MORUPA MARKETING & COMMUNICATIONS (Pty) LTD

MORUPA ACCEPTABLE USE POLICY (UAP)

General

By contracting with us for services, you agree, without limitation or qualification, to be bound by this Policy and the terms and conditions it contains, as well as any other additional terms, conditions, rules or policies which are displayed to you in connection with the services/website.

The purpose of this AUP is:

- to ensure compliance with the relevant laws of the Republic;
- to specify to clients and users of our service what activities and online
- behaviour are considered an unacceptable use of the service;
- to protect the integrity of our network; and
- to specify the consequences that may flow from undertaking such prohibited activities.

This document contains a number of legal obligations which you will be presumed to be familiar with. As such, we encourage you to read this document thoroughly and direct any queries to our client services/legal department at +27-11-612-7200.

Morupa respects the rights of our clients and users of our services to freedom of speech and expression; access to information; privacy; human dignity; religion, belief and opinion in accordance with our Constitution.

Unacceptable Use

Morupa's services may only be used for lawful purposes and activities. We prohibit any use of our website/network including the transmission, storage and distribution of any material or content using our network that violates any law or regulation of the Republic. This includes, but is not limited to:

- Any violation of local and international laws prohibiting child pornography; obscenity; discrimination (including racial, gender or religious slurs) and hate speech; or speech designed to incite violence or hatred, or threats to cause bodily harm.
- Any activity designed to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.
- Any violation of Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets.
- Any violation of another's right to privacy, including any effort to collect personal data of third parties without their consent.
- Any fraudulent activity whatsoever, including dubious financial practices, such as pyramid schemes; the impersonation of another subscriber without their consent; or any attempt to enter into a transaction with Morupa on behalf of another subscriber without their consent.
- Any violation of the exchange control laws of the Republic.
- Any activity that results in the sale, transmission or distribution of pirated or illegal software.
- Failing to respond to a request by a recipient of unsolicited mail to be removed from any mailing or direct marketing list and continuing to send unsolicited mail following such a request for removal.

Threats to Network Security

Any activity which threatens the functioning, security and/or integrity of Morupa's network is unacceptable. This includes:

- Any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by Morupa for this goal.
- Any effort to use Morupa's equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking").
- Forging of any TCP/IP packet headers (spoofing) or any part of the headers of an email or a newsgroup posting.
- Any effort to breach or attempt to breach the security of another user or attempt to gain access to any other person's computer, software, or data without the knowledge and consent of such person.
- Any activity which threatens to disrupt the service offered by Morupa through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of others' networks.
- Any activity which in any way threatens the security of the network by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus, trojan horse, worm, malware, botnet or other harmful, destructive or disruptive component.
- Any unauthorised monitoring of data or traffic on the network without Morupa's explicit, written consent.
- Any unsolicited mass mailing activity including direct marketing; spam and chain letters for commercial or other purposes, without the consent of the recipients of those mails.
- Running services and applications with known vulnerabilties and weaknesses, e.g. insufficient anti-automation attacks, any traffic amplification attacks, including recursive DNS attacks, SMTP relay attacks.
- Failing to respond adequately to a denial of service attack (DOS / DDOS). If your facilities are targeted by a DOS attack that affects other network users, your service will be suspended.

Public Space and Third Party Content and sites

You acknowledge that Morupa has no power to control content passing over the Internet, its facilities and its applications, including email; chat rooms; news groups; or other similar fora, and that Morupa cannot be held responsible or liable, directly or indirectly, for any of the abovementioned content, in any way for any loss or damage of any kind incurred as a result of, or in connection with your use of, or reliance on, any such content.

Our services also offer access to numerous third party web pages. You acknowledge that we exercise absolutely no control over such third party content or sites nor are we obliged to monitor our network: our network is merely a conduit or means of access and transmission. This includes, but is not limited to, third party content contained on or accessible through the Morupa network websites and web pages or sites displayed as search results or contained within a directory of links on the Morupa network. It remains your responsibility to review and evaluate any such content, and that any and all risk associated with the use of, or reliance on, such content rests with you.

