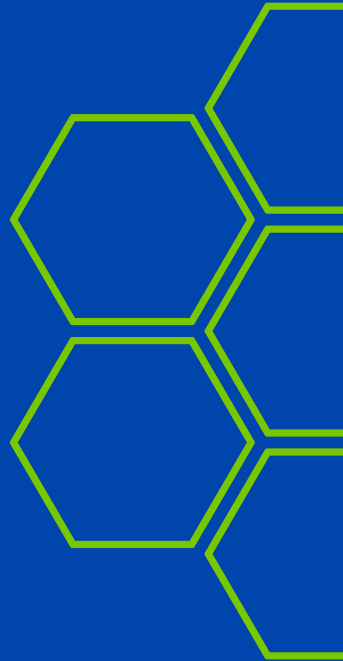




DATA PROTECTION POLICY





DOC REF:	RANS/ DP-001/ 2026
TITLE:	DATA PROTECTION POLICY
ISSUE DATE:	FEBRUARY 2026
ISSUE NUMBER:	01
REVISION DONE:	0
APPROVED BY:	
Sign Here:	

TABLE OF CONTENT

1. POLICY STATEMENT.....	5
2. SCOPE	6
3. DEFINITIONS	6
4. PERSONAL DATA PROTECTION PRINCIPLES.....	7
5. LAWFUL PROCESSING OF PERSONAL DATA.....	7
6. PROCESSING OF SENSITIVE PERSONAL DATA	8
7. COLLECTION OF PERSONAL DATA	9
8. DATA SUBJECT RIGHTS AND REQUESTS	9
9. SHARING PERSONAL DATA.....	10
10. REPORTING PERSONAL DATA BREACHES.....	10
11. RETENTION OF PERSONAL DATA	11
12. SECURITY, INTEGRITY AND CONFIDENTIALITY	11
13. DATA COLLECTED AND PURPOSE OF THE DATA COLLECTED.....	11
14. RESPONSIBILITIES	12
15. COMPLAINTS HANDLING MECHANISM	13
16. COMMUNICATION	13
17. APPROVAL, REVIEW AND UPDATES	13

1. Policy Statement

The Company understands that protecting the privacy and security of Personal Data is crucial in maintaining customer trust, complying with data protection laws and regulations, and safeguarding sensitive information from unauthorised access or misuse. With the increasing reliance on technology and the collection of personal information, we recognise our responsibility to handle data with utmost care and respect.

We also recognise that in UGANDA, every person has a constitutionally-guaranteed, and statutory-buttressed right to have their private affairs remain confidential and undisclosed, and the privacy of their communication safeguarded.

Our commitment to data protection goes beyond mere compliance with applicable laws and regulations. We strive to cultivate a culture of trust, transparency, and accountability when it comes to managing personal information. We believe that individuals have the right to know how their data is being collected, used, and protected. By adhering to this Data Protection Policy, we aim to foster a secure and respectful environment for our customers, Employees, partners, and other stakeholders. We understand the importance of safeguarding Personal Data not only to protect individuals' privacy but also to maintain the trust and confidence they place in us.

This Data Protection Policy is built upon a set of fundamental principles that guide our data protection practices. These principles include ensuring lawful, fair, and transparent processing of Personal Data, limiting data collection to specified and legitimate purposes, minimising the data collected to what is necessary, maintaining data accuracy and relevancy, setting limits on data retention, safeguarding data integrity and confidentiality, and being accountable for our data processing activities.

The objective of this Data Protection Policy is to ensure effective protection and management of the Personal Data of our customers, suppliers, Employees, workers and other third parties processed by the Company in an automated or non-automated manner, whether in manual, electronic or any other form. This includes ensuring responsible processing, outlining applicable standards and guiding on best practices for privacy and Personal Data protection.

We recognise that data protection is an ongoing commitment, and we continuously strive to improve our practices. Our Employees receive training and guidance to ensure that they understand their roles and responsibilities in safeguarding Personal Data. We regularly review and assess our data protection measures to adapt to evolving technologies and regulatory requirements, and we embrace opportunities to enhance the security and privacy of Personal Data. This Data Protection Policy's recommendations have considered the state of the Company's technological development, the cost of implementing any of the security measures, the special risks that exist in the processing of the data and the nature of the data the Company processes.

