ACCEPTABLE USE POLICY
JUNE 2019

nexus.net
wired and wireless

OVERVIEW

NEXUS.NET strive to ensure all clients get a good, fast and reliable Internet service at all times. We provide plenty of redundancy and surplus bandwidth to meet our client's needs. That said, we have to implement some acceptable usage policies (AUPs) to ensure that the few clients, who may abuse their connection, do not impact on the performance of the overall network.

NEXUS.NET classify our packages, both fibre and wireless, into 4 categories, BRONZE, SILVER, GOLD and PLATINUM. BRONZE packages can have some protocols (torrents, heavy downloads) shaped and restricted in busy peak periods, no shaping applies to SILVER, GOLD and PLATINUM packages.

BRONZE, SILVER and GOLD Uncapped packages have the below AUPs applied:

AUP - BRONZE UNCAPPED

Our BRONZE packages are aimed at home users. These packages offer great value, have 1:4 contention ratio and next business day support. These packages are truly uncapped, and will never be blocked, but may be subject to the AUP. It must be noted that there is a daily download quota on these packages, implemented from 7am each morning, Monday to Friday. If traffic reaches either of 2 quota levels, speed is reduced on the line by 40 and 60% respectively. At midnight, speed is restored to normal. Traffic midnight to 7am is not counted towards this quota. To avoid your line being slowed by the AUP, preferably setup big downloads for late in the evening.

DAILY QUOTA LIMITS	USAGE	SPEED REDUCTION	USAGE	SPEED REDUCTION
Uncapped 2mb	5 gigs	40%	8 gigs	60%
Uncapped 4mb	8 gigs	40%	12 gigs	60%
Uncapped 6mb	10 gigs	40%	15 gigs	60%
Uncapped 8mb	12 gigs	40%	18 gigs	60%
Uncapped 10mb	15 gigs	40%	20 gigs	60%
Uncapped 15mb	20 gigs	40%	25 gigs	60%
Uncapped 20mb	30 gigs	40%	35 gigs	60%
Uncapped 40mb	40 gigs	40%	45 gigs	60%
Uncapped 50mb	50 gigs	40%	60 gigs	60%
Uncapped 100mb	70 gigs	40%	90 gigs	60%

AUP - SILVER & GOLD UNCAPPED

Suitable for larger homes with heavy usage, as well as for small and medium size businesses. These packages offer great value, have 1:2 contention ratio and next business day support. They are truly uncapped, and will never be blocked, but may be subject to the AUP. It must be noted that there is a daily download quota on these packages, implemented from 7am each morning, Monday to Friday. If traffic reaches either of 2 quota levels, speed is reduced on the line by 40 and 60% respectively. At midnight, speed is restored to normal. Traffic midnight to 7am is not counted towards this quota. To avoid your line being slowed by the AUP, preferably setup big downloads for late in the evening.

DAILY QUOTA LIMITS	USAGE	SPEED REDUCTION	USAGE	SPEED REDUCTION
Uncapped 4Mb	20 gigs	40%	30 gigs	60%
Uncapped 6Mb	25 gigs	40%	35 gigs	60%
Uncapped 8Mb	30 gigs	40%	40 gigs	60%
Uncapped 10Mb	35 gigs	40%	45 gigs	60%
Uncapped 15Mb	40 gigs	40%	50 gigs	60%
Uncapped 20Mb	45 gigs	40%	55 gigs	60%
Uncapped 40Mb	55 gigs	40%	65 gigs	60%
Uncapped 50mb	70 gigs	40%	80 gigs	60%
Uncapped 100mb	90 gigs	40%	100 gigs	60%

1. Introduction

1.1 Nexus.Net is committed to business practices in compliance with legislation and acceptable industry standards.

1.2 The purpose of this Acceptable Use Policy ("this policy") is to inform all users of the Nexus.Net services on what Nexus.Net regards as acceptable use and to protect Nexus.Net against any unacceptable customer behavior and to ensure that all users of Nexus.Net's services can access the services without concerns of abusive behavior by fellow customers.

1.3 By making use of any of the Nexus.Net services or by visiting the website, you agree to be bound by the terms of this policy.

2. Application

2.1 This policy applies to services provided by Nexus.Net to customers and includes but is not limited to all services where access to the internet is provided or where the internet or wireless networks are required to provide the service.

2.2 The policy will apply to Nexus.Net customers, resellers and the customers of resellers or any one accessing the Nexus.Net website ('users').