Access to public Internet spaces, such as bulletin boards, Usenet groups, chat rooms and moderated forums is entirely voluntary and at your own risk.

Morupa employees do not moderate any of its services, or your communications, transmissions or use of these services. We do not undertake any responsibility for any content contained therein, or for any breaches of your right to privacy that you may experience as a result of accessing such spaces.

Spam and Unsolicited bulk mail

Spam and unsolicited bulk mail are highly problematic practices. They affect the use and enjoyment of services by others and often compromise network security.

Morupa regards all unsolicited bulk email as spam, with the following exceptions:

- Mail sent by one party to another where there is already a prior relationship between the two parties and the subject matter of the message(s) concerns that relationship;
- Mail sent by one party to another with the explicit consent of the receiving party.

In essence, Morupa believes that clients should only receive bulk mail that they have requested and/or consented to receive and/or which they would expect to receive as a result of an existing relationship.

Morupa will take swift and firm action against any user engaging in any of the following unacceptable practices:

- Sending unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail.
- Using any part of Morupa’s infrastructure for the purpose of unsolicited bulk mail, whether sending, receiving, bouncing, or facilitating such mail.
- Operating or maintaining mailing lists without the express permission of all recipients listed. In particular, Morupa does not permit the sending of "opt-out" mail, where the recipient must opt out of receiving mail which they did not request. For all lists, the sender must maintaining meaningful records of when and how each recipient requested mail.
- Failing to promptly remove from lists invalid or undeliverable addresses or addresses of unwilling recipients or a recipient who has indicated s/he wishes to be removed from such list.
- Using Morupa's service to collect responses from unsolicited email sent from accounts on other Internet hosts or e-mail services, that violate this AUP or the AUP of any other Internet service provider. Advertising any facility on Morupa’s infrastructure in unsolicited bulk mail (e.g. a web site advertised in spam).
- Including Morupa's name in the header or by listing an IP address that belongs to Morupa in any unsolicited email whether sent through Morupa's network or not.
- Failure to secure a client's mail server against public relay as a protection to themselves and the broader Internet community. Public relay occurs when a mail server is accessed by a third party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mail-server. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed. Morupa reserves the right to examine users' mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. Morupa also reserves the right to examine the mail servers of any users using Morupa's mail servers for "smarthosting" (when the user relays its mail via a Morupa mail server to a mail server of its own or vice versa) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in strict accordance with Morupa's Privacy Policy and the laws of South Africa.

Users outside of South Africa

Where any user resides outside of the Republic, permanently or temporarily, such user will be subject to the laws of the country in which s/he is currently resident and which apply. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, Morupa will assist foreign law enforcement agencies (LEAs) in the investigation and prosecution of a crime committed using Morupa's resources, including the provisioning of all personal identifiable data.

Spam/Virus Filtering

Morupa provides a spam and virus filtering system to protect clients from unsolicited mail and viruses. The client acknowledges that this system might incorrectly identify a valid message as spam or as a virus and consequently this message might not be delivered to the client. The client acknowledges and agrees that Morupa shall without limitation have no responsibility for, or liability in respect of any data lost as a result of this system Morupa reserves the right to examine incoming or outgoing mail to the extent necessary to determine if it is classified as spam or malicious.

Webmail

Webmail and other web-based email services made available by Morupa are provided on an "as is" basis without representations, warranties or conditions of any kind, and the client acknowledges and agrees that Morupa shall have no responsibility for, or liability in respect of, any aspect of the webmail services, including without limitation for any lost or damaged data or any acts or omissions of Morupa. As webmail storage space is limited, some webmail messages may not be processed due to space constraints or message limitations.

Webmail is provided to individuals and for personal use only. Any unauthorised commercial use of the webmail service or resale of the webmail service is expressly prohibited.

