Acceptable Use Policy

rain Group Holdings (Pty) Ltd, Reg. 1947/024435/07, together with its subsidiaries

This Acceptable Use Policy (the "Policy") sets out how you may and may not use rain's services and network. It protects our customers and the wider internet community from abusive or illegal activity, helps us provide a reliable service, protects the integrity of our network, and keeps us compliant with South African law.

This Policy forms part of, and must be read with, the rain Terms & Conditions and Privacy Policy. As a member of the Internet Service Providers' Association (ISPA), rain also subscribes to the ISPA Code of Conduct. Where this Policy conflicts with any product-specific terms, the product-specific terms prevail on pricing, product features and customer entitlements, while this Policy prevails on prohibited use, security, network management and fair-use enforcement.

By using any rain service you agree to comply with this Policy. If you do not agree, you must stop using the service and notify us so your account can be closed.

1. Scope and changes

1.1 This Policy applies to all rain customers and anyone who has access to rain's network.

1.2 We may revise this Policy at any time by posting a new version at rain.co.za. Revisions take effect immediately on posting and replace earlier versions, so please review it regularly to make sure your activity complies with the current version.

1.3 Failure to comply with this Policy or any other rain policy could result in suspension or termination of your service.

2. Your responsibilities

2.1 You are responsible for all use of your service, even if the misuse is committed by a family member, friend or guest. Keep your username and password confidential and secure.

2.2 You are solely responsible for the security of any device you connect to the service and any data stored or shared on it. Secure your equipment against viruses, spam and intrusion, and protect any shared files or printers with a strong password.

3. Prohibited uses and activities

You may not use the service to do any of the following (this list is not exhaustive):

- Carry out any illegal or unlawful activity, including posting or transmitting material that is defamatory, obscene, discriminatory, threatening or unlawful, that infringes intellectual property rights, or that encourages criminal conduct or civil liability.
- Post or transmit material that a reasonable person would find objectionable, offensive, indecent, pornographic, harassing, hateful, or racially or ethnically offensive.
- Gain or attempt to gain unauthorised access to any computer, system, network, account or data; breach security or authentication; or probe, scan or test the vulnerability of any host, network or account without authorisation. Unauthorised port scanning is strictly prohibited.
- Use or distribute tools designed to compromise security, such as password crackers, packet sniffers, decoders, Trojan horses or encryption-circumvention devices.
- Reproduce, distribute or sublicense copyrighted or proprietary material, or rain or third-party software, without the owner's permission.
- Restrict, inhibit, disrupt or degrade any other person's use of the service, or the service, network, servers or facilities themselves – including by transmitting viruses, worms or harmful code, or generating excessive traffic.
- Exceed current bandwidth, data-storage or other limits, place an excessive burden on the network, or set up a LAN behind the user terminal in breach of this Policy.
- Send unsolicited bulk or commercial messages (spam), chain mail, or numerous duplicate or empty messages; harvest email addresses or identifiers; or collect responses from unsolicited messages.
- Impersonate any person or entity, falsify sender or header information, forge signatures, or carry out any similar fraudulent activity.
- Service, alter, modify or tamper with rain equipment or the service, or let an unauthorised person do so.
- Collect personal information about third parties without their consent, or interfere with networking or telecommunications service (for example through denial-of-service attacks or flooding).

4. Network and system security

4.1 You may not circumvent the authentication or security of any host, device, network or account ("hacking"), interfere with service to any user ("denial-of-service"), or use any host, network or account for an illegal purpose, including phishing.

4.2 Examples of security violations include unauthorised access to or monitoring of data, systems or networks; mail bombing or flooding; deliberate attempts to overload a system; and forging packet headers or email/newsgroup header information (spoofing).

4.3 If our network security is breached, rain will take appropriate civil and criminal action, may investigate the incident, and will cooperate with law enforcement where a criminal violation is suspected. The rain website is protected by reCAPTCHA, to which Google's Privacy Policy and Terms of Service apply.

5. Fair use and network management

5.1 You must comply with all current bandwidth, data-storage and other limits, and use only a dynamic IP address (DHCP) unless your plan expressly permits otherwise. Your activity must not unfairly restrict, degrade or burden other users or rain's ability to deliver and monitor the service. All services have a total capacity limit.

