Background

FireNet's Acceptable Use Policy (AUP) also known as FireNet's Fair Usage Policy (FUP) is designed to provide a clear understanding of the rules, regulations, and restrictions regarding the use of FireNet services.

By using our services, you agree to abide by these AUPs and any changes or modifications to this policy that may occur in the future.

Violations of any AUP is strictly prohibited and may result in the immediate termination or suspension of the service you receive from FireNet. Termination or suspension may occur without notice to customer if deemed necessary by FireNet management.

Customer Security Responsibilities

The customer is solely responsible for all breaches to security affecting any servers / systems under customer control. If a customer's server is involved in an attack on another server or system, it will be shut down and an immediate investigation will be launched to determine the cause/source of the attack. In such event, the customer is responsible for the cost to rectify any damage done to the customer's server and any other requirement affected by the security breach.

System And Network Security Violations of system or network security are prohibited and may result in criminal and civil liability. FireNet may investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

Unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.

High-risk services, which are services which tend to attract denial of service attacks, are strictly prohibited. This includes, but is not limited to, IRC related services and selling of shell accounts.

Violators of the policy are responsible, without limitations, for the cost of labour to clean up and correct any damage done to the operation of the network and business operations supported by the network, and to respond to complaints incurred by FireNet. Such labour is categorized as emergency security breach recovery and is currently charged at $500 AUD per hour required. Enquiries regarding security matters may be directed to abuse@firenet.net.au. FireNet is concerned with the privacy of online communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, FireNet urges its customers to assume that all of their online communications are insecure. FireNet cannot take responsibility for the security of information transmitted over FireNet's facilities.

Password Protection

The customer is responsible for protecting customer's password and for any authorized or unauthorized use made of customer's password. The customer will not use or permit anyone to use FireNet's service to guess passwords or to access other systems or networks without authorization. FireNet will fully cooperate with law enforcement authorities in the detection and prosecution of illegal activity.

Contact Information

Customers are responsible for maintaining their contact information in the ticketing system such that the email address is always reachable even in the event of their FireNet servers being shut down.

Internet Etiquette

The customer is expected to be familiar with and to practice good Internet etiquette (Netiquette). The customer will comply with the rules appropriate to any network to which FireNet may provide access. The customer should not post, transmit, or permit Internet access to information the customer desires to keep confidential. The customer is not permitted to post any material that is illegal, libellous, tortuous, indecently depicts children or is likely to result in retaliation against FireNet by offended users. FireNet reserves the

right to refuse or terminate service at any time for violation of this section. This includes advertising services or sites via IRC or USENET in clear violation of the policies of the IRC channel or USENET group.

Copyright Infringement - Software Piracy Policy

The FireNet network may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of Australian or United States law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights. Making unauthorized copies of software is a violation of the law, no matter how many copies you are making. If you copy, distribute or install the software in ways that the license does not allow, you are violating federal copyright law. FireNet will cooperate fully with any civil and/or criminal litigation arising from the violation of this policy.

Network Responsibility Customers have a responsibility to use the FireNet network responsibly. This includes respecting the other customers of FireNet. FireNet reserves the right to suspend and or cancel service with any Customer who uses the FireNet network in such a way that adversely affects other FireNet customers. This includes but is not limited to:

Attacking or attempting to gain unauthorized access to servers and services that belong to FireNet or its customers (i.e. computer hacking), and/or

FireNet will react strongly to any use or attempted use of an Internet account or computer without the owner's authorization. Such attempts include, but are not limited to, "Internet Scanning" (tricking other people into releasing their passwords), password robbery, security hole scanning, port scanning, etc. Any unauthorized use of accounts or computers by a FireNet customer, whether or not the attacked account or computer belongs to FireNet, will result in severe action taken against the attacker. Possible actions include warnings, account suspension or cancellation, and civil or criminal legal action, depending on the seriousness of the attack. Any attempt to undermine or cause harm to a server, or customer, of FireNet is strictly prohibited.

Lawful Purpose

All services may be used for lawful purposes only. Transmission, storage, or presentation of any information, data or material in violation of any applicable law, regulation, or AUP is prohibited. This includes, but is not limited to:

- copyrighted material or
- material protected by trade secret and other statute or
- Dissemination of harmful or fraudulent content.

Using any FireNet service or product for the purpose of participating in any activity dealing with subject matters that are prohibited under applicable law is prohibited.

Any conduct that constitutes harassment, fraud, stalking, abuse, or a violation of federal export restriction in connection with use of FireNet services or products is prohibited. Using the FireNet network to solicit the performance of any illegal activity is also prohibited, even if the activity itself is not performed. In addition, knowingly receiving or downloading a file that cannot be legally distributed, even without the act of distribution, is prohibited.

Servers hosted within FireNet network are open to the public. You are solely responsible for your usage of the FireNet network and servers and any statement you make on servers hosted within the FireNet network may be deemed "publication" of the information entered. Acknowledging the foregoing, you specifically agree not to use our service in any manner that is illegal or libellous.

