RIFUMO
EMPOWERMENT HOLDINGS (PTY) Ltd

Microsoft
Solutions Partner

Acceptable Use Policy

Document Number:

Effective Date:

Review Date:

Version: 1.0

Document Control

Document Version History

This table shows a record of significant changes to the document.

Version	Date	Author	Description of Change
1.0		Tebogo, Puke and Nkosana	17 June 2025

APPROVALS

This table shows the approvals on this document for circulation, use, and withdrawal.

Version	Date	Approver	Title/Authority	Approval Remarks
1.0		Mitch Chanza	CTO	
1.1		Thompson Mpenyane	Group Executive Chairman	
1.2				

TABLE OF CONTENTS

1. Overview

Rifumo Empowerment Holdings provides computer devices and other electronic information assets, and it becomes the responsibility of the user of the equipment, devices, and information, to responsibly maintain the confidentiality, integrity, and availability, within the framework of Information Security policies at Rifumo Empowerment Holdings.

2. Purpose

The purpose of this procedure is to set out the rules for acceptable use of Company information systems and services for individuals that have been authorized to use or access the Company information systems. To identify organizational assets and define appropriate protection responsibilities.

The Company uses digital assets for its operations. This policy is in place to protect the Company's information against loss or theft, unauthorized access, disclosure, copying, use, modification, or destruction.

3. Scope

This policy applies to all the Company's directors, officers, and employees, as well as third-party contractors and agents who have access to Company information or Computer Systems that the Company owns or leases.

4. Unacceptable Use

The lists below are not exhaustive and only provide examples of unacceptable use:

5. Security Cameras

In the areas where security cameras are placed, there should be no physical barriers to prevent the cameras from taking images, the cameras should not be closed, and physical damage should not be done. In case of detection of such situations, the relevant security units should be informed.

6. Cabinets and Printers

Cabinets and printers where Company data are stored should not be kept open for unauthorized access, they should be locked before leaving work areas, and keys should be kept in a secure area. Food and beverage items should be stored separately from documents for the documents not to be damaged.

7. Internet Access

- Users cannot give or make others use their internet access credentials.
- The downloading or distribution of illegal, offensive, or inappropriate content is strictly forbidden. This prohibition extends to content that may be discriminatory, harassing, or harmful to our organization's reputation.
- Transactions that may conflict with the interests of the Company and negatively affect the image, operations and activities of the Company cannot be performed with internet access.

- No copyright infringement operations, such as the use of unlicensed software, unauthorized access to intellectual and artistic works, duplication and sharing are carried out through internet access.
- Internet access is not used to store, link, access and send inappropriate content.
- Do not enter suspicious and uncertain websites. Files cannot be downloaded from these sites. Application and mobile code (ActiveX, Java, etc.) installation requests encountered on such sites are not accepted.
- Employees other than permitted employees cannot participate in discussions, forums, news boards and chat rooms provided by the internet with their corporate identities. It cannot act in a way that harms the corporate identity, and cannot express opinions, ideas, and explanations on behalf of the Company.
- Port scanning, security scanning, network monitoring and similar administrative activities cannot be carried out within the Company without informing the ISMS Team leader, even if it is a job requirement.
- Users cannot retrieve or try to retrieve data without authorisation.
- Any activity that may expose the Company's critical information or render Company services inaccessible is prohibited.

8. Hardware

- Desktop/ Laptop computers must be physically protected and positioned to avoid damage.
- It should be preferred to keep computer cases on the table. Concussions, physical impacts, and liquid contact should be avoided.
- Unauthorized hardware or software installations are strictly prohibited. Such actions can introduce security vulnerabilities and compromise the stability of our IT infrastructure.
- Users are responsible for the proper care and maintenance of company-provided hardware. This includes protecting devices from physical damage, ensuring software updates are installed, and reporting any malfunctions promptly.
- Company hardware must never be used for illegal activities. This prohibition underscores our commitment to ethical conduct and compliance with all applicable laws.
- Computers should be turned off outside of working hours. If the computers must be left on due to a systemic necessity, their monitors should be turned off.
- Users should not allow other employees to use the personal computers allocated to them, except in obligatory cases.
- No additional hardware, apparatus or software can be installed on personal computers, except for the IT Support unit.

- Hardware and apparatus on personal computers cannot be removed from devices other than the IT Support unit and cannot be used for other purposes.