5.2 To keep usage fair and protect the network, rain may limit throughput, restrict specific ports or protocols, or terminate service to customers who grossly abuse the network through improper or excessive use. rain's 5G network prioritises downlink speeds, so uplink speeds are expected to be slower.

5.3 rain cannot control the data passing over the internet and is not responsible for it, but you must comply with the acceptable-use policies of any other network you connect to, and you may not distribute copyrighted material without permission or obtain or facilitate unlawful material such as child sexual abuse material or unlawful hate speech.

6. Messaging, content and newsgroups

6.1 The service may not be used to send unsolicited bulk or commercial email, to collect responses from such email, or to forge, alter or remove email headers. You may not reference rain in any unsolicited email. Mailing lists are permitted only with the consent of list members, and undeliverable or unwilling addresses must be removed promptly. Mail servers must be secured against public relay, and rain may check this in accordance with its Privacy Policy.

6.2 Newsgroup posts must comply with the relevant newsgroup charter; excessive cross-posting and off-topic posting (USENET spam) are forbidden. You are solely responsible for the content of your instant messages, and rain is not responsible for their delivery or storage.

6.3 rain may refuse, remove or block any content it considers offensive, indecent or inappropriate. rain has no obligation to monitor transmissions, but reserves the right to do so to identify violations and protect the network and its customers.

7. Copyright and intellectual property

7.1 You must comply with South African copyright law and may not store or distribute material over the service that infringes third-party intellectual property rights.

7.2 Copyright owners may report alleged infringements stored on the service. On receiving a satisfactory notice, rain will expeditiously remove or disable access to the material and notify the affected customer, who may submit a counter-notification. rain will not be a party to disputes about alleged infringement.

7.3 In terms of section 75 of ECTA, rain has designated ISPA as its agent to receive take-down notifications. Take-down notices should follow the process at ispa.org.za/tdn (complaints@ispa.org.za). rain is legally required only to establish whether a notice is procedurally correct, not whether the material is in fact unlawful.

8. Protection of minors

You must ensure that children do not use the service to access illegal content, including pornography and gambling, and you must lock the service with a password to prevent unmonitored access.

9. VPN policy and use as intended

9.1 All VPNs are currently allowed, but rain reserves the right to determine which VPN protocols are supported and to throttle or terminate VPN services in line with this Policy, to ensure products are used as intended and fairly across all customers.

9.2 rain has no obligation to support use outside the intended design of a service or product (including misapplication or use of intermediary software such as VPNs). If rain determines a service is being used outside its intended design, it may throttle or terminate the service, and is not liable for any resulting problem.

10. Monitoring, enforcement and consequences

10.1 rain does not routinely monitor accounts, but will respond appropriately to inappropriate use. We prefer to advise customers of an issue and the corrective action needed, but where a service is used in breach of this Policy we may take any responsive action we consider appropriate.

10.2 Such actions include removing or blocking content, filtering transmissions, recovering equipment, and suspending or terminating all or part of the service. We may investigate suspected violations, gather information, examine material on

our network, and cooperate with law enforcement (including providing personally identifiable information where appropriate).

10.3 For individual customers, rain may suspend the account and withdraw network access, and may institute legal action for administrative and other costs. In severe cases, rain may suspend an entire network until abuse is prevented, apply technical measures such as shutting down affected ports or services, and share incident information with other providers or law enforcement. Neither rain nor its suppliers are liable for these responsive actions, and rain's failure to enforce the Policy is not a waiver of its rights.

10.4 You indemnify and hold rain, its affiliates, suppliers and agents harmless against all claims and expenses (including legal costs) resulting from your prohibited activity or breach of this Policy. This indemnity survives termination.

11. Reporting abuse

If you believe you have been the victim of internet abuse on the rain network, please report it to rain's abuse department. Where possible, provide the date and time of the incident (including time zone), and any evidence such as full email headers or syslog files.

Questions about this Policy can be sent to legal@rain.co.za, or contact the Customer Engagement Centre on 081 610 1000.