By implementing this Data Protection Policy, we aim to demonstrate our dedication to protecting Personal Data and respecting the rights of individuals. We invite all stakeholders to engage with us, provide feedback, and work collaboratively to uphold the highest standards of data protection. Together, we can foster an environment where privacy is valued, Personal Data is treated with care, and trust is preserved.

We encourage everyone associated with our Company to familiarise themselves with this Data Protection Policy, as it serves as a cornerstone of our commitment to data protection. We are determined to maintain the privacy and security of Personal Data while promoting responsible and ethical data-handling practices across our organisation.

2. Scope

This Data Protection Policy applies to:

- All Personal Data collected, stored, processed, or transmitted by the Company in any format, whether it electronic, paper, or verbal;
- The Company and all its operations within and outside Uganda in relation to the Data Subjects located in Uganda;
- All Company staff, who will include permanent, fixed term and temporary/casual Employees, interns (hereinafter “Employees”) and directors;
- All individuals who deal with the Company including third-party representatives, agents and representatives who are carrying out any work for or on behalf of the Company, operators, service providers, contractors and any associated third parties who handle and use Personal Data for or on behalf of the company in any format (hereinafter “Third Parties”); and,
- All data processed by the Company in an automated or non-automated manner and whether in manual, electronic or any other form.

All Employees and Third Parties who process Personal Data on behalf of the company are expected to comply with the company’s legal obligations in so far as they relate to the handling and processing of Personal Data.

3. Definitions

Applicable Laws means the Data Protection Act and the Regulations;

- Company means RANS;
- Complaint means an expression of dissatisfaction about the company’s handling of a Data Subject’s Personal Data;
- Consent means any manifestation of express, unequivocal, free, specific and informed indication of the Data Subject’s wishes by a statement or by a clear affirmative action, signifying agreement to the processing of Personal Data relating to the Data Subject;
- Data Protection Act means the Data Protection and Privacy Act, 2019, Laws of Uganda;
- Data Protection Policy means this Company Policy;
- Data Subject means an identified or identifiable natural person who is the subject of Personal Data (which phrase includes “Data Subjects”).
- ODPC means the Office of the Data Protection Commissioner established under Section 5 of the Data Protection Act;
- Personal Data means any information relating to an identified or identifiable, natural person, who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity;
- Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- Processing means any activity or operation or set of operations, whether of automated means or not, such as collection, recording, organisation, structuring; storage, adaptation or alteration; retrieval, consultation or use; disclosure by transmission, dissemination, or otherwise making available; or alignment or combination, restriction, erasure or destruction and will include any activity which will be deemed to be further processing of Personal Data;
- Regulations means the Data Protection and Privacy Regulations, 2021;
- Sensitive Personal Data means data revealing the natural person’s race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person’s children, parents, spouse or spouses, sex or the sexual orientation of the Data Subject; and,

- Third Party means a natural or legal person, public authority, agency or other body, other than the Data Subject, the Company or persons who, under the direct authority of the Company, are authorised to process Personal Data (which phrase includes “Third Parties”).

4. Personal Data Protection Principles

The Company follows the guiding principles outlined in the Applicable Laws for the processing of Personal Data and will endeavour to ensure:

- Lawfulness, fairness and transparency: That Personal Data is processed pursuant to Applicable Laws and in accordance with the right to privacy of the Data Subject, and in a lawful, fair and transparent manner in relation to any Data Subject. Data Subjects must be informed about the collection, use and disclosure of their data;
- Integrity, confidentiality and availability: The Company will employ industry best practices to prevent unauthorised modifications, corruption, or tampering of Personal Data. The Company will implement resilient infrastructure, regular backups, and disaster recovery measures to minimise downtime and ensure uninterrupted access by Data Subjects.
- Purpose Limitation: Personal Data is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes. Personal Data cannot be used for new, different or incompatible purposes from those disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and has Consented where necessary;
- Data Minimisation: Personal Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- Accuracy: Personal Data is accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate Personal Data is erased or rectified without delay;
- Storage Limitation: Personal Data is kept in a form which identifies the Data Subjects for no longer than is necessary for the purposes for which it was collected in accordance with the company’s data retention guidelines; and,
- Transfer Limitation:[2] Personal Data is not transferred outside Uganda unless there is proof of adequate data protection safeguards or Consent from the Data Subject. The Company may only transfer Personal Data outside Uganda if the following conditions are met:
 - i. Based on appropriate safeguards;
 - ii. There being an adequacy decision made by the ODPC;
 - iii. Where the transfer is necessary for the performance of a contract involving the Data Subject, is in the public interest, is in exercise or defence of a legal claim or is in the Data Subject’s interest; or,
 - iv. Subject to the Consent of the Data Subject.