2.3 The policy will apply in conjunction with any other agreement entered into between the parties.

3. Use of the Nexus.Net network and services

3.1 The user may only use the Nexus.Net network and services in compliance with all applicable legislation and this policy and in a manner that would not interfere with the Nexus.Net system or network or the systems of networks of other service providers.

3.2 The applicable legislation includes but is not limited to the following:

- 3.2.1 Electronic Communications and Transactions Act 25 of 2002;
- 3.2.2 Electronic Communications Act 36 of 2005;
- 3.2.3 Films and Publications Act 65 of 1996 (as amended);
- 3.2.4 Regulation of Interception and Provision of Communication-related Information Act 70 of 2003

3.3 The user must use the network and service in accordance with the Guidelines of Use specified in clause 4.

3.4 The user may not:

- 3.4.1 use the network or service for any criminal or unlawful conduct or anything that would amount to a contravention of the law;
- 3.4.2 distribute any material in violation of this policy or any laws, including but not limited to copyright laws;
- 3.4.3 use the network for service for automated operations;
- 3.4.4 use the network for distributing spam or email abuse which will include but not be limited to the following:
  - 3.4.4.1 unsolicited bulk mail messages ("junk mail" or "spam") of any kind;
  - 3.4.4.2 sending multiple unsolicited mail messages to one or more recipients;
  - 3.4.4.3 forwarding or propagating chain letters or petitions of any kind;
  - 3.4.4.4 sending emails to addresses where you have received an opt-out;
  - 3.4.4.5 public relay - accessing and using another mail server to deliver mails, without the authority or consent of the owner of that mail-server.

3.5. obtain, use or distribute any material which in the sole opinion of Nexus.Net amounts to any of the following:

- 3.5.5.1 Hate speech or discrimination based on one of the grounds listed in the Constitution;
- 3.5.5.2 Pornography , sexually explicit material, material of a violent nature;
- 3.5.5.3 Material that violates any person's right to privacy.

3.6 Nexus.Net's infrastructure may be used to link into other networks and the user agrees to conform to the acceptable use policies of these networks.

4. Restrictions on Use

4.1 Users may not use the services in a way to result in excessive data transfer.

4.2 Excessive data transfer includes but is not limited to the following:

- 4.2.1 Downloading in our sole opinion large files or large quantities for files, including movies, MP3's, games and software;
- 4.2.2 On-Line gaming;
- 4.2.3 Mail/ news groups/ Chat - Email, Newsgroups and Chat clients used to communicate online;
- 4.2.4 Browser Use - Automated copying of website content which results in high data transfer.

4.3 The user acknowledges that Nexus.Net as ISP makes use of third party service providers to provide email services. Users are bound by the third party's terms which include the following:

- 4.3.1 Users are bound by the SAIX acceptable usage policy (AUP) located at: http://www.saix.net/accept.html;

4.3.2 Users can only send to a maximum of 25 recipients per mail message, this includes To:, Cc: and Bcc:;

4.3.3 The size limitation is 40mb per message sent or received;

4.3.4 The sender and recipient domains must be a Fully Qualified Domain Name and be a valid resolvable DNS domain;

4.3.5 No sender From: addresses from free mail services, i.e. Yahoo and Hotmail, are accepted;

4.3.6 Testing for open relays on the SAIX ADSL user IP?s, 41.240.0.0/13, 165.145.0.0/16 and 165.146.0.0/16, and blocking access to these abusers;

4.3.7 Manual process of blacklisting domains and sender addresses when mail from a particular ?From:? address exceeds 10 000 mails in 24 hours;

4.3.8 Rate limiting incoming mail from client connections: Limit to 400 or less messages per hour, this will give an IP total of 9600 messages in 24 hours. This limit counts all the recipient addresses as a message, thus a message with 25 recipients will count as 25 messages;

4.3.9 Limit the total message volume to 250 Mega Bytes per hour;

4.3.10 When one of the limits is exceeded block the offending IP for the remainder of the hour. Blacklisting and block IP's identifying themselves as one of the local SMTP relay hosts. Blacklist IP's sending mail to known spam traps for a minimum of 1 hour.

4.4 DDOS (Distributed Denial of Service) attacks emanating from a client's router, where such router is not supplied and manageable by NEXUS.NET will result in immediate suspension of service, without notice. No warning will be given in the case of a DDOS attack. Service will be suspended immediately and no refund for remainder of client contract will be allowed.

