contact us if you require further information as to the specific mechanisms used by us when transferring your Personal Information outside of South Africa or to a jurisdiction that is different to the one in which we collected your Personal Information.

13. **Data Subject Rights**

13.1 Data protection laws confer certain rights on Data Subjects in respect of your Personal Information, which include the right to:

13.1.1 Block all cookies, by setting your browser to do so, including cookies associated with our products and services or to indicate when a cookie is being sent by us;

13.1.2 Request access to Personal Information: (commonly known as a "data subject access request"), thereby enabling you to receive a copy of the Personal Information retained about you;

13.1.3 Request the correction of your Personal Information, in order to ensure that any incomplete or inaccurate Personal Information is corrected;

13.1.4 Request erasure of your Personal Information, where there is no lawful basis for the retention or continued Processing of it;

13.1.5 Object to the Processing of your Personal Information for legitimate interest (or those of a third-party) and there is something about your particular situation which makes you want to object to Processing on this ground as you feel it impacts on your fundamental rights and freedoms;

13.1.6 Request restriction of Processing of your Personal Information. This enables you to ask us to suspend the Processing of your Personal Information in limited circumstances, which may differ by jurisdiction; and

13.1.7 Withdraw Consent previously given in respect of the Processing of your Personal Information at any time which withdrawal of Consent will not affect the lawfulness of any Processing carried out prior to your notice of withdrawal. Withdrawal of Consent may limit our ability or that of our third party service providers to provide certain products or services to you but will not affect the continued Processing of your Personal Information in instances where your Consent is not required.

13.2 As far as the law allows, we may charge a fee for attending to any of the above requests and may also refuse to carry out any of your requests in whole or in part.

14. **Sharing Personal Information**

14.1 We will not intentionally share your Personal Information with third parties, whether for commercial gain or otherwise, other than with your permission, as permitted by applicable law.

14.2 We may share your Personal Information under the following circumstances:

14.2.1 with our agents, advisers, service providers and suppliers that have agreed to be bound by this Policy or similar terms, which offer the same level of protection as this Policy;

14.2.2 with our employees, contractors and agents if and to the extent that they require such Personal Information in the provision of services for or to us, which include hosting, development and administration, technical support and other support services relating to the operation of our business. We will authorise any Personal Information Processing done by a third party on our behalf, amongst other things by entering into written agreements with those third-parties governing our relationship with them and containing confidentiality and non-disclosure provisions;

14.2.3 to enable us to enforce or apply any other contract between you and us;

14.2.4 to protect our rights, property or safety or that of our customers, employees, contractors, suppliers, service providers, agents and any other third-party;

14.2.5 to mitigate any actual or reasonably perceived risk to us, our customers, employees, contractors, agents or any other third-party;

14.2.6 with governmental agencies and other regulatory or self-regulatory bodies, if required to do so by law or we reasonably believe that such action is necessary to:

14.2.6.1 comply with the law or with any legal process;

14.2.6.2 protect and defend the rights, property or safety of Zudomanzi, or our Customers, employees, contractors, suppliers, service providers, agents or any third-party;

14.2.6.3 detect, prevent or manage actual or alleged fraud, security breaches, technical issues and contraventions of this Policy; and

14.2.6.4 protect the rights, property or safety of members of the public (if the Data Subject provides false or deceptive information or misrepresent, we may proactively disclose such information to the appropriate regulatory bodies and/or commercial entities).

15. **Data breach notification**

We have implemented procedures to address actual or suspected data breaches. We will notify the Information Regulator and you, in accordance with legal requirements and within the period such notification is required.

16. **Complaints**

You can file a complaint with us if you believe your data protection rights have been violated. Complaints can be emailed to admin@edgepointsoftware.com. Moreover, you also have the right to file a complaint with the Information Regulator by sending an email to POPIAComplaints@inforegulator.org.za.

17. **Role of the Information Officer (IO)**

Our Chief Operating Officer (COO) serves as the Information Officer. The IO is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection laws.

18. **Policy review and updates**

This Policy will be reviewed and updated on an annual basis or as necessary according to changing legislation and business requirements. We will take reasonably practicable steps to inform you when this Policy has been updated.