5. Lawful Processing of Personal Data

In order to collect and process Personal Data, the Company must always have a legal basis and purpose for doing so. Consent to process a Data Subject’s Personal Data will not always be required. The Company may lawfully process Personal Data without a Data Subject’s Consent under the following circumstances:

- Where the processing is necessary for the performance of a contract with the Data Subject (for instance a contract of employment or registration with the Company as a vendor) or in order to take steps at the request of the Data Subject before entering into a contract;
- To meet the Company’s legal compliance obligations and requirements (for instance to comply with the employment laws);
- To protect the Data Subject’s or another person’s vital interests;

- Where the processing is in order to perform a public duty or to perform tasks carried out in the public interest;
- To pursue a legitimate interest (or those of a third party) for purposes where they are not overridden because the processing prejudice the interests or fundamental rights and freedoms of the Data Subjects; or,
- For historical, statistical, journalistic, literature and art or scientific research purposes.

Where the processing of a Data Subject's Personal Data is required for purposes which are not detailed above, the Company will obtain the Data Subject's Consent. In seeking Consent prior to processing, the Company will inform the Data Subject of the following:[4]

- The purpose of each of the processing operations for which Consent is sought;
- The type of Personal Data that is to be collected and used;
- Information about the use of Personal Data for automated decision-making, where relevant;
- The possible risks of data transfers due to the absence of an adequacy decision or appropriate safeguards;
- Whether the Personal Data processed will be shared with third parties; and,
- The right to withdraw Consent and the implications of providing, withholding or withdrawing Consent.

Additionally, when seeking Consent, the Company will ensure the Data Subject has the capacity to give Consent, voluntarily gives Consent, and the Consent is specific to the purpose of processing.

Where a third party provides the Company with another's Personal Data, the Company will make every effort to confirm that:

- It was collected by the third party in accordance with the Applicable Laws;
- such Personal Data was lawfully processed;
- That the sharing of the Personal Data with the company was clearly explained to the Data Subject by such third party; and,
- Where required Consent to process including sharing of the information was obtained from the Data Subject.

6. Processing of Sensitive Personal Data

Any Sensitive Personal Data will be processed in accordance with the Applicable Laws. This includes where:

- The processing relates to Personal Data which is manifestly made public by the Data Subject; or,
- Processing is necessary for:
 - i. The establishment, exercise or defence of a legal claim;
 - ii. The purpose of carrying out the obligations and exercising specific rights of the company or of the Data Subject; or,
 - iii. Protecting the vital interests of the Data Subject or another person where the Data Subject is physically or legally incapable of giving Consent.

Employees processing sensitive Personal Data on behalf of the Company must only process sensitive Personal Data on the grounds described above. Processing sensitive Personal Data without the Data Subject's Consent or where such processing cannot be justified may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties on the Company.

7. Collection of Personal Data

The Company may collect Personal Data directly from the Data Subject, or indirectly where:

- The Data Is Contained In A Public Record;
- The Data Subject Has Deliberately Made The Data Public;
- The Data Subject Has Consented To The Collection From Another Source;
- The Data Subject Has An Incapacity, The Guardian Appointed Has Consented To The Collection From Another Source;
- The Collection From Another Source Will Not Prejudice The Interests Of The Data Subject;
- The Collection From Other Sources Is Necessary:
 - i. For The Prevention, Detection, Investigation, Prosecution And Punishment Of Crime;
 - ii. For The Enforcement Of A Law Which Imposes A Pecuniary Penalty; Or,
 - iii. For The Protection Of The Interests Of The Data Subject Or Another Person.

