**connec telecoms**
21 North Street
Derby 0347
South Africa
0100 210 777
www.connec.co.za

# Acceptable Use Policy

This policy forms part of the agreement between the client and connec telecoms and is binding on clients using connec telecoms services. The AUP sets out in detail what forms of conduct connec telecoms regards as unacceptable on the part of its clients and the steps which connec telecoms may take in response to unacceptable use of its services. Please take the time to acquaint yourself fully with the provisions of this policy.

## 1. General

1.1 By contracting with connec telecoms for services, the client agrees, 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 the client relating to the services.

1.2 The purpose of this AUP is to:
1.2.1 Ensure compliance with the relevant laws of the Republic.
1.2.2 Specify to clients and users of connec telecoms services what activities and online behaviour are considered an unacceptable use of the service.
1.2.3 Protect the integrity of connec telecoms network
1.2.4 Specify the consequences that may flow from undertaking such prohibited activities.

1.3 This document contains several legal obligations which the client will be presumed to be familiar with, as such, connec telecoms encourages the client to read this document thoroughly and direct any queries to admin@connec.co.za.

1.4 connec telecoms respects the rights of connec telecoms clients and users of connec telecoms services to freedom of speech and expression, access to information, privacy, human dignity, religion, belief and opinion.

## 2. Unacceptable Use

2.1 connec telecoms services may only be used for lawful purposes and activities. connec telecoms prohibits any use of its services including the transmission, storage and distribution of any material or content using connec telecoms network that violates any law or regulation of the Republic Of South Africa. This includes, but is not limited to:
2.1.1 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.
2.1.2 Any activity designed to defame, abuse, stalk, harass or physically threaten any individual in the Republic of South Africa or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.
2.1.3 Any violation of Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets.

2.1.4 Any violation of another's right to privacy, including any effort to collect personal data of third parties without their consent.

2.1.5 Any fraudulent activity whatsoever, including dubious financial practices, such as pyramid schemes; the impersonation of another client without their consent; or any attempt to enter into a transaction with connec telecoms on behalf of another client without their consent.

2.1.6 Any violation of the exchange control laws of the Republic of South Africa.

2.1.7 Any activity that results in the sale, transmission or distribution of pirated or illegal software.

## 3. Threats to Network Security

3.1 Any activity which threatens the functioning, security and/or integrity of connec telecoms network is unacceptable. This includes:

3.1.1 Any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by connec telecoms for this goal.

3.1.2 Any effort to use connec telecoms equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking").

3.1.3 Forging of any TCP/IP packet headers (spoofing) or any part of the headers of an email or a newsgroup posting.

3.1.4 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.

3.1.5 Any activity which threatens to disrupt the service offered by connec telecoms through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of others' networks.

3.1.6 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.

3.1.7 Any unauthorised monitoring of data or traffic on the network without connec telecoms explicit, written consent.

3.1.8 Running services and applications with known vulnerabilities and weaknesses, e.g. insufficient anti-automation attacks, any traffic amplification attacks, including recursive DNS attacks, SMTP relay attacks.

3.1.9 Failing to respond adequately to a denial of service attack (DOS / DDOS).

## 4. Uncapped Services

4.1 To ensure the quality and availability of our Internet services, connec telecoms has implemented systems to ensure fair use on all uncapped Internet products. connec telecoms at its own discretion, makes use of bandwidth shaping and/or throttling to slow down Internet speeds where a client’s behaviour is determined to be excessive or is affecting the experience of other clients on connec telecoms network.

4.2 During peak network traffic times, connec telecoms may also block bandwidth intensive protocols such as peer-to-peer or network news transfer to ensure the user experience of other clients on connec telecoms network is not effected.

4.3 In the event of abusive client behaviour being detected, connec telecoms reserves the right to immediately suspend the account of a client whose usage is affecting connec telecoms network.

4.4 If found that the same client continuously effects the experience of other clients on the connec telecoms network or continues to bypass warnings or systems put in place by connec telecoms to stop abusive behaviour, then connec telecoms reserves the right to immediately terminate the account of that client and the client agrees to pay all applicable fees that may be due on termination (normal cancellation fees will apply if the client abuses the link).

4.5 connec telecoms reserve the right to establish policies, rules and limitations, from time to time, concerning the use of any service. The client must comply with any bandwidth or other limitations connec telecoms may impose, in connec telecoms reasonable discretion. Failure to comply with these rules may result in the client's service being restricted, suspended or terminated, at connec telecoms reasonable discretion.

**5. Contention**

5.1 Network capacity and performance is subject to contention for services from users. This means that a significant rise in demand can affect the availability of bandwidth to users. connec telecoms manages contention through the implementation of Quality of Service and Throttling (on applicable products). Contention is a function of demand from users and is not strictly within connec telecoms direct control, however connec telecoms will use the provisions of the AUP and Terms and Conditions to manage contention and minimise the impact to performance to offer the best possible experience at all times.

**6. Spam and Unsolicited Bulk Mail**

6.1 connec telecoms regards all unsolicited bulk email (whether commercial in nature or not) as spam, with the following exceptions:

6.1.1 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;

6.1.2 Mail sent by one party to another with the explicit consent of the receiving party.

6.1.3 Clients should only receive bulk mail that they have requested and/or consented to receive and/or which they would expect to receive because of an existing relationship.

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

6.2.1 Sending unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail.

6.2.2 Using any part of connec telecoms infrastructure for unsolicited bulk mail, whether sending, receiving, bouncing, or facilitating such mail.

