Virtual Comms (Pty) Ltd Acceptable Use Policy

General

Please read this document carefully before accessing Virtual Comms network and systems. By using any Virtual Comms internet service you agree to comply with the terms of our acceptable use policy.

This Policy applies to all customers who acquire Internet Services from us, including but not limited to, any service providing access to the Internet. Your obligation to comply with this Policy includes your obligation to ensure any person who you allow to use your Internet Service also complies with this Policy.

Virtual Comms reserves the right to amend the AUP from time to time and an update version will be located at:
www.virtualcomms.co.za/docs/AcceptableUsePolicy.pdf.
Customer's continued use of Virtual Comms service after changes to the AUP is posted, will constitute acceptance of the variation.

SPAM and Unsolicited Email

Sending unsolicited commercial communication is not permitted via Virtual Comms' network.

Spam/E-mail abuse shall include, but are not limited to, the following activities:

- use of an e-mail account to send an unsolicited bulk or commercial message is prohibited on your Virtual Comms account. This includes but is not limited to, advertising or promotion of products or services; petitions for signatures or requests for charitable donations and political or religious tracts.
- sending multiple unsolicited e-mail messages or "mail-bombing" to one or more recipient
- Sending emails where the recipient must opt-out of receiving further emails that they didn't originally request is considered unsolicited.
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the Virtual Comms network or of the networks with which Virtual Comms interconnects, by virtue of quantity, size or otherwise;
- use of e-mail to harass or intimidate other users is prohibited.
- sending e-mail that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;

Mailing list operators should maintain meaningful records of recipient requests and their consent to receive said email communications. There should also be an option for the recipient to unsubscribe from receiving further email communications.

Complaints can be send to info@virtualcomms.co.za. If Virtual Comms receives a spam complaint, in order to establish if the communication was unsolicited, we may ask you to verify whether the recipient agreed to receive communications from you and if so, when and where you recorded their email address.
Virtual Comms reserves the right to suspend or terminate the account of any user who sends out unsolicited email otherwise known as Spam with or without notice.

Account and Network Security

It is your responsibility to keep your password secure and not to share your password and account access with anyone. Attempting to obtain another user's account information is strictly prohibited, and may result in termination of service.

It is also your responsibility to implement security measures to the following (but not limited);

- Installing licensed internet security software, which includes, but are not limited to protection against internet threats such as viruses, malicious software, spy-ware, hacking attempts, etcetera;
- Monitoring your internet account for irregularities. Users are ultimately responsible for all actions taken under their account.

Virtual Comms reserves sole discretion to determine whether any customer's use of Virtual Comms service interferes with other customers' use and enjoyment of any services provided by Virtual Comms to customers over the same network.

Security Violations shall include, but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- you may not provide network services from your account
- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- You may not use resource-intensive programs which negatively impact other customers or the performance of Virtual Comms systems or networks. Virtual Comms reserves the right to terminate or limit such activities;
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software;
- Failure to take reasonable security precautions to help prevent violation(s) of this AUP.

Illegal Activities

You are responsible for determining the content and information you choose to access on the Internet when using your Internet Service. Virtual Comms does not allow any of the following content or links to such content:

- **Child Pornography – Virtual Comms services** shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography.
- **Inappropriate Interaction with Minors:** Virtual Comms services should not be used for the purpose of commission an offence against a child or in way that would constitute or promote unlawful interaction with children.
- Content of a pornographic, sexually explicit or violent nature.
- "Hate" sites or content that could be reasonably considered as discriminatory in any way including by way of sex, race or age discrimination.
- Content of an illegal nature (including stolen copyrighted material).
- Content that is defamatory or violates a person's privacy.
- Content that involves theft, fraud, drug-trafficking, money laundering or terrorism.
- intentionally spreading or threatening to spread computer viruses;
- Pirated software sites.
- Illegal gambling sites.
- any other activities declared to be illegal in terms of any applicable law.

If Virtual Comms in its sole discretion determines that any customer content violates any law, it may:

- Request the customer to immediately remove such content
- Immediately suspend or termination the services without notice to you
- Notify the relevant authorities of the existence of such content

Internet usage

Virtual Comms Internet services / products are designed for either home or business use, and customers need to select the appropriate package designed for their type of usage application. Virtual Comms uncapped products are not capped in the ordinary course. However, Virtual Comms reserves the right to apply restrictions on an uncapped account if a customer's behaviour is determined to be affecting the user experience of other customers on Virtual Comms' network. Such restrictions may include but are not limited to throttling a customer's throughput speeds to an appropriate proportion of the actual speed.

A Fair usage Policy does apply to Virtual Comms uncapped Lite packages, which is located at: www.virtualcomms.co.za/docs/FairUsagePolicy.pdf. Shaping is implemented via download throttling and priority control. Virtual Comms reserves the right to suspend or terminate the services if you unreasonably or excessively use the capacity or resources of our Network in a manner which may hinder or prevent us from providing services to other customers or which may pose a threat to the integrity of our Network or systems.

Breach of Acceptable use Policy

Virtual Comms reserves the right to suspend or terminate your Internet Service if you are in breach of this Policy. Our right to suspend or terminate your Internet Service applies regardless of whether the breach is committed intentionally, through misconfiguration, or by other means not authorized by you including but not limited to through a Trojan horse or virus.

In addition to the above, users who violate systems or network security may incur criminal or civil liability. Virtual Comms will co-operate fully with investigations of violations of systems or network security at other sites, including co-operating with law enforcement authorities in the investigation of suspected criminal violations.

Complaints

Complaints regarding violation of this AUP should be forwarded to info@virtualcomms.co.za or you can contact us on 018 468 2119.