Protection of Personal Information (POPIA) Policy

1. Purpose

The purpose of this policy is to ensure that Kuuh Internet Services (Pty) Ltd complies with the Protection of Personal Information Act, 4 of 2013 (POPIA). It sets out how personal information of employees, customers, suppliers, and other stakeholders is collected, processed, stored, and safeguarded.

2. Legal Basis

This policy is guided by:

- The Protection of Personal Information Act, 4 of 2013 (POPIA).
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA).
- The Electronic Communications and Transactions Act, 25 of 2002 (ECTA).
- Other applicable South African data protection and labour legislation.

3. Scope

This policy applies to all employees, contractors, service providers, and systems handling personal information on behalf of Kuuh Internet Services (Pty) Ltd. It covers:

- Employee records.
- Customer records (including RICA information, contact details, and billing data).
- Supplier and business partner information.

4. Definitions

- **Personal Information:** Any information relating to an identifiable individual, including names, ID numbers, contact details, addresses, billing and payment details.
- **Special Personal Information:** Identity documents and proof of residence collected for RICA purposes.
- **Processing:** Any operation involving personal information, such as collection, storage, use, modification, or deletion.
- **Responsible Party:** Kuuh Internet Services (Pty) Ltd, which determines the purpose and means of processing.
- **Operator:** Any third party processing personal information on behalf of Kuuh Internet Services (Pty) Ltd.
- **Data Subject:** Any individual whose personal information is processed by Kuuh Internet Services (Pty) Ltd.

5. POPIA Principles

Kuuh Internet Services (Pty) Ltd applies the following eight conditions for lawful processing:

1. **Accountability:** Management ensures compliance.
2. **Processing Limitation:** Only relevant information is collected, with consent or legal justification.
3. **Purpose Specification:** Information is collected for service delivery, regulatory compliance, billing, and support.
4. **Further Processing Limitation:** Data is not used beyond its original purpose without consent or lawful basis.
5. **Information Quality:** Records are kept accurate and up to date.
6. **Openness:** Individuals are informed why information is collected and how it will be used.
7. **Security Safeguards:** Data is protected against unauthorised access, loss, or damage.
8. **Data Subject Participation:** Individuals may access, correct, or request deletion of their personal data.

6. Collection of Personal Information

- **Employees:** Contact details, ID numbers, tax and banking information.
- **Customers:** Names, ID copies, proof of address, contact details, billing details, and service usage linked to accounts.
- **Suppliers:** Business registration details, contact persons, banking information.
- **Purpose:** Information is required for regulatory compliance, service delivery, financial administration, and customer support.

7. Use and Sharing of Personal Information

- Information is used strictly for providing services, regulatory compliance, and internal administration.
- Personal information may be shared with:
    - Regulators (e.g., SARS, Information Regulator, ICASA).
    - Banks (for payments).
    - Approved service providers acting on behalf of the company.
- Personal information will never be sold or shared for unauthorised purposes.

8. Security Safeguards

- Access to customer and employee information is restricted and monitored.
- Digital information is stored securely with encryption and access control.
- Paper records are stored in locked cabinets (if applicable).
- Regular backups and breach monitoring are in place.
- Any data breach must be reported immediately to the Information Officer.

9. Data Subject Rights

Individuals have the right to:

- Request access to their personal information.
- Request correction or updating of inaccurate information.
- Request deletion of information no longer legally required.
- Object to the use of their personal information for direct marketing.

10. Retention and Destruction

- Customer RICA records will be retained for at least 5 years after termination of services (per RICA).
- Employee records will be retained as required under labour and tax laws.
- Once retention periods expire, records will be securely deleted or destroyed.

11. Breach Management

In the event of a suspected or actual data breach:

1. The Information Officer must be informed immediately.
2. An internal investigation will be conducted.
3. If required, the Information Regulator and affected data subjects will be notified.

12. Roles and Responsibilities

- **Information Officer:** Responsible for compliance, breach reporting, and policy enforcement.
- **Employees:** Must safeguard information they handle, attend POPIA training, and follow this policy.
- **Management:** Ensures compliance, training, and enforcement.

13. Non-Compliance

Failure to comply with this policy may result in disciplinary or contractual consequences, as applicable.

14. Review of Policy

This policy will be reviewed regularly to ensure compliance with legislative and business requirements.