INFORMATION SECURITY POLICY

Real People Kenya Ltd

S. No	Version	Revision Date	Author	Areas Revised	Scope	Document Owner
1.	1.0.0	Nov-2013	CIO-EA	Initial Draft	GVR	CIO - EA
2.	2.0.0	Dec-2015	CIO-EA	Policy localization	GVR	CIO - EA
3.	3.0.0	Oct-2020	CIO	Scope	RPKL	CIO - RPKL
4.	3.0.1	Aug 2023	S. Riachi	7.1, 8.3.1-8.3.5, 9.3.1.7, 9.4, 9.6, 9.7.1.9	RPKL	ICT Department
5.	4.0.0	April 2025	S. Riachi	1.2-1.4, 2.1, 3.1.1,3.1.2, 6.2-6.5, 16, 17.27	RPKL	ICT Department

1. Introduction

1.1 Information is one of the most important assets in Real People Kenya Ltd (RPKL). Timely and accurate information is imperative towards the success of RPKL.

1.2 This policy establishes the framework for protecting information assets against threats to confidentiality, integrity, and availability.

1.3 RPKL must operate and be perceived as a safe and reliable organisation that ensures the security of the information assets, the reputation of the organization and the staff optimally.

1.4 For this reason, management has determined a need for, and is committed to, ensuring proper information security. This policy document serves to outline management's expectations of our IT systems and employees regarding information security. All personnel are required to abide by this policy document. Any deviations to this policy must first be authorized by Exco.

2. Definition

2.1 See Annexure on page 8.

3. Scope

3.1 This policy applies to:

3.1.1 All RPKL employees, contractors, consultants, and third parties

3.1.2 All information systems, whether owned or leased.

3.1.3 Cloud services and SaaS applications used for company business.

4. Statement of Policy

4.1 In business, having the right information at the right time can make the difference between profit and loss, success and failure. Information security will help us to control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure.

4.2 The objective of information security is to ensure:

4.2.1 A high level of *confidentiality*, i.e. protecting information from unauthorised disclosure.

4.2.2 A high level of *integrity*, i.e. protecting information from unauthorised modification, and ensuring that information can be relied upon as accurate and complete.

4.2.3 A high level of *availability*, i.e. ensuring information is available when needed.

4.3 Through meeting these objectives, we wish to:

4.3.1 Ensure that RPKL is perceived as a reliable and respected business partner (protect the reputation of the company);

4.3.2 Ensure correct access to the RPKL's information.;

4.3.3 Limit the impact of any damage to a defined and accepted scope;

4.3.4 Protect against violation or attempted violation of the security regulations and measures and ensure that violation or attempted violation can be discovered and tracked to the relevant person(s);

4.3.5 Reduce business and compliance risk.

5. Policy

5.1 It is RPKL's policy that all messages created, sent, or retrieved over the Internet e.g. through email systems using the RPKL system and network, are the property of RPKL. RPKL reserves the right to access the contents of any messages sent over its facilities if RPKL believes, in its sole judgment, that it has a business need to do so.

5.2 All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver, i.e. don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

6. Security Procedures

Security procedures should be defined, and it is the responsibility of each user to familiarise themselves with the content. These include but are not limited to:

6.1 Email Usage

6.1.1 All email messages sent externally should include RPKL's disclaimer.

6.1.2 Each email will be limited to a maximum size of 25Mb.

6.2 Access Control

6.2.1 Role-based access control is implemented.

6.2.2 Principle of least privilege is in place (i.e. users are granted the minimum necessary access)

6.2.3 Multi-factor authentication is required for key systems.

6.2.4 Password requirements are in place.

6.3 Network Security

6.3.1 Firewall implementation should be in place

6.3.2 Vulnerability scanning and penetration testing is conducted annually

6.3.3 Network segmentation between critical systems

6.3.4 Secure VPN for remote access

6.4 Endpoint Protection

6.4.1 Automatic critical updates and bug fixes for systems

6.4.2 Mobile device management policy

6.4.3 Encryption of all mobile devices and laptops

6.5 **Data Protection**

6.5.1 Information classification policy (Public, Confidential, Restricted)

6.5.2 Encryption of sensitive data when stored and/or in transit

6.5.3 Secure disposal procedures for media containing sensitive data

6.5.4 Regular backup verification and testing

7. Roles and Responsibilities

7.1 For this Policy to be effectively implemented, it is essential that security related roles are defined and that specific responsibilities are assigned to each of these roles.