9. Software Usage

Only licensed software, approved by the IT department, may be installed on company devices. This policy ensures compliance with copyright laws and protects our systems from potentially harmful or unauthorized software. To control this, the measures implemented by the Company must be followed.

10. System and Network Activities

Without exception, the following acts are strictly prohibited:

- Violating any person's or Company's rights under copyright, trade secret, patent, or other intellectual property laws, such as installing or distributing "pirated" or other software products that are not properly licenced for use by Company.
- Using any Company account to make fraudulent or deceptive offers of products or services.
- Introducing malicious programmes (e.g., viruses, worms, Trojan horses, e-mail bombs, and so on) to the Company's network or server, or to any other computer system.

11. Communication and E-mail/Instant Messaging Activities

- Company email and access are tools for business-related communication and research. While occasional personal use is acknowledged, it should not impede work-related activities or compromise network security.
- Users must exercise extreme caution when opening email attachments or clicking on links from unknown sources. Phishing attacks and malware distribution are prevalent threats, and vigilance is essential for protecting our systems.
- Sending unsolicited email communications, such as "junk mail" or other advertising material to those who haven't asked for it (email spam)
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or collect replies.
- Use of unsolicited email
- Employees should be educated, and training sessions with fake phishing scenarios should be held.

12. Use of Recording Devices

- In the areas where the Company operates, sounds or images should not be recorded secretly without the permission of the people by using audio and video recording devices.
- Secure areas such as system rooms, safe rooms, computer screenshots, meetings, interviews, and interviews should not be recorded.

- Company employees and suppliers are informed about this.
- In the areas where the company registers for security reasons, information is given with warning signs so that those entering the areas can see it.

13. Archiving

- All messages sent to and from Company e-mail addresses can be archived.
- The Company can start and end the archiving process at any time without prior notice to the employees. These e-mails can be used as evidence by Company audit units and relevant official authorities in case of conflict.
- Employees ensure that e-mail messages containing critical Company data remain on Company servers so that they can be backed up appropriately. Employees are responsible for deleting unnecessary messages from the e-mail server.
- The responsibility for backup and security of e-mails transferred to the employee's own backup media via Company servers is the employee's own responsibility.

14. Blogging and social media

- The policy on appropriate usage also applies to blogging.
- Users must exercise extreme caution when opening email attachments or clicking on links from unknown sources. Phishing attacks and malware distribution are prevalent threats, and vigilance is essential for protecting our systems.
- Using Company's trademarks, logos, or any other intellectual property without specific permission from the Legal Department; attributing personal statements, opinions, or beliefs to Company; or using Company's trademarks, logos, or any other Company intellectual property are prohibited without specific permission from the Legal Department.
- When blogging or otherwise engaging in any conduct, making any discriminatory, defamatory, or harassing comments is banned by the Company's Non-Discrimination and Anti-Harassment Policy.

15. Employee Responsibilities

- Any security flaws, incidents, probable misuse, or policy violations must be reported by justified employee personnel shall contact the IT helpdesk Team and ensure that the latest version of antivirus software is installed on their desktop / laptop and that the virus definitions are updated before attempting to access data, information, applications, or programmes contained on information systems for which they do not have authorisation or approval from the owner.
- Employees are not permitted to change the configuration of, remove, deactivate, or otherwise tamper with any antivirus programme or other software installed on their systems.

- Where a mobile device policy permits for the use of privately owned devices (e.g., Bring Your Own Device – BYOD), security measures such as separating personal and work use of the devices must be considered. Personnel must take reasonable steps to safeguard the device's physical security as well as the security of any business information stored on it.

