BCP 1 ISSUE 2: **Blocking and filtering of Internet traffic**

A Best Common Practice (BCP) document is a non mandatory recommendation representing what ISPA believes is best practice at the time of writing. Prescriptive language including words like 'should' and 'would' refer to members who are trying to comply with the BCP. Mandatory requirements are set out in the ISPA Code of Practice.

1. Definitions.

In this Best Common Practice Document:

(1) "filtering traffic" means materially blocking, filtering, modifying the content of, degrading the quality of, diverting the traffic to a different destination, or otherwise altering the information in Internet traffic passing through its systems.

(2) “bandwidth caps” means a limit or allowance on the amount of traffic a customer can pass over their connection before certain other restrictions may be applied, usually measured over a specified period of time. The limit may cover all traffic types or may only be applied to a subset of traffic.

(2) For the avoidance of doubt, "Internet traffic" includes all communications carried over IP, including but not limited to HTTP, email, VoIP, "instant messaging", and "peer-to-peer".

2. Prohibitions.

(1) An ISPA Member must not deliberately filter Internet traffic unless it makes available to its customers and users in a clear manner the nature of the filtering that takes place. The information provided must identify the form of filtering and the general criteria used to filter but need not provide a complete set of details, particularly where they are subject to change.

(2) An ISPA Member must not deliberately operate bandwidth caps unless it makes available to its customers and users in a clear manner the nature of the caps that apply. The information provided must identify the general criteria used to calculate the customers bandwidth, but need not provide a complete set of details, particularly where they are subject to change. Where the filtering and/or bandwidth caps vary by customer package or otherwise, this should be indicated clearly.

3. Example.

The following example shows the level of detail to be expected:

On all our services:

- We block access to the IP addresses that host those web sites which IWF informs us publish child abuse images that are illegal to possess.
- We filter incoming email using the "Eulerian filter service" from SpammersMustDie.com, and discard any email that meets its criteria.
- We block traffic to and from UDP ports 2048 to 32767 on our links to the rest of the Internet, but not between our customers.
- We give all other ICMP and UDP traffic a lower priority than TCP and SCTP, so such packets are more likely to be dropped, but do not select them based on content or port number.
- Connections to TCP port 25 (SMTP), no matter what the destination address, are diverted to our own mail servers.

BCP 1 ISSUE 2: **Blocking and filtering of Internet traffic**

On our "Basic" service:

- We give you a monthly bandwidth allowance of 40GB (40,000,000,000 bytes). This allowance is a measure of all data (including packet headers) sent to your system in the calendar month, but excludes data sent by your system.

On our “Enhanced” service:

We do not operate bandwidth caps, but you are advised to note our Fair Use Policy

4. Exclusions

This Best Common Practice Document does not apply to:

(1) Routine and automated annotation of traffic (for example, the addition of Received header lines to email).

(2) Accidental filtering and normal packet loss due to line quality.

(3) Filtering or modification of service quality due to contention on contended links or connection failure due to server load.

(4) Temporary filtering to stop or mitigate faults or attacks (e.g. "bogon storms" or denial of service attacks).

(5) Action against customers whose traffic are deemed to be in breach of the ISP’s Terms and Conditions or Fair Use Policy.