7.2 CEO and Senior Management

7.2.1 Responsibilities:

7.2.1.1 Formally endorse and actively support this Policy

7.2.1.2 Approve all exceptions from external or non-secure networks

7.3 ICT Department

7.3.1 Responsibilities:

7.3.1.1 To develop, implement and periodically review the information security policy, procedures and controls;

7.3.1.2 Ensure that all appropriate personnel are aware of and comply with this policy;

7.3.1.3 Be informed in all firewall configuration changes;

7.3.1.4 Control the physical access to all IT Infrastructure controlled server rooms;

7.3.1.5 Performs monthly checks to ensure that access lists are up to date;

7.3.1.6 Safeguard the server room key.

7.4 IT Steering Committee.

7.4.1 A cross-functional forum of management representatives from relevant parts of the organization.

7.4.2 Responsibilities:

7.4.2.1 Monitor significant changes in the exposure of information assets to threats;

7.4.2.2 Review and monitor security incidents;

7.4.2.3 Approve major initiatives to enhance information security;

7.4.2.4 Actively promote information security within the organization.

7.5 Information Owners

7.5.1 Responsibilities:

7.5.1.1 Authorize access and assign custody of information;

7.5.1.2 Communicate the control requirements to the custodian and users of the information;

7.5.1.3 Determine the statutory requirements regarding retention and privacy of the information and communicate this information to the custodian.

7.6 Custodian - ICT staff

7.6.1 Responsibilities

7.6.1.1 Implementation of physical and technical controls;

7.6.1.2 Identifying procedural guidelines for the users;

7.6.1.3 Administering access to information;

7.6.1.4 Evaluate the cost-effectiveness of controls;

7.6.1.5 Perform regular disk capacity management on all application servers;

7.6.1.6 Ensure that the applications are available to the users;

7.6.1.7 Source and manage vendor support when calls are logged with vendors;

7.6.1.8 Ensure that user workstations are secured by screensavers where possible (maximum of 30 minutes unattended usage should start the screensaver);

7.6.1.9 Install and maintain appropriate anti-virus software on all servers and workstations as prescribed by RPKL;

7.6.1.10 Respond to all virus attacks, destroy any virus detected, and document each incident;

7.6.1.11 Ensure that all virus signature files must be automatically updated as and when released by the vendor. The Logon Scripts has to ensure that all system wide changes required as from time to time are timeously updated each time a workstation connects to the network via the logon script;

7.6.1.12 Block files if this poses a risk to overall security;

7.6.1.13 Install and maintain the firewalls.

7.7 Users

7.7.1 Responsibilities:

7.7.1.1 Use the information only for the purpose intended by the owner;

7.7.1.2 Comply with all the controls established by the owner and custodian;

7.7.1.3 Ensure that classified or sensitive information is not disclosed to anyone without permission from the owner;

7.7.1.4 Ensure that his/her identification and passwords are not disclosed to or used by others;

7.7.1.5 If your machine is removed by ICT staff to be configured, repaired or for software to be installed or restored, your password may be changed to a randomly generated password in order for the necessary work to be conducted. However, you are responsible for changing your password to a secure and confidential password immediately upon receiving of your machine back from ICT;

7.7.1.6 Employees shall not knowingly introduce a computer virus into RPKL computers;

7.7.1.7 Employees shall ensure that his workstation(s) and server(s) have RPKL's prescribed anti-virus software installed, active and with the latest pattern file;

7.7.1.8 Employee shall not load electronic - magnetic – or optical storage media of unknown origin;

7.7.1.9 Any employee who suspects that their workstation has been infected by a virus shall log a HIGH Priority call at the Incident Management Service (ims{at}realpeople.co.ke) desk;

7.7.1.10 All reasonable precautions must be taken to protect business critical data against unauthorised access, especially data on notebooks and portable data storage devices. For example: Leaving a laptop on the backseat of a locked car in a public area is not a reasonable precaution.

7.7.1.11 It will be the sole responsibility of the user to backup and maintain security of all business data;

7.7.1.12 Do not make unauthorised copies of data;

7.7.1.13 All notebooks are to be fitted with a computer security lock.

7.7.1.14 Employees must exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result;

8. Approach to Risk Management

8.1 A comprehensive Information Security Management System will be defined, implemented and maintained, based on our specific information security requirements and ISO27002 (a standard based on best practices and inter-organizational trust).

9. Outsourcing Management

9.1 An outsourcing contract between parties, addressing the potential risks, security controls and procedures for information systems and/or desk top environments, must be in place before the work can commence.

10. Information Security Awareness

10.1 The Information Security Officer is responsible to provide appropriate training to all users of information, including management, on:

10.1.1 The contents of this policy;

10.1.2 The specific information security controls and procedures introduced and

10.1.3 Their responsibility towards the Policy and meeting the information security objectives.

11. Maintenance of Policy

11.1 The Head of ICT will be responsible for the maintenance of the Policy on a continual basis or following any major security incident, acquisition or implementation of hardware and/or software, change to the Scope of Influence to this policy or any event affecting the applicability of this Policy.