19. **Children**

Our products and services are not targeted at children (a natural person under the age of 18 years). We will not knowingly Process Personal Information in respect of children.

20. **General**

20.1 You agree that this Policy, our relationship and any dispute of whatsoever nature relating to or arising out of this Policy whether directly or indirectly is governed by South African law, without giving effect to any principle of conflict of laws.

20.2 Our failure to exercise or enforce any right or provision of this Policy shall not constitute a waiver of such right or provision.

20.3 Each provision of this Policy, and each part of any provision, is removable and detachable from the others. As far as the law allows, if any provision (or part of a provision) of this Policy is found by a court or authority of competent jurisdiction to be illegal, invalid or unenforceable (including without limitation, because it is not consistent with the law of another jurisdiction), it must be treated as if it was not included in this Policy and the rest of this Policy will still be valid and enforceable.

21. **Contact**

For queries related to your rights under data protection laws or this Policy, please contact the IO by emailing admin@edgepointsoftware.com .

PART B:

22. **Definitions**

For purposes of this Part B:

All references to Personal Information shall mean Customers' Personal Information.

22.1 Best Industry Practice: includes, in relation to an obligation, undertaking, activity or a service, the exercise of the degree of skill, speed, care, diligence, judgment, prudence and foresight and the use of practices, controls, systems, technologies and processes, which would be expected from a skilled, experienced and market leading service provider that is an expert in performing the same or similar obligation, undertaking, activity or service and utilising and applying skilled resources with the requisite level of expertise;

22.2 Company Data: means any data, including Personal Information, supplied to the Employee or the Service Provider (or its personnel) by or on behalf of the Company, or Processed by or on behalf of the Company or its personnel;

22.3 Data Protection Legislation: means any data protection or data privacy laws applicable in the Republic of South Africa from time to time, including but not limited to the Protection of Personal Information Act 4 of 2013, the Electronic Communications and Transactions Act 25 of 2002 and the Consumer Protection Act 68 of 2008;

22.4 Employee: means the Company's directors, employees, agents and partners involved in the Processing of Personal Information and similar activities ("**Employees**" has a corresponding meaning); and

22.5 Services Provider: means third-parties contracted by the Company to provide one or more service and/or goods that will have access to and/or be involved in the Processing of Personal Information and similar activities ("**Services Providers**" has a corresponding meaning).

23. **Data Protection Principles**

23.1 We adhere to the following data protection principles:

23.1.1 Lawfulness, fairness, and transparency in Processing

Personal Information shall be processed lawfully, reasonably and in a transparent manner in relation to the Data Subject. This means, the Company must tell the Data Subject what processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection Legislation (lawfulness).

23.1.2 Purpose specification for data collection

Personal Information shall be collected with the Data Subject's knowledge of the purpose for which the Personal Information is collected, which purpose must be specified, explicit, and legitimate. The Company may not further Process Personal Information in a manner that is incompatible with the stated purpose. This means the Company must specify exactly what Personal Information collected will be used for and limit the Processing of that Personal Information to only what is necessary to meet the specified purpose.

23.1.3 Processing minimisation

Processing of Personal Information shall be done lawfully, in a reasonable manner, and given the purpose for which it is Processed, it is adequate, relevant, and not excessive. This means that the Services Providers and Employees may only Process Personal Information strictly in line with the performance of their services to the Company, as further detailed in the services and/or employment contract. Employees and Services Providers cannot Process Personal Information for any reason unrelated to the provision of the services to the Company. Furthermore, Employees and Services Providers must ensure (i) that any Personal Information collected is adequate and relevant for the intended purposes, and (ii) that when Personal Information is no longer needed for specified purposes, it is deleted or de-identified in accordance with the Company's data retention policy.

23.1.4 Further Processing limitation

Personal Information shall be Processed in a manner compatible with the purpose for which it was originally collected. To establish whether further Processing is compatible with the purpose of collection, consider: (i) the nature of the information concerned; (ii) the manner in which the information has been collected; and (iii) any contractual rights and obligations between the Data Subject and the Company.

