daraco™
I.T. SERVICES

Acceptable Usage Policy

Last Update: 23rd January 2011

The Daraco Services Broadband (‘provider’) Acceptable Use Policy is set out below. Please read it carefully.

If you use any service ('service') of the ‘provider’, you must comply with the Acceptable Use Policy. If you fail to comply, the ‘provider’ may suspend or terminate your use of the ‘service’.

The Acceptable Use Policy is designed to ensure that your use of the ‘service’ does not break any laws or interfere with the right of other users of the ‘provider’ which also to use the ‘service’.

The ‘provider’ may change this Policy from time to time. You must check the Policy regularly to ensure that you are aware of your obligations. See the details at the end of this document.

1. Acceptable Use

You must not use the ‘service’ in a manner which interferes with the rights of other users or which breaches Internet netiquette.

Examples of things you must not do:

a. monitor data or traffic on any network or system if you do not have the authorisation of the owner of the network or system to do so;

b. forge any TCP-IP packet header, any part of the header information or an email source address in an email or newsgroup posting;

c. provide false user information to the ‘provider’ or other users;

d. send ANY amount of unsolicited or unwanted email to any destination – also known as SPAM or UCE (Unsolicited Commercial Email). This is now covered under new Australian Laws;

e. gain access to a person's private information (or attempt to do so);

f. disobey the rules of any newsgroup, forum, email mailing list or other similar group; or

g. post the same or similar messages to more than one USENET newsgroups (including by excessive cross-posting or multiple-posting, also known as 'SPAM').

2. Unauthorised Access

You must not use the ‘service’ to obtain unauthorised access to any computer, system or network.
If you do not have authorisation, you must not:

a. access or use any data, systems or networks;

b. probe, scan or test the vulnerability of a system or network;

c. breach any security or authentication measures for a system or network; or

d. Attempt to gain access to the account of any other user or system or network.

Unlawfully accessing or damaging data in a computer is not only a breach of the Acceptable Use Policy - it is also a criminal offence punishable by fine, imprisonment or both according to the Commonwealth Crimes Act section 76 and possibly other State and Federal Acts.
You must not use the ‘service’ in a manner which may interfere with the technical operation of the ‘service’ or any other computer, system or network
You must not attempt to interfere with the regular workings of the ‘providers’ systems or network connections or the ‘provider’ or its upstreams or any other network. The ‘provider’ may override any attempt by you to specify a particular traffic routing pattern.
You must not impair the ability of other people to use the ‘providers’ systems or the Internet or any other connected networks.
You must not use the ‘service’ as a staging ground to disable or interfere with other systems; for example DoS/DDoS attacks, Port Scans, etc.
You must not use IRC (or other ‘chat’ networks) bots or clone-bots on the ‘service’. An IRC bot is a program that runs and is connected to an IRC server 24 hours a day, automatically performing certain actions.

3. Legal Material

In using the ‘service’, you must not break any laws or infringe the rights of other persons.
For example, you must not:

a. distribute or make available any abusive, obscene, defamatory or pornographic material;

b. distribute or make available any material which would be classified R or X (or refused classification) by the Classification Board or Banned under the laws of the Commonwealth of Australia or any state or territory of Australia; or

c. Copy or attempt to copy any material if you do not have the owner's permission to do so.

4. Detection/Co-operation

To detect and deal with breaches of the Acceptable Use Policy, the ‘provider’ may take the following actions:

a. The ‘provider’ will co-operate with other service providers to control unacceptable user behaviour.

b. The ‘provider’ will co-operate with the Police (state or federal), other law enforcement or Intelligence Agencies of the states or Commonwealth of Australia, by providing the details and related data (i.e. log files) of users who are suspected of breaking any laws of the states or Commonwealth of Australia.

c. The ‘provider’ will co-operate with any court order requiring information about the activities or the service details.

The ‘provider’ may implement technical mechanisms to prevent behaviour which breaches this Policy (for example, which block multiple postings before they are forwarded to their intended recipients, access to Peer-to-Peer networks or websites or network addresses deemed to hold illegal content).

The ‘provider’ may exercise any rights it has under its contract with the customer whose account is being used in breach of this Policy. Such rights include the right to suspend or terminate the customer's use of the ‘service’.

The ‘provider’ may take any other action it deems appropriate, including taking action against offenders to recover the costs and expenses of identifying them.

5. Usage of ‘Flat Rate’ services on Residential Grade DSL services

The Flat Rate services of the ‘provider’ are not to be considered ‘Unlimited’ services.