6.2.3 Operating or maintaining mailing lists without the express permission of all recipients listed. connec telecoms 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 maintain meaningful records of when and how each recipient requested mail. connec telecoms will also monitor clients deemed to be operating "cleaning lists", which is using illegally obtained email addresses but removing addresses as complaints arise. Should connec telecoms, at its discretion, believe that this is the case, it will be treated as SPAM.

6.2.4 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, or failing to provide the recipient with a facility to opt-out.

6.2.5 Using connec telecoms 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 connec telecoms infrastructure in unsolicited bulk mail (e.g. a website advertised in spam).

6.2.6 Including connec telecoms name in the header or by listing an IP address that belongs to connec telecoms in any unsolicited email whether sent through connec telecoms network or not.

6.2.7 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. connec telecoms 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. connec telecoms also reserves the right to examine the mail servers of any users using connec telecoms mail servers for "smarthosting" (when the user relays its mail via an connec telecoms 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 connec telecoms Privacy Policy and the laws of The Republic Of South Africa.

**7. Users Outside of South Africa**

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

**8. Hosting**

8.1 connec telecoms offers unlimited bandwidth (web traffic) usage on Shared Hosting platforms. However, this is subject to reasonable and responsible usage, as determined at connec telecoms discretion. Shared Hosting is designed for serving personal hosting requirements or that of small enterprises, and not medium to large enterprises. connec telecoms 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.

8.2 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.

8.3 For Shared Hosting and Managed Dedicated Solutions, connec telecoms will implement security updates, software patches and other updates or upgrades from time to time, to maintain the best performance, at their sole discretion. These upgrades include, but are not limited to, PHP, MySQL and CPanel release versions. connec telecoms is under no obligation to effect such upgrades, or to rectify any impact such changes could potentially have to Hosting Clients.

8.4 connec telecoms 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.

8.5 connec telecoms prohibits clients from doing the following on hosting platforms administered by connec telecoms:

8.5.1 Running applications that are not production-ready. Any applications on the hosting platform must be optimised with respect to memory usage and must have appropriate data indexing.
8.5.2 Running applications with inadequate security controls.
8.5.3 Generating significant side-channel traffic from an application, whether by design or otherwise. Databases should be stored locally, and remote content should be cached.
8.5.4 Failure to maintain proper “housekeeping” on a shared server including storing or generating useless content, including comment spam, unused cache files, log file and database entries.
8.5.5 Storing malicious content, such as malware or links to malware.
8.5.6 Monopolising server resources, including CPU time, memory, network and disk bandwidth.
8.5.7 Maintaining long-running processes and long-running database queries.
8.5.8 Storing or running back-door shells, mass mailing scripts, proxy servers, web spiders, phishing content, or peer-to-peer software.
8.5.9 Sending bulk mail of any form, particularly mail that cannot be efficiently delivered due to volume or incorrect addresses.
8.5.10 Using poor passwords.
8.5.11 Sharing security credentials with untrusted parties.
8.5.12 Running Torrents for download or Seed Servers.
8.5.13 Running TOR (or other Online Anonymity Services).
8.5.14 Otherwise circumventing the Acceptable Use Policy or intended use of the product.
8.5.15 The mining of cryptographic currencies on our Physical and Virtual hosting platforms. This causes considerable strain on our hosting resources outside of reasonable limits and is therefore prohibited.

**9. Protection of Minors**

9.1 connec telecoms prohibits clients from using connec telecoms 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 and cyber bullying.

9.2 connec telecoms prohibits clients from using connec telecoms service to host sexually explicit or pornographic material of any nature.

**10. Privacy and Confidentiality**

10.1 connec telecoms respects the privacy and confidentiality of connec telecoms clients and users of connec telecoms service.

10.2 When you send us personally identifying information in an e-mail, we use the information you provide only to help us gather the information you might request. In an effort to respond to your request, information you submit may be viewed by various people within connec telecoms. Once received, the information to your email is protected in accordance with law, (e.g. the Privacy Act and the Freedom of Information Act).

**11. User Responsibilities**

11.1 Clients are responsible for any misuse of connec telecoms 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 connec telecoms service.

11.2 connec telecoms 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 connec telecoms cannot be held liable for the client being placed on any bulk mailing lists as a result.

11.3 Where the client has authorised a minor to use any of the connec telecoms services or access its websites, the client accepts that as the parent/legal guardian of that minor, the client is 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.

**12. Complaints Procedure**

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

**13. Action Following Breach of the AUP**

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

13.1.1 In the case of clients, warn the client, suspend the client account and/or revoke or cancel the client's service access privileges completely;

13.1.2 In the case of an abuse emanating from a third party, inform the third party's network administrator of the incident and request the network administrator or network owner to address the incident in terms of this AUP and/or the ISPA Code of Conduct (if applicable).

13.1.3 In severe cases suspend access of the third party's entire network until abuse can be prevented by appropriate means.

13.1.4 In all cases, charge the offending parties for administrative costs as well as for machine and human time lost due to the incident.

13.1.5 Assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP.

13.1.6 Institute civil or criminal proceedings.

13.1.7 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; and/or

13.1.8 suspend or terminate the service as provided for in the Agreement.

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

**14. Reservation and Non-Waiver of Rights**

14.1 connec telecoms reserves the right to amend or alter this policy at any time, and without notice to the client.

14.2 connec telecoms reserves the right to take action against any individuals, companies or organisations that violate the AUP, or engage in any illegal or unlawful activity while accessing connec telecoms services, to the fullest extent of the law.

14.3 connec telecoms 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 connec telecoms network.

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