Whenever Personal Data is collected directly from the Data Subject, the Company will, in so far as practicable, inform the Data Subject of the following:

- Their Rights – As Set Out In Section 25 Of This Data Protection Policy;
- The Fact That Personal Data Is Being Collected;
- The Purpose For Which Personal Data Is Being Collected;
- The Third Parties To Whom The Personal Data Has Been Or Will Be Transferred To Including Details Of Safeguards Adopted And Their Contact Details;
- A Description Of The Technical And Organisational Security Measures Taken To Ensure The Integrity And Confidentiality Of The Data;
- The Data Being Collected Pursuant To Any Law And Whether Such Collection Is Voluntary Or Mandatory; And,
- The Consequences If Any, Where The Data Subject Fails To Provide All Or Any Part Of The Requested Data.

The above information will be provided through appropriate privacy notices.

8. Data Subject Rights and Requests

Right to be informed of the use to which their Personal Data is to be put: The Company will pre-emptively provide clear and concise information about the purposes for which data is being collected, processed, and used.

Right to withdraw Consent: Where a Data Subject has given Consent to the processing of Personal Data, the Data Subject has the right to withdraw such Consent at any time. Such withdrawal will apply from the date of the withdrawal only and will not affect the legality of the processing of the Personal Data to which the Consent applied, prior to the withdrawal.

The right to object and/or restrict processing: A Data Subject may request the company to restrict the processing of their Personal Data where the accuracy of the Personal Data is contested, where the Personal Data is no longer required for the purpose of processing, or pending verification as to whether the company's legitimate interests override those of the Data Subject. A request for restriction to processing will be made in Form one set out in the First Schedule of the Regulations. The Company will consider and deal with such requests in accordance with the Applicable Laws.

Data access request: The Data Subject has the right to obtain from the Company confirmation as to whether or not Personal Data concerning them is being processed, and, where that is the case, access to the Personal Data and the information as to:

- The purposes of the processing;
- The categories of personal data concerned;

- The recipients or categories of recipients to whom the personal data have been or will be disclosed, including recipients in other countries or territories;
- Where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and,
- Where the personal data is not collected from the data subject, any available information as to the source of collection.

Subject, the Company will inform the Third Party that the Data Subject has requested rectification of their Personal Data.

Right to erasure: a Data Subject has a right to request that the Company erases the personal information which the Company holds about it in the following circumstances:

- The personal data is no longer necessary for the purpose for which it was collected;
- The data subject withdraws their consent that was the lawful basis for retaining the personal data;
- The data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing;
- The processing of personal data is for direct marketing purposes and the individual objects to that processing;
- The processing of personal data is unlawful including in breach of the lawfulness requirement; or,
- The erasure is necessary to comply with a legal obligation.

Right to object to direct marketing: A Data Subject who has opted into any form of direct marketing has the right to opt-out from any subsequent direct marketing, i.e. the right to ask the Company not to process its Personal Data for any further direct marketing purposes. Our opt-out mechanisms will be visible, clear and easily understood; will include a process for opting out that requires minimal time and effort; will provide a direct and accessible communication channel; will be free of charge or where necessary involve a nominal cost to a Data Subject; and, will be accessible to persons with a disability.

Right to object to decisions based solely on automated processing: a Data Subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the Data Subject. The Company will inform a data subject when engaging in processing based on automated individual decision-making.

Any requests by a Data Subject can be directed to

9. Sharing Personal Data

The Company may share Personal Data with any of its third-party service providers whose services are necessary to perform the Company's obligations. Personal Data will not be shared with any Third Parties, unless:

- There is a legitimate company need to share the Personal Data;
- The fact that Personal Data will be shared with third parties has been communicated to the Data Subject in a privacy notice beforehand; and,
- The person receiving the information has either agreed to keep the Personal Data confidential and to use it only for the purpose for which it was shared under a data transfer agreement or where acting as an operator or a processor, (i.e. such person will be processing the personal information on behalf of the Company), has concluded a written agreement with the Company, before receipt of the Personal Data.