Shared Hosting

Morupa offers unlimited bandwidth (web traffic) usage on Shared Hosting platforms. However, this is subject to reasonable and responsible usage, as determined at Morupa's discretion. Shared Hosting is designed for serving personal hosting requirements or that of small enterprises, and not medium to large enterprises. Morupa reserves the right to move clients deemed to have excessive bandwidth usage to a Cloud product which will better suit their requirements. Clients will be given notice as such, and will be informed of any cost implications.

Disk Space on Shared Hosting may only be used for Website Content, Emails and related System Files. General data storage, archiving or file sharing of documents, files or media not directly related to the website content is strictly prohibited. Unauthorised storage or distribution of copyrighted materials is prohibited, via FTP hosts or any other means.

Morupa will implement security updates, software patches and other updates or upgrades from time to time, to maintain the best performance, at their sole discretion. Morupa is under no obligation to effect such upgrades, or to rectify any impact such changes could potentially have to Shared Hosting clients.

Morupa will not be liable or responsible for the backing up, restoration or loss of data under any circumstances. Clients are solely responsible for ensuring their data is regularly backed up and for restoring such backups in the event of data loss or corruption.

Morupa prohibits clients from doing the following on hosting platforms administered by Morupa:

- Running applications that are not production-ready. Any applications on the hosting platform must be optimized with respect to memory usage and must have appropriate data indexing.
- Running applications with inadequate security controls.
- Generating significant side-channel traffic from an application, whether by design or otherwise. Databases should be stored locally, and remote content should be cached.
- Storing or generating useless content, including comment spam, unused cache files, log file and database entries.
- Storing malicious content, such as malware or links to malware.
- Monopolizing server resources, including CPU time, memory, network and disk bandwidth.

- Maintaining long-running processes and long-running database queries.
- Storing or running back-door shells, mass mailing scripts, proxy servers, web spiders, phishing content, or peer-to-peer software.
- Sending bulk mail of any form, particularly mail that cannot be efficiently delivered due to volume or incorrect addresses.
- Using poor passwords.
- Sharing security credentials with untrusted parties.

Protection of Minors

Morupa prohibits clients from using Morupa's service to harm or attempt to harm a minor, including, but not limited to, by hosting, possessing, disseminating, distributing or transmitting material that is unlawful, including child pornography.

Morupa prohibits clients from using Morupa’s service to host sexually explicit or pornographic material of any nature.

Privacy and Confidentiality

Morupa respects the privacy and confidentiality of our clients and users of our service. Please review our Privacy Policy which details how we collect and use personal information gathered in the course of operating this service.

User Responsibilities

Clients are responsible for any misuse of Morupa's services that occurs through the client's account. It is the client's responsibility to ensure that unauthorised persons do not gain access to or misuse Morupa's service.

Morupa urges clients not to reply to unsolicited mail or "spam", not to click on any suggested links provided in the unsolicited mail. Doing so remains the sole responsibility of the client and Morupa cannot be held liable for the Client being placed on any bulk mailing lists as a result.

Where the client has authorised a minor to use any of the Morupa's services or access its websites, you accept that as the parent/legal guardian of that minor, you are fully responsible for: the online conduct of such minor; controlling the minor's access to and use of any services or websites; and the consequences of any misuse by the minor, including but not limited to transactions entered into by the minor using such access.

It is also your responsibility to ensure that you are aware, stay aware of, and shall at all times comply with, all statutory or other regulatory provisions and rules applicable to the provision and use of the Morupa Internet service as amended from time to time, including but not limited to the provisions of the Electronic Communications and Transactions Act 25 of 2002, the Films and Publications Act 65 of 1996 and the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

Complaints procedure

Complaints relating to the violation of this AUP should be submitted in writing to abuse@morupa.co.za.. Complaints must be substantiated, and unambiguously state the nature of the problem, and its connection to our network and services.

