



Telstra Wholesale Acceptable Use Policy

Commercial in Confidence

Issue Number 1, 12 July 2006

Acceptable Use Policy

The following is the Telstra Wholesale Acceptable Use Policy (Telstra AUP) for users of the Telstra Network. Telstra may modify this Telstra AUP at any time in its sole and absolute discretion.

Changes and modifications will be effective when posted on the Telstra website and any use of the Telstra Network after the posting of any changes will be considered acceptance of those changes.

Important Note: Telstra is serious about working towards eliminating spam from travelling through its network, whether originating from the Customer, end users or otherwise and ensuring that the use of the Telstra Network complies with all applicable laws. If Telstra, in its complete discretion, considers that this Telstra Wholesale AUP has been violated in any way whatsoever, Telstra reserves the right to take all legal and technical steps available under the Customer's agreement with Telstra which incorporates this Telstra Wholesale AUP including suspending or disconnecting the Customer's services.

1. Use only for lawful purposes

The Telstra network, including the network of any service provider from whom Telstra acquires a Service for the purpose of resale, and including the web sites operated by Telstra (collectively, the Telstra Network), may be used only for lawful purposes. Users may not use the Telstra Network in order to transmit, distribute or store material:

- a) in violation of any applicable law;
- b) in a manner that will infringe the copyright, trade mark, trade secret or other intellectual property rights of others or the privacy, publicity or other personal rights of others; or
- c) that is obscene, threatening, abusive or hateful or contains a virus, worm, Trojan horse, or other harmful component.

2. No SPAM

It is a prohibited use of the Telstra Network to accept, transmit or distribute unsolicited bulk data (which includes, without limitation, e-mail, bulletin boards, newsgroups, software, files). The only circumstances in which the Telstra Network may be used to send unsolicited data of an advertising or promotional nature is where the unsolicited data is sent to persons with whom the sender has a pre-existing business, professional or personal relationship or to persons who have previously indicated their consent to receive data from the sender from time to time, for example by ticking a box to that effect on the sender's web site. Unless these requirements are met, users must not send unsolicited bulk data on the Telstra Network. If these requirements are met, the user must also provide an unsubscribe function on their web site (and make this function known to recipients in the relevant data) which allows those recipients to elect to be removed from that mailing list.

3. Other Prohibited Uses

The following activities are also prohibited uses of the Telstra Network:

- (a) Sending data, or causing data to be sent, to or through the Telstra Network that hides or obscures the source of the data, that contains invalid or forged headers or domain names or deceptive addressing;
- (b) Receiving or collecting responses from bulk unsolicited data whether the original was sent via the Telstra Network or not or hosting a web site to which recipients of bulk unsolicited data are directed;
- (c) Relaying data from a third party's mail server without permission or which employs similar techniques to hide or obscure the source of the data;
- (d) Collecting or harvesting screen names or e-mail addresses of others for the purpose of sending unsolicited e-mails or for exchange;
- (e) Sending large or numerous amounts of data for the purpose of disrupting another's computer or account;
- (f) Sending data that may damage or affect the performance of the recipient's computer;
- (g) Persistently sending data without reasonable cause or for the purpose of causing annoyance, inconvenience or needless anxiety to any persons;
- (h) Sending mass postings of messages to post advertisements other than in newsgroups that specifically encourage or permit advertising; and
- (i) Sending post binary files other than in newsgroups that specifically encourage or permit such postings.

4. System and Network Security

Users are prohibited from violating or attempting to violate the security of the Telstra Network, including, without limitation:

- (a) accessing material not intended for such user or logging into a server or account which such user is not authorised to access;
- (b) attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorisation;
- (c) attempting to interfere with, disrupt or disable service to any user, host or network, including, without limitation, via means of overloading, "flooding", "mail bombing" or "crashing";
- (d) forging any TCP/IP packet header or any part of the header information in any e-mail or newsgroup posting; and
- (e) taking any action in order to obtain services to which such user is not entitled. Violations of system or network security may result in civil or criminal liability. Telstra will investigate occurrences which may involve such violations and may involve, and cooperate with, law enforcement authorities in prosecuting users who are involved in such violations.

5. Viruses, Worms, Trojans and Denial of Service Attacks

As you should be aware, it is important to protect your computer and any connected networks against higher level computer programs (such as viruses, worms, Trojans and other malicious programs) and lower level Denial of Service (DoS) attacks that can be distributed or propagated via the Internet, including electronic mail. It is the Customer's responsibility to ensure that the Customer has in place appropriate protection for the Customer's systems and to prevent circulation of such computer programs and attacks from the Customer's computer of networks through the Telstra Network. Such protection methods may include firewalls, an appropriate policy regarding email attachments and the most up to date virus scanning software.

6. Suspension or Termination.

Any user which Telstra determines, in its sole discretion, to have violated any element of this Telstra AUP will receive a written warning, and may be subject at Telstra's discretion to a temporary suspension of service pending such user's agreement in writing to refrain from any further violations; provided, however, that if Telstra deems it necessary, in Telstra's sole discretion, Telstra may immediately suspend or terminate such user's service without issuing such a warning. Users which Telstra determines to have committed a second violation of any element of this Telstra Wholesale AUP will be subject to immediate suspension or termination of service without further notice and Telstra may take such further action as it solely determines to be appropriate under the circumstances to eliminate or preclude such violation, and Telstra will not be liable for any damages of any nature suffered by any Customer, user, or any third party resulting in whole or in part from Telstra's exercise of its rights under these policies. If required by applicable law Telstra may suspend or terminate a service immediately and without notice.

7. Monitoring

Telstra has no obligation to monitor the Telstra Network, but reserves the right to do so, including as required by applicable law, and remove any material in its sole discretion. Telstra takes no responsibility for any material input by others and not posted to the Telstra Network by Telstra.

Telstra is not responsible for the content of any other web sites linked to the Telstra Network; links are provided as Internet navigation tools only.

8. Site blocking

Telstra may block access to global Internet sites or the global Internet where required to do so by Applicable Law.