10. Reporting Personal Data Breaches

The Applicable Laws require the Company to notify the ODPC of any Personal Data Breaches and in certain instances, the Data Subject. In line with the Applicable Laws, the company will notify the

ODPC of any notifiable Personal Data Breaches within 72 hours of becoming aware of such breaches.

Any discovered or suspected Personal Data Breaches including any losses comprising Personal Data must immediately be reported to the designated office or through

11. Retention of Personal Data

The Company will retain Personal Data only as long as may be reasonably necessary to satisfy the purpose for which the Personal Data was processed unless the retention is:

- Required or authorised by law;
- Reasonably necessary for a lawful purpose;
- Authorised or consented by the data subject; or,
- For historical, statistical, journalistic literature and art or research purposes.

The Company will ensure the deletion of Personal Data or the anonymisation of Personal Data to the extent that the Data Subject can no longer be identified, once the Company no longer has a legitimate need for such data.

12. Security, Integrity and confidentiality

The Company has put in place appropriate technical and organisational measures to implement the data protection principles in an effective manner. Employees must maintain data security by protecting the confidentiality, integrity and availability of Personal Data as follows:

- Only personnel who have a need to know and are authorised to use Personal Data can access it;
- Personal Data must be accurate and suitable for the purpose for which it is processed; and,
- Authorised users are able to access the Personal Data when they need it for authorised purposes.

13. Data Collected and Purpose of the Data Collected

The Company may collect the following data:

a. Personal Data:

- General Personal Data (e.g., name, address, contact details): We collect this information to maintain accurate records of our customers, suppliers, and business partners for effective communication, order fulfilment, and invoicing purposes.
- Employee data (e.g., name, address, contact details, employment history): We collect employee data to manage various aspects of the employment relationships, including payroll, benefits administration, performance evaluation, and compliance with legal obligations.
- Website usage data (e.g., IP address, cookies): We collect this information to analyse website traffic, improve user experience, and ensure the security and integrity of our online platforms.
- Financial data (e.g. bank account details, credit card information): We collect financial data to process payments, facilitate transactions, and maintain financial records in accordance with legal and accounting requirements.
- Real Estate data Real Estate and Property Data (e.g. land use information, property characteristics, location details, zoning and planning data, environmental and site conditions, and market-related indicators) This data is collected and processed to enable accurate property valuation, support due diligence, inform development and investment decisions, assess suitability and risk, ensure compliance with planning and regulatory requirements, and deliver appropriate real estate services to clients, tenants, investors, and other stakeholders.
- Marketing data (e.g., preferences, purchase history, feedback): We collect marketing data to tailor our promotional activities, deliver personalised offers, conduct market research, and improve our products and services based on customer feedback.

Data Retention Schedule

The Company reiterates that it retains Personal Data only for as long as necessary to fulfil the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce our agreements. Our data retention schedule is as follows:

Personal Data:

1. Customer and supplier data: We retain Personal Data related to customers and suppliers for the duration of the business relationship and for a period afterwards as required by contractual, legal, or regulatory obligations.
2. Employee data: Employee data is retained for the duration of employment and for a reasonable period afterwards to fulfil legal obligations, address potential disputes and maintain employment records.
3. Website usage data: Website usage data is retained for a period necessary to analyse traffic, ensure website security, and improve user experience.

The retention period may vary based on the nature and purpose of the data.

- Financial data: Financial data, including payment records and invoices, is retained for a period necessary to comply with accounting and tax regulations. Typically, financial data is retained for a minimum of seven (7) years from the end of the financial year in which the transaction occurred.
- Marketing data: Marketing data, including preferences, purchase history, and feedback, is retained for a period necessary to deliver targeted marketing campaigns, track customer preferences, and improve marketing strategies. The retention period may vary based on the effectiveness and relevance of the data for marketing purposes.

14. Responsibilities

All Employees who process Personal Data on behalf of the Company must read, understand and comply with this Data Protection Policy when processing Personal Data in the course of performing their tasks and must observe and comply with all Personal Data controls, practices, and protocols to ensure such compliance. Any breach of this Data Protection Policy and related company policies and procedures by Employees may result in disciplinary action.