12. Legal and Regulatory Requirements

12.1 All statutory, regulatory or contractual security requirements should be explicitly defined and documented for each information system. In addition to this, appropriate procedures should be implemented to ensure legal compliance to:

12.1.1 intellectual property rights, e.g., copyright, trademarks, etc.;

12.1.2 safeguarding of organizational records.

12.1.3 misuse of information processing facilities.

12.1.4 regulation of cryptographic controls and

12.1.5 collection of evidence.

13. Incident Handling

13.1 All information security incidents or suspected/potential security incidents must be reported to the ICT Support Desk using the Incident Management System (ims{at}realpeople.co.ke).

14. Compliance to Policy

14.1 This information security policy will be supported with standards, setting minimum levels for controls and procedures, on how to meet the security requirements identified. These controls and procedures will be reviewed and audited regularly to ensure ongoing compliance with the standards set.

15. Penalties and Consequences

15.1 Failure to adhere to this policy will be regarded in a very serious light and will lead to disciplinary proceedings and/or legal proceedings being instituted. This may lead to employees being subject to disciplinary sanctions which may include summary dismissal. This also applies to anyone who

attempts to disable, defeat or circumvent any RPKL security facility or making any misrepresentation to RPKL in respect of this policy.

16. **Policy Review**

16.1 This policy will be reviewed annually or as need arises to ensure it remains relevant.

 # End #

Signed By: Dr. Robert Shibutse

CEO – RPKL

DATE 30/05/2025

17. Annexure A - Definition of Terminology (Glossary)

This document deals with Information Security, a topic usually mainly familiar to the IT staff within the organization. Thus, certain terminology is used which is not known to the general staff. The following is a brief definition of those terms which may not be known to the general staff of the organization:

17.1 **Access**

To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

17.2 **Access control**

The enforcement of specified authorisation rules based on positive identification of users and the systems or data they are permitted to access.

17.3 **Auditability**

The ability to identify which users, both authorised and unauthorised, have performed certain tasks.

17.4 **Authentication**

The process that verifies the claimed identity of a station, originator, or individual as established by an identification process.

17.5 **Authenticity**

The ability to prove that a user is who he or she claims to be.

17.6 **Authorisation**

Positive determination by the owner of an information resource that a specific individual may access that information resource, or validation that a positively identified user has the need and the owner's permission to access the resource.

17.7 **Availability**

Ensuring that authorised users have access to information and associated assets when required.

17.8 **Confidential information**

Information maintained by RPKL that is exempt from disclosure under law. The controlling factor for confidential information is dissemination.

17.9 **Confidentiality**

Ensuring that information is accessible only to those authorised to have access.

17.10 **Critical information resource**

That resource determined by RPKL management to be essential to RPKL's critical mission and functions, the loss of which would have an unacceptable impact.

17.11 **Custodian of an information resource**

Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource. The custodian is normally a provider of services.

17.12 **Data**

A representation of facts or concepts in an organised manner in order that it may be stored, communicated, interpreted, or processed by automated means.

17.13 **Data integrity**

The state that exists when computerised information is predictably related to its source and has been subjected to only those processes which have been authorised by the appropriate personnel.

17.14 **Data security or computer security**

Those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.

17.15 **Disclosure**

Unauthorised access to confidential or sensitive information.

17.16 **Encryption**

The process of cryptographically converting plain text electronic data into a form unintelligible to anyone except the intended recipient.

17.17 **Exposure**

Vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

17.18 **Information resources**

The procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

17.19 Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

17.20 **Integrity**

Safeguarding the accuracy and completeness of information and processing methods.

17.21 **Owner of an information resource**

The manager or agent responsible for the function which is supported by the resource.

17.22 **Risk**

The likelihood or probability that a loss of information resources or breach of security will occur.

17.23 **Risk management**

Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

17.24 **Security controls**

Hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing it.

17.25 **Security incident or breach**

An event which results in unauthorised access, loss, disclosure, modification or destruction of information resources whether accidental or deliberate.

17.26 **Sensitive information**

Information maintained by RPKL that requires special precautions to protect it from unauthorised modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher-than-normal assurance of accuracy and completeness. The controlling factor for sensitive information is that of integrity.

17.27 SaaS – stands for Software as a Service, a cloud computing service that allows users to access software applications over the internet.

17.28 **User of an information resource**

An individual or automated application that is authorised access to the resource by the owner, in accordance with the owner's procedures and rules.