Child Pornography on the Internet

Our policy on child pornography is zero tolerance. FireNet will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for any actions over the FireNet network, and will be liable for illegal material posted by their clients.

According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in

explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years or any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years.

Adult Content on the Internet

FireNet will provide notification and will inform any customers in writing of improper materials on our servers. However, FireNet reserves the right to disconnect any customers immediately.

Commercial Advertisements with E-mail

FireNet takes a zero tolerance approach to the sending of Unsolicited Commercial E-mail (UCE) or SPAM over our network. Very simply, this This means that customers of FireNet may not use or permit others to use our network to transact in UCE. Customers of FireNet may not host, or permit hosting of, sites or information that is advertised by UCE from other networks. Violations of this policy carry severe penalties, including termination of service.

Violation of FireNet's SPAM policy may be reported to abuse@firenet.net.au

IP Address Overlap

FireNet administers the network on which customer servers reside. The customer cannot use IP addresses which were not assigned to them by FireNet staff. Any server found using IPs which was not officially assigned will be suspended from network access until such time as the IP addresses overlap can be corrected.

Suspension

FireNet reserves the right to suspend network access to any customer if, in the judgment of the FireNet network administrators, the customer's server is the source or target of the violation of any of the other terms of the AUPs or for any other reason which FireNet chooses. If inappropriate activity is detected, all accounts of the Customer in question will be deactivated until an investigation is complete. Prior notification to the Customer is not assured. In extreme cases, law enforcement will be contacting regarding the activity. The customer will not be credited for the time the customer's machines were suspended. The Customer will be credited on a prorated basis based on the monthly fees the Customer pays for the servers that are suspended for the time the Customer's machines were suspended.

Cancellation

FireNet reserves the right to cancel service at any time. If inappropriate activity is detected, all accounts of the customer in question will be deactivated until an investigation is complete. Prior notification to the Customer is not assured. In extreme cases, law enforcement will be contacting regarding the activity. All fees paid in advance of cancellation are non-refundable if FireNet institutes its right of cancellation. Any violation of policies which results in extra costs will be billed to the customer (i.e. transfer, space etc.).

Network Responsibility Customers have a responsibility to use the FireNet network responsibly. This includes respecting the other customers of FireNet. FireNet reserves the right to suspend and or cancel service with any Customer who uses the FireNet network in such a way that adversely affects other FireNet customers. This includes but is not limited to:

Upload of Data

FireNet services with no fixed upload data cap are not designed to provide sustained, high-volume access as it will compromise the Service for other users. As such, continuous uploading of data in excess of a 4:1 (uploads:downloads) ratio will be considered excessive use. If a client is found making excessive use of the Service, the client will be warned via email and if this behaviour continues, may be charged an excess usage charge, have the service speed shaped or have the service disconnected.

Unauthorised Access

FireNet customers must not use a FireNet supplied service to obtain unauthorised access to any computer, system or network. If you do not have authorisation, you must not:

- access or use any data, systems or networks
- probe, scan or test the vulnerability of a system or network
- breach any security or authentication measures for a system or network
- 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.

You must not use FireNet services in a manner which may interfere with the technical operation of the service or any other computer, system or network. FireNet may override any attempt by you to specify a particular traffic routing pattern.

You must not impair the ability of other people using FireNet's systems, the Internet, or any other connected networks. You must not use FireNet's network or systems 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 FireNet network. An IRC bot is a program that runs and is connected to an IRC server 24 hours a day, automatically performing certain actions.

Legal Material

In using FireNet services, you must not break any laws or infringe the rights of other persons.

For example, you must not:

- distribute or make available any abusive, obscene, defamatory, or pornographic material.
- 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.
- copy or attempt to copy any material if you do not have the owner's permission to do so.

Detection / Co-operation

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

- FireNet will co-operate with other service providers to control unacceptable user behaviour.
- FireNet 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.
- FireNet will co-operate with any court order requiring information about the activities or the service details.

FireNet 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).

FireNet 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 Services being used.

FireNet may take any other action it deems appropriate, including acting against offenders to recover the costs and expenses of identifying them.

Open Relay Mail Servers

FireNet defines an Open Relay mail server as a Simple Mail Transfer Protocol (SMTP) email server that allows anyone on the Internet to send messages through it while hiding or obscuring the source of the messages being sent.

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 provider networks 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 FireNet support.

Any customer, who operates an Open Relay mail server, whether purposefully or accidentally, will be liable for any costs incurred by FireNet in dealing with the situation and have their service disconnected until this violation has been resolved.

Disclaimer of Responsibility

FireNet is under no duty to look at each customer's or user's activities to determine if a violation of the AUPs has occurred, nor do we assume any responsibility through our AUPs to monitor or police Internet-related activities. FireNet disclaims any responsibility for any such inappropriate use and any liability to any person or party for any other person's or party's violation of this policy.

Please note that this policy document may change without notice, and this is up to the customer to ensure they are aware of the most up to date policy information.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUPs AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON YOUR BEHALF, SHALL BE CONSIDERED VIOLATIONS OF THESE AUPs BY YOU.