Action following breach of the AUP

Upon receipt of a complaint, or having become aware of an incident, Morupa may, in its sole and reasonably-exercised discretion take any of the following steps:

- In the case of a network, inform the user's network administrator of the incident and request the network administrator or network owner to address the incident in terms of this AUP and the ISPA Code of Conduct (if applicable);
- In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means;
- In the case of individual users, warn the user; suspend the user's account and/or revoke or cancel the user's network access privileges completely;
- In all cases, charge the offending parties for administrative costs as well as for machine and human time lost due to the incident;
- Assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP;
- Institute civil or criminal proceedings;
- Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies.

Any one or more of the steps listed above, insofar as they are deemed necessary by Morupa, may be taken by Morupa against the offending party.

To help ensure that all clients have fair and equal use of the service and to protect the integrity of the network, Morupa reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof. Such steps include but are not limited to:

- Limiting throughput (on specifc protocols or services or entirely);
- Preventing or limiting service through specific ports or communication protocols; and/or
- Complete termination of service to clients who grossly abuse the network through improper or excessive usage.

This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

Online activity will be subject to the available bandwidth, data storage and other limitations of the service provided, which Morupa may, from time to time, revise at its own discretion and without prior notice to the client.

Capped Data Accounts

As a Capped client you are completely unshaped no matter what you are doing, and no matter what the time of day or night it is. This means that we will not slow down your connection speed (by either shaping or throttling) no matter what you download or connect to. Your speed will be as fast as contracted line speed allows for every kind of traffic (Actual speed is dependent on line speed, distance from the exchange, quality of the cabling on your premises, weather conditions and current capacity of the destination servers).

Uncapped Data Accounts

This Policy will try to explain as clearly as possible what you can expect from your Uncapped Morupa data account. We want our Uncapped Internet experience to be the best it can be, subject to our Fair Usage Policy. In order to do this we manage our network by prioritising the different kinds of traffic used.

There are two main types of traffic that you can use when connected to the Internet:

1. Instant, Realtime traffic protocols such as: Web browsing (HTTPS); Live Streaming (YouTube); Secure browsing (HTTPS); VOIP; Email; Terminal services (SSH)
2. Non-Realtime Downloading protocols such as: HTTP Downloads (downloading a file from your browser), Torrents (BitTorrent), News servers (NNTP)

In order to ensure that everybody has the best experience possible, we will manage our network by prioritising the types of traffic to make sure that our clients' Internet experience is as fast as it can be - no matter the time of the day or the utilisation of our network. We will seldom throttle nor shape the Realtime services at any time of the day or night Your speed will be as fast as your agreed line speed allows for Realtime traffic (Actual speed is dependent on line speed, distance from the exchange, quality of the cabling at your premises, weather conditions and current capacity of the destination).

To make this possible, we will shape non-Realtime services during our busiest times. Non-real time services will be shaped on a sliding scale, with our higher bandwidth users getting shaped more than lower bandwidth users, only on these services (NEVER on real time services). This will ensure that our network is not congested and that all of our clients' experience is not negatively affected.

If left completely unchecked Torrents and non-Realtime downloads would use most of the network capacity, which makes the use of all other types of traffic very slow, unstable and unpleasant for all clients. We need to manage the non-realtime downloads of our higher bandwidth users so that everyone (including them) can have a great Realtime Internet experience.

What does this practically mean?

This means that on an Uncapped account will get the fastest Realtime Internet experience that your line can handle for 24 hours a day. For our high bandwidth users users, non-Realtime Internet traffic (such as torrents) will be dynamically shaped during peak network usage so that congestion can be prevented and a good overall quality of service can be guaranteed. During non-peak usage, everyone (even the highest bandwidth users) will get as close to full speeds on ALL types of traffic (Realtime and non-Realtime) as the network will allow.

Morupa's Uncapped Fair Usage Policy

Morupa's uncapped accounts are designed for either home or business use, and customers need to select the appropriate package designed for their access port speed and type of usage application (for example, for business or home use).