23.1.5 Information quality ensuring accuracy of data

Personal Information shall be complete, accurate, not misleading and, kept up to date. Services Providers and Employees must check the accuracy of any Personal Information at regular intervals after receipt of same and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Information (subject to the Company's data retention policy).

23.1.6 Openness and data retention limitation to necessary periods

Services Providers and Employees must maintain documentation of all Processing operations in sufficient detail to facilitate a request for access to the records of Processing operations. The Company must keep and maintain accurate corporate records reflecting the Company's Processing

including records of Data Subjects' Consents and procedures for obtaining Consents. If the Company has used a record of Personal Information to make a decision about a Data Subject, then that record must be retained in accordance with the Company's data retention policy.

23.1.7 Data security to maintain integrity and confidentiality of data

Employees must follow all procedures and technologies which the Company puts in place to maintain the security of all Personal Information from the point of collection to the point of destruction. Employees may only transfer Personal Information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Anyone who Processes Personal Information on behalf of the Company is required to Process Personal Information only with the knowledge or authorisation of the Company, and to treat Personal Information which comes to their knowledge as confidential. The Company is required to conclude a written agreement with everyone who Processes Personal Information on our behalf. Employees may refer any queries they have in this regard to the Information Officer.

23.1.8 Data Subject participation

Data Subjects have rights when it comes to how the Company handles their Personal Information. These include, depending on the Data Subject's location, the right to (i) be notified that Personal Information is being collected; (ii) be notified of a Personal Information breach; (iii) access Personal Information held by the Company; (iv) request the correction, destruction or deletion of Personal Information; (v) object to Processing; (vi) restrict the Company's Processing of the Data Subject's Personal Information; (vii) object to direct marketing; (viii) request that the Company transfers their Personal Information to a third party in an easily accessible format; (ix) object to automated decision making; and (x) submit a complaint to the appropriate regulator.

Employees must (i) verify the identity of an individual making a request under any of the rights listed above; and (ii) immediately forward any Data Subject request that they receive to their supervising officer.

24. **Service Provider data protection obligations**

24.1 In addition to and without prejudice to, or limiting the generality of, its further obligations contained in any other agreements concluded with the Company, when Processing any Company Data, the Service Provider shall:

24.1.1 comply with all applicable industry codes of conduct to the extent that they regulate or relate to the Processing of Personal Information;

24.1.2 use and apply appropriate measures, procedures and controls in relation to Personal Information, in accordance with Best Industry Practice;

24.1.3 not do anything, or omit to do anything, which will cause the Company to contravene any applicable laws, including any Data Protection Legislation;

24.1.4 keep the Company Data confidential; and

24.1.5 at all times strictly comply with Company policies and procedures pertaining to the protection, privacy, Processing and destruction of Personal Information that apply to the Company and to which the Company is subject to.

24.2 The Service Provider may only Process Company Data:

24.2.1 for the specific purposes for which it was disclosed to the Service Provider, delineated in any agreement concluded between the Parties;

24.2.2 as required or permitted by applicable law, including any Data Protection Legislation; and/or

24.2.3 with the express prior written consent of the Company.

24.3 In addition and without prejudice to, or limiting the generality of, its further obligations in any other agreement concluded with the Company, the Service Provider shall take all reasonable and appropriate technical and organisational precautions and measures necessary to secure the integrity and confidentiality of the Company Data, and to prevent any (i) loss of, damage to, or unauthorised destruction of the Company Data; or (ii) unauthorised or unlawful access to or Processing of the Company Data.

24.4 The Service Provider must:

24.4.1 provide the Company with all assistance and co-operation requested by the Company in relation to any requests or complaints received from any person or entity, including requests for the deletion, updating or correction of Personal Information; and

24.4.2 immediately notify the Company where there are reasonable grounds to believe that the Personal Information has been accessed or acquired by an unauthorised person. In such event, the Service Provider must immediately:

24.4.2.1 comply with all instructions and directions given by the Company;

24.4.2.2 take all measures necessary to determine the scope of the compromise and to restore the integrity of the Company's infrastructure;

24.4.2.3 take steps to minimise the impact of the security compromise on the Company and the Company's Data;

24.4.2.4 provide all information which may be requested by the Company, co-operate fully with the Company in relation to any notifications which

may be made by the Company to any regulator, data subjects (as defined in any applicable Data Protection Legislation) or any other person; and

24.4.2.5 co-operate fully with the Company in relation to any investigations that the Company may initiate or which may be initiated by an investigator or other authority.