Data Protection Officer

- The Company's data protection officer will be responsible for all matters relating to the Company's registration as a data controller or data processor.
- This officer will liaise with the ODPC and any other authority in all relevant respects, including reporting to and coordinating with the ODPC during periodic audits or any other regulatory activities conducted by the ODPC.
- The data protection officer will advise the Company on compliance with Applicable Laws and this Data Protection Policy.
- This officer will facilitate the capacity building of staff involved in any data processing operations.
- Where necessary, the data protection officer will be responsible for all data protection impact assessments and the generation of any appurtenant reports.
- The data protection officer will identify reasonably foreseeable internal and external risks to Personal Data under the Company's possession or control; and will establish and maintain appropriate safeguards against the identified risks.
- The officer will be responsible for suggesting which Personal Data will be anonymised, pseudonymised or encrypted.
- The officer will establish a personal data retention schedule with appropriate time limits for the periodic review of the need for the continued storage of personal data that is no longer necessary or where the retention period is reached.
- Where the company is a data controller, the data protection officer will review any written contracts and will advise the Company on any engagements with data processors.

15. Complaints Handling Mechanism

Data Subjects may make a complaint relating to the use of their Personal Data. Complaints should be sent directly to The Company will acknowledge the Complaint within 7 working days. The Company will only accept a Complaint from the Data Subject's representative if the representative provides the Data Subject's written Consent authorising the personal representative to act on the Data Subject's behalf in relation to the Complaint.

Once all the identification requirements have been verified, the investigation will be carried out within 30 working days. If further clarification is required from the complainant or more time is required for the response to be completed, the company will inform the complainant prior to the original deadline. The complaint outcome will be communicated to the complainant in writing by email.

If the complainant does not agree with or is dissatisfied with the outcome, they can request a review of the decision. If the complainant is aggrieved by the Company's decision after such review, the complainant may lodge a complaint with the ODPC.

16. Communication

a. Notice to Data Subjects

The Company adequately notifies all Data Subjects of the parts of this Data Protection Policy that are appropriate for such notification.

b. Incident Reporting

Any discovered or suspected Personal Data Breaches including any losses comprising Personal Data must immediately be reported to the designated office or through **mail@RANS.co.ke**. Employees are also encouraged to report any suspected or actual breaches of communication security or incidents that may compromise the confidentiality or integrity of data to the designated office or the data protection officer.

c. Employee Training and Awareness

The Company's Employees will be regularly trained on data privacy and security. Additionally, all Employees are expected to be familiar with this Data Protection Policy and their obligations herein.

d. Third-Party Communication

When communicating with Third Parties, the company takes reasonable steps to ensure the secure transmission of personal data and confidential information. This may include contractual obligations and due diligence to ensure the third party follows adequate data protection practices.

17. Approval, Review and Updates

I, _____, hereby acknowledge that I have received, read, and fully understood the **Rans Property Ltd Data Protection Policy**.

I confirm my commitment to comply with all operational requirements, standards, and responsibilities set out in this policy, together with any related procedures, guidelines, directives, or amendments issued by Rans Property Ltd from time to time.

I understand and accept that:

- Adherence to this policy is a mandatory condition of my employment, engagement, or authorization to act on behalf of Rans Property Ltd
- Any breach or failure to comply with this policy may result in corrective or disciplinary action, including but not limited to suspension, termination of employment or contract, and/or legal action, depending on the severity of the breach
- I am responsible for seeking clarification on any part of this policy that I do not clearly understand

- This policy applies to all operational activities of the real estate agency, including interactions with clients, partners, regulators, and any professional or public representation of the company

I further acknowledge that this policy may be reviewed and updated periodically, and that my continued engagement with Rans Property Ltd constitutes acceptance of the most current version of the policy.

Employee / Agent Declaration

Full Name: _____

Signature: _____

Date: _____

Employee / Agent ID: _____

Department / Branch: _____

Management Approval & Authorization

This policy is approved and issued under the authority of the management of Rans Property Ltd.

Chief Executive Officer (CEO)

Name: _____

Signature: _____

Date: _____

Policy Status & Review

This policy is a living document and shall be reviewed annually, or earlier where necessary, to accommodate changes in legislation, regulatory requirements, industry standards, or operational practices. All updates and revisions shall be communicated to relevant stakeholders in a timely manner.