5. Nexus.Net's rights

5.1 Nexus.Net may examine users' mail servers to ensure that their server is not a public relay and will make the results available to the user.

5.2 Nexus.Net also reserves the right to examine the mail servers of any users using Nexus.Net's mail servers for "smart hosting", content filtering or similar services at any time to ensure that the servers are properly secured against public relay. Nexus.Net may take any required steps as determined in Nexus.Net's sole discretion to protect the system and network and prevent excessive use.

5.3 Nexus.Net's rights in terms of this policy will apply to both intended and unintended prohibited use, such as viruses, worms and malicious codes.

5.4 Nexus.Net may limit online activity subject to the available bandwidth, data storage and other limitations of the access service, which Nexus.Net may, from time to time, revise at its own discretion and without prior notice to the customer. The user acknowledges that this may have the temporary effect of degrading the service.

5.5 NEXUS.NET reserve the right to suspend services to clients who contravene any of the clauses in 4 above, without warning or notice.

6. Monitoring

6.1 Nexus.Net may intercept and monitor communications in compliance with the provisions of the Regulation of Interception and Provision of Communication-related Information Act 70 of 2003 ('RICA').

6.2 The user agrees to the monitoring of all activities for purposes of determining compliance with this policy. It is recorded that Nexus.Net is not under any obligation to monitor but may monitor in its discretion and when requested.

7. Data

7.1 Nexus.Net does not have the obligation to monitor data passing over the network and internet, including but not limited to any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure.

7.2 Nexus.Net will not be responsible for the data being transmitted through the network. Users will be solely liable and responsible for all content and material used, hosted, posted, uploaded, downloaded, transmitted, created or accessed using the Nexus.Net services.

8. Security

8.1 Users must ensure that they maintain the security of their systems and hardware used in the service.

8.2 Users must also actively assist to prevent violation of this policy by taking security pre-cautions.

8.3 Security violations will include but not be limited to:

8.3.1 circumventing user authentication or security of any host, device, network, or account (referred to as "cracking" or "hacking");

8.3.2 interfering with service to any user, host, device, or network (referred to as "denial of service attacks");

8.3.3 using the services, devices, network or account for any illegal purpose, including phishing;

8.3.4 accessing the data, network or system without authority, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorization of Nexus.Net;

8.3.5 monitoring data traffic on the network or system without express authorization from Nexus.Net;

8.3.6 interfering with the service to any user, device, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

8.3.7 forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

8.4 Violations of system or network security by the user are prohibited, and may result in civil or criminal liability. Nexus.Net will investigate incidents involving such violations and will involve and co-operate with law enforcement officials if a criminal violation is suspected.

8.5 DDOS (Distributed Denial of Service) attacks emanating from a client's router, where such router is not supplied and manageable by NEXUS.NET will result in immediate suspension of service, without notice. No warning will be given in the case of a DDOS attack. Service will be suspended immediately and no refund for remainder of client contract will be allowed.

9. Enforcement

9.1 Any violation of this policy will be regarded as a material breach of contract.

9.2 Where reasonably possible, Nexus.Net will use best efforts to inform a user of any breach.

9.3 For breach of this policy, Nexus.Net may on its own initiative or if it receives any complaint, take any of the following action in addition to any other rights in law:

9.3.1 inform the user's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this policy;

9.3.2 suspend the user's account and withdraw the user's access to the network;

9.3.3 suspend access of the user's entire network until abuse can be prevented by other means;

9.3.4 take any action as may be necessary to protect the integrity of the system, including, but not being limited to, system monitoring, as well as protocol management and shutting down of ports affected by viruses, worms or other malicious code;

9.3.5 implement appropriate technical mechanisms in order to prevent usage patterns that violate this AUP.

9.3.6 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;

9.3.7 terminate all agreements with the user with immediate effect; investigating suspected violations of this policy,

9.3.8 taking action to recover costs and expenses incurred in identifying and resolving abuse.

10. Reporting and regulation

10.1 All cases of violation or where violation seems imminent should be reported to support@nexus.net.co.za.

10.2 This policy will be regulated by the laws of South Africa.

10.3 Any users outside the borders of the Republic of South Africa will also be bound by the applicable laws from the jurisdiction from which they are accessing the service to the extent possible to interpret both jurisdictions' legislation, failing with the laws of South Africa will apply.