24.5 The Service Provider shall, on request from the Company, supply all information, data and materials required by the Company to assess and confirm the Service Provider's compliance with its obligations in this Policy. This information shall be provided at no additional cost where provided in an electronic format only, but otherwise at a cost where the Company requests the information other than in electronic format. The information shall be provided to the Company promptly and in any event within 5 Business Days of request, provided that if the Company is unable to receive the information within this period, then such information will be provided as soon as the Company is able to receive the information.

24.6 The Service Provider shall comply with all reasonable directions and instructions which may be given by the Company regarding the Processing of the Personal Information. It is further agreed that any directions or instructions which are required for purposes of ensuring compliance with any applicable laws, including Data Protection Legislation, shall also be deemed to be reasonable.

24.7 Upon termination of the Service Provider's contract for any reason, the Service Provider and any of its sub-contractors and personnel (if applicable), with respect to Company Data or data Processed (on behalf of the Company), created, maintained or received by the Service Provider pursuant to the performance of the services, shall:

24.7.1 retain only that Personal Information which is necessary for the Service Provider to carry out its legal responsibilities;

24.7.2 return to the Company, or destroy with the express written consent of the Company, the remaining Personal Information that the Service Provider and any of its sub-contractors or personnel (if applicable) still maintain in any form;

24.7.3 continue to use appropriate safeguards and comply with clauses 24.3 above, and any applicable law, including Data Protection Legislation in respect of security safeguards to prevent loss of, damage to, or unauthorised access or disclosure of the Personal Information, other than as provided for in terms of this Policy, for as long as the Service Provider and any of its sub-contractors or personnel (if applicable) retain the Personal Information;

24.7.4 not Process, use or disclose the Personal Information retained by the Service Provider and any of its sub-contractors or personnel (if applicable) for any purpose, other than the purposes for which such Personal

Information was retained, and subject to the provisions as outlined in this Policy, which applied prior to termination thereof; and

24.7.5 return to the Company, or destroy with the express written consent of the Company, the Personal Information retained by the Service Provider and any of its sub-contractors or personnel (if applicable) when it is no longer needed to carry out their legal responsibilities.

24.8 The Service Provider shall not transfer to a third-party the Personal Information or allow Processing of the Personal Information by a third-party without the written consent of the Company.

24.9 The Service Provider shall not transfer or Process the Personal Information disclosed pursuant to the provision of the services outside of the Republic of South Africa without the prior written consent of the Company.

24.10 The Service Provider indemnifies the Company and holds the Company harmless against any and all claims or loss arising from a breach by the Service Provider, its sub-contractors or its personnel of this Policy and/or arising from the unauthorised Processing of, access to, use and/or disclosure of any Personal Information by the Service Provider, its sub-contractors and/or any of their respective personnel.

24.11 Any breach by the Service Provider of its obligations set out in this Policy shall be deemed to be a material breach of this Policy and every other agreement concluded between the Company and the Service Provider, and shall entitle, but not oblige, the Company to immediately terminate the agreement concluded between the Company and the Service Provider on written notice to the Service Provider.

25. Employee data protection obligations

25.1 Each Employee must learn:

25.1.1 what actions are specifically required or prohibited by Data Protection Legislation; and

25.1.2 to recognise areas where Data Protection Legislation problems may arise and seek guidance from the relevant manager, who may in turn refer matters to the Information Officer.

25.2 Periodic Data Protection Legislation surveys, audits and reviews will be conducted to ensure and monitor Employees' adherence to this Policy.

25.3 Employees are encouraged to seek advice if they have any questions. To this end, the Information Officer will assist Employees on matters relating to the interpretation of the relevant Data Protection Legislation.

25.4 Senior management shall use all reasonable efforts to ensure awareness of, and compliance with, this Policy. Such reasonable efforts include, but are not limited to, frequent communications with Employees.