16. Information Security Department

- Rifumo Empowerment Holdings Information Security Department authorized personnel shall, for security, compliance, and maintenance purposes, monitor and audit equipment, systems, and network, as per this policy.
- Devices that interfere with other devices or users on the Rifumo Empowerment Holdings network shall be disconnected.
- Any Breach of Information Security policies, practices by personnel, or information assets shall be reported to Information Security Team.
- Users shall be responsible for the security of information assets, including information and all devices, as deemed to be provided and approved by the Management.
- User shall not share passwords, accounts details, or any other information on Information assets with anyone, including other personnel, families, and friends.
- Violation of clause five shall be deemed to be a violation of this policy.
- User of any password is required to adhere to the password policy.
- User shall ensure to lock the screen when the information assets are left unattended or not in use, as per clear screen and Clear Desk Policy,
- All devices not in use and unattended shall have an automatic activation feature of screen saver activation within 5 minutes.
- User shall not take out information assets, paper, or electronic information.
- User shall be required to take prior approval of only and information security team.
- Violation of clause 4.6.1 shall be deemed to be a violation of this policy.
- The following are Prohibited, as per this policy, user is requested to comply with this policy in words and true spirit of the policy, but not limited, including,
- User shall not use Rifumo Empowerment Holdings e-mail or IP address that violates Rifumo Empowerment Holdings policies or guidelines,
- User devices use information assets, approved, and provided by Rifumo Empowerment Holdings, other than for inappropriate use.
- User shall be responsible for the use of information assets.
- User shall exercise good judgment to avoid any violation of mentioned policy, or in case he does not know the policy, in whole or is aware partially, of acceptable usage of the information asset,

- User will refer it to the superior or to the Information Security team located at Rifumo Empowerment Holdings, Roodeport.
- In case of violation of the policy, the User is subjected to disciplinary action, as per Rifumo Empowerment Holdings Disciplinary guidelines & policies.
- For the whole information life cycle, acceptable usage policies should be developed in accordance with the material's classification and identified hazards. The following things should be considered:
    - Access limitations that support each level of classification's protection criteria.
    - Keeping track of the resources' authorised users as well as other related information.
    - Information copies, whether they are temporary or permanent, should be protected to the same extent as the original data.
    - Storage of information assets in accordance with manufacturer's instructions.
    - All copies of storage media, whether digital or physical, should be clearly marked with the authorised recipient's attention.
    - Approving the disposal of data, related assets, and supported deletion technique(s).

17. Incidental Use

Incidental usage of Information Resources is permitted for the convenience of Rifumo Empowerment Holdings personnel. The following limitations are in effect:

- Personal use of electronic communications, Internet access, fax machines, printers, copiers, and other office equipment is limited to (Company) approved personnel; it does not include family members or other acquaintances.
- Indirect costs should not be incurred as a result of incidental use.
- Accidental usage should not interfere with an employee's ability to fulfil his or her job obligations.
- No files or documents may be transferred or received that may expose (Company) or its customers to legal action or embarrassment.
- Personal email communications, voice messages, files, and papers must be kept to a minimum within (Company) Information Resources.

18. Training and Awareness

- Prior to or within 30 days of being provided access to any Information Resources, all new employees must complete an authorized security awareness training course.
- Before being permitted access to Information Resources, all personnel must be supplied with, acknowledge receipt of, and agree to follow the (Company) Information Security Policies.
- Annual security awareness training is required for all employees.

- Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources.
- Employees are responsible for their use of any information processing resources and of any such use carried out under their responsibility.

19. Management Responsibility

The BOARD OF DIRECTORS OR Executive OR CTO oversees the overall operation of this policy, but Information Security Team oversees the day-to-day implementation. All managers have a specific duty to operate within the parameters of this policy, to take appropriate steps to ensure that all employees understand the anticipated standards of behaviour, and to act when behaviour falls short of those standards. Managers will receive training to enable them to do so.

- The asset managers are responsible to monitor the employees who work according to the policy.
- The Security manager is responsible to detect a breach of emails and social media breach.

20. Intellectual Property Rights

- The Company retains all rights, title, and interest in any Company Intellectual Property created, conceived, developed, contributed to, or improved upon by the employee during his employment, and such creation, conception, development, contribution, or improvement shall vest with the Company upon such creation, conception, development, contribution, or improvement.
- The employee shall not reverse-engineer, decompile, or disassemble any methodologies, software, whitepaper article, themes, headlines, or Confidential Information disclosed under this Agreement, and shall not remove, overprint, deface, or change any notice of confidentiality, copyright, trademark, logo, legend, or other notices of ownership from any originals or copies of Confidential Information it receives from the Company.
- During the Employment, whatever gets created, developed, or modified in the form of any hardware or software design, engineering, hardware code, software code, hardware and software library, schematic, architecture, layout, protocol, model, or any Intellectual Property or document in any format by the employee with or without the assistance or involvement of any other Person during the Term using own tools or the Company's or its partners/Affiliates' tools and systems with or without the assistance or involvement of any other Person.