The ‘provider’ does not charge excess data for the ‘fair use’ of Flat Rate services.

‘Fair Use’ is defined as the ordinary use of a broadband service. Ordinary use does not include the downloading of illegal or infringing materials.

As a guideline, the ‘fair use’ download levels would be exceeded in a rolling 1 month period if downloads were in greater than the following levels:

256/64k 25 Gigabytes
512k/128k 35 Gigabytes
1.5M/256k+ 60 Gigabytes
24/1M (ADSL2+) 80 Gigabytes

Based on our analysis of our current user base, these levels far exceed to typical usage of the size services quoted.

Should a user exceed the above values, it does not mean that the service will be disconnected or suspended. What it does mean thought, is that the ‘provider’ reserves the right to throttle (slow down) the service after this point. At this point in time (23 January 2012), no throttling policy exists, but should there be consistent extreme usage beyond the levels defined, we reserve the right to institute such a policy.

6. Usage of 'Flat Rate' services on Business Grade Broadband Services

The Flat Rate services of the 'provider' are not to be considered 'Unlimited' services.

The 'provider' does not charge excess data for the 'fair use' of Flat Rate business services.

Broadband includes Standard DSL, Premium DSL, Fibre, x.163, Co-locations and other Meet-Me Services.

256/64k 25 Gigabytes

512k/128k 35 Gigabytes

1500k/256k 60 Gigabytes

2M/{384k/640k} 80 Gigabytes

4M/640k 80 Gigabytes

6M/640k 100 Gigabytes

512k/512k 40 Gigabytes

1M/1M 60 Gigabytes

1.5M/1.5M 60 Gigabytes

2M/2M 80 Gigabytes

3M/4M 85 Gigabytes

4M/4M 90 Gigabytes

10M/10M 200 Gigabytes

For the purpose of measuring upstream traffic on flat-rate services, uploaded data is measured separately and uses the same values above.

7. IP Address Allocation

An IP Address is a number(s) that identify a connection to the internet.

a. Residential grade services are assigned a dynamic IP address upon successful authentication. This means that an IP address from an allocated pool is assigned to the customer upon login and that IP address will change from time to time as set by the system.

   1. Customers with Static IP Addresses are exempt from the above

   2. Business Grade services, who always have Static IP Addresses, are exempt from the above

b. Residential Grade services are required to re-connect/re-authenticate to the 'providers' network every 24 hour period (from initial logon). This provides consistency and accuracy for usage and accounting purposes.

c. Premium/Business DSL and fibre services are exempt from the above

8. Blocked Servers/Services

There are internet 'servers' or 'services' which are considered not appropriate to be hosted on Residential Grade services of the 'provider'.

a. Anything that may be defined as a 'server'; examples are as follows:

1. Web Server (Port 80)
2. Mail Server (Port 25, 110, 143)
3. Game Servers (Various Ports)
4. Any FTP Server (20,21)
5. DNS Servers (53)
6. P2P Server (Various Ports)
7. IRC (or other Chat) servers (Various Ports)

Services specifically exempt are:

1. Non-Business VPN
2. Remote Control (i.e. Remote Administrator, PC Anywhere, Terminal Services, Laplink, VNC, etc.)

b. Business grade services must not operate the following services without written permission of the 'provider'

1. DNS Server (53)
2. Anonymous FTP Servers (20,21)
3. "Open Relay" Mail Servers (25)

The 'provider' reserves the right to 'block' these or any other like services from operating on the 'providers' network by utilising access-lists, firewall, filtering or other bandwidth control technologies.

9. Open Relay Mail Servers

We define an “Open Relay” mail server as an SMTP mail server that allows third-parties to send emails to other third-parties. Third-partied are those people/services that are not authorised to use an end-customers mail server.

One use of an Open Relay server is that they are used to send spam/viruses to many people (perhaps hundreds of thousands). Open Relay servers cause significant stress on the ‘providers’ network and are not allowed under any circumstances.

Business customers who choose to operate their own mail servers are responsible for the orderly administration of those servers. They must be configured not to be able to be used for ‘open relaying’. If you need assistance, please contact the ‘provider’.

Any customer, who operates an Open Relay mail server, whether purposefully or accidentally, will be liable for costs incurred by the provider in dealing with the situation.

10. This Document

This document is a living document and will be added to from time to time. This document will be available of the ‘providers’ website, located at http://www.daraco.com.au/policies/aup

Date: 23rd January 2012
Version: 1.2