26. Employee reporting procedures

26.1 If an Employee has been involved in, or becomes aware of any violation of this Policy by another Employee, it is the Employee's responsibility to report it to one of the following individuals, as soon as possible:

26.1.1 their manager or supervisor;

26.1.2 their local compliance manager; or

26.1.3 the Company's compliance officer.

26.2 The individual receiving the report, if not the Information Officer, bears the responsibility to report the violation to the Information Officer, as soon as possible.

26.3 To the extent possible and practical, the Company will endeavour to maintain the confidentiality and anonymity of the report. If an Employee fears reprisal, he or she should express this concern at the time of the report. In such circumstances the Employee's identity will be kept confidential.

26.4 Retaliation, retribution or harassment against any Employee who in good faith reports a violation of this Policy is strictly prohibited and, where applicable, constitutes grounds for disciplinary action, including dismissal.

27. Employee training

27.1 All Employees are required to familiarise themselves with the contents of this Policy.

27.2 It is the responsibility of the Information Officer (or a person designated by them) to ensure that all new Employees are made aware of this Policy. Compliance messages and updates regarding Data Protection Legislation developments will be delivered to Employees to prevent contraventions of Data Protection Legislation.

28. The Information Officer

The Information Officer's details are as follows: admin@edgepointsoftware.com . The Information Officer is required to:

28.1 administer a comprehensive Data Protection Legislation training programme, including but not limited to workshops, online training, email bulletins and manuals;

28.2 administer the training of all relevant Employees regarding the importance and expectation of compliance with Data Protection Legislation: (i) during initial orientation sessions; and (ii) on an ongoing basis;

28.3 train senior management, as required, to recognise and address issues with complying with Data Protection Legislation;

28.4 regularly assess Employees' knowledge of Data Protection Legislation compliance policies and procedures;

28.5 document all training sessions;

28.6 monitor and investigate all potential Data Protection Legislation violations and report their findings directly to the Company's risk committee or board of directors;

28.7 implement adequate remedial measures to prevent violations of Data Protection Legislation and consult with the human resources managers responsible for making recommendations regarding disciplinary measures for contraventions of this Policy;

28.8 review minutes, agendas, registers, policies, standards and relevant correspondence as well as the filing structure of documents, whether electronically or manually, in order to identify and address any unlawful data protection practices or concerns;

28.9 confirm that the current technical standards are Data Protection Legislation compliant;

28.10 conduct an annual audit of compliance procedures and policy;

28.11 attend training with specific reference to developments in Data Protection Legislation; and

28.12 undertake any other responsibility as set out elsewhere in this Policy.

29. Consequences of non-compliance

29.1 Although an Employee's manager is responsible for the implementation and monitoring of the adherence to this Policy, each Employee is responsible for his or her own actions. Consequences of violations of this Policy are serious and may expose the Company to litigation, fines and harm its reputation and competitive position. Violation of certain provisions of applicable Data Protection Legislation amounts to a criminal offence, which may result in imprisonment of the individuals involved.

29.2 Employees should be aware that in the event that the Company is found to be in contravention of any Data Protection Legislation, civil claims for damages can be instituted by third parties (individuals or companies) against the Company to recover any loss or damage suffered by the third parties as a result of the Company's unlawful conduct, regardless of whether or not there is intent or negligence.

29.3 The Company will investigate each reported violation and will take the appropriate action. All Employees have a responsibility to assist and cooperate in any investigation conducted by the Company or by the Information Regulator.

29.4 Any Employee of the Company found to have consciously engaged in unlawful Processing activities or to be negligent in exercising his or her managerial responsibilities in preventing a violation of the relevant Data Protection Legislation will be subject to disciplinary measures and may in certain cases face dismissal and/or the immediate termination of the business relationship between the parties.

30. **Acknowledgement of receipt and review**

[By clicking "Accept"**] OR [**By signing this Policy**]**, you hereby acknowledge that you received and read a copy of this Policy, and understand that you are responsible for knowing and abiding by its terms. This Policy does not set terms or conditions of employment or form part of an employment contract (in the case of Employees).

Signed ……..

Name: ……..

Date ……..