Morupa's uncapped products are not capped in the ordinary course. However, Morupa reserves the right to apply restrictions on an uncapped account if a customer’s behaviouris determined to be affecting the user experience of other customers on Morupa’s network. Such restrictions may include but are not limited to throttling a customer’s throughput speeds to an appropriate proportion of the actual port speed and / or shaping a customer’s bandwidth to limit the use of bandwidth intensive protocols and applications.

Examples of customer behaviour which may compromise Morupa’s network performance include, for example, causing network congestion, include running excessive concurrent internet sessions or accessing excessive bandwidth intensive protocols such as peer-to-peer.

In the event of such behaviours, Morupa reserves the right to terminate the account of a customer whose usage is continuously affecting Morupa’s network performance, as a customer of Morupa'suncapped products.

In order to assist a customer to be made aware of when his or her behaviour is compromising Morupa's network performance,

Morupa will provide to the customer such information as is practically available regarding the customer's usage status by way of a usage tracker tool. A customer will be able to track when his or her usage is dangerously high. Once usage is indicated as being dangerously high, Morupa reserves the right to suspend the relevant customer's usage within 24 (twenty four) hours of usage having reached such levels. Customers who are restricted by Morupa in the aforementioned manner in a calendar month will be returned to full service profile at the beginning of the next month.

The above controls will be implemented by Morupa in addition to those set out elsewhere in this AUP regarding unlawful behaviour.

In general, peak times on our network are between 08h00 and 0h00 every day. This means that non-Realtime services will be shaped on a sliding scale, with higher bandwidth users getting shaped more than lower bandwidth users, and the higher bandwidth users will not get full speeds during these times for non-Realtime services (Realtime services will continue at full speeds).

Generally, after midnight and before 08h00 each day, non-Realtime traffic will be less shaped (or not at all) and you will get the fastest speed your Telkom line (and the network) allows.

What determines who will be shaped (or who is a high bandwidth user)?

Our system looks at a variety of factors, such as bandwidth consumption patterns and historical usage, to determine which users are grouped together. The system does this dynamically, so there is no set guideline to determine how you will be grouped or shaped, as it is determined by the network capacity at that point in time. The network management system determines how to optimise the available network capacity to benefit all clients and give the best possible overall internet experience.

Are there ways around QoS so I can download more?

The QoS is an important feature which protects the integrity of the network and ensures that all clients get the best experience. We strongly discourage (and take active measures to prevent) clients from using means which bypass or override our network management. This constitutes abuse of our network, and will be dealt with as such.

How much can you move each month?

This will depend on your Internet usage habits. All Realtime usage will not be throttled or shaped. Non-Realtime usage may be shaped during peak hours. Uncapped users can expect shaping to take place once 60GB download threshold has been reached in a calendar month.

Reservation and Non Waiver of Rights

Morupa reserves the right to amend or alter this policy at any time, and without notice to you.

Morupa reserves the right to take action against any individuals, companies or organisations that violate any of the prohibited activities set out herein, or engage in any illegal or unlawful activity while accessing our services, to the fullest extent of the law.

Morupa reserves the right, at its sole discretion, to act against other types of abuse not listed in this document and to investigate or prevent illegal activities being committed over our network.

Morupa reserves the right to monitor user and network traffic for site security purposes and prevent any unauthorised attempts to tamper with our site or cause damage to our property.

Morupa does not undertake to guarantee the security of any data passing through its networks.

Morupa will provide a "best effort" service, including regular updates on computer viruses and other threats to security of data, it is the responsibility of the communicating parties to safeguard their data, and Morupa cannot be held liable for any loss or damage arising as result of the failure to do so.

Morupa does not waive its right to enforcement of this AUP at any time, or prejudice its right to take subsequent action, should Morupa fail, neglect or elect not to enforce a breach of the AUP at any time.

Morupa Marketing & Communications (Pty) Ltd

August 2013

Email : accounts@morupa.co.za

Fax : 086-586-0079