Schedule 1

ALNCOM Acceptable Usage Policy

Contents

Introduction

Alncom’s relationship with its customers, other networks, and ultimately its connectivity to the rest of the internet, require its customers to behave responsibly. Accordingly, Alncom cannot permit irresponsible behaviour by its customers, which could damage these relationships, the Alncom network or the use and enjoyment of the internet by others.

In addition to the customer’s own actions it is the customer's responsibility to ensure that their network is configured in a secure manner. A customer may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A customer may not permit their network, through action or inaction, to be configured in such a way that it gives a third party the capability to use their network in an illegal or inappropriate manner.

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

Acceptable Use

Alncom Network Equipment

You must not tamper with, reset or attempt to access Alncom network equipment.

Illegal Activities

You must not, by using the service, possess or transmit illegal material. You should be aware that as the internet is a global network, some activities/material which may be legal in the UK, may be illegal elsewhere in the world and vice versa. When you visit a website, a copy of the visited pages is stored on your pc in the web browsers' cache files. Storage of illegal material in this way may well be a criminal offence, as well as contravening this Acceptable Use Policy.

You must not, by using the service, possess or transmit material in breach of the terms of its copyright. Any of the following activities may be illegal and therefore not permitted on the Alncom Network:

- Copying and sharing images, music, movies, television shows or other copyrighted material through the use of P2P technology

- Purchasing copyrighted material and then making copies for others

- Downloading anything of which you don't legally own a copy of (software, MP3s, movies, television shows, etc.)

If you are in any doubt as to the legality of anything, before proceeding take independent legal advice.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the internet. As well as being in breach of your contract for the particular service, such hacking or attempted hacking is a criminal offence.

Forging Addresses and Spoofing

You must not; add, remove, or modify identifying network header information ("spoofing") or attempt to impersonate any person or piece of equipment by using forged headers or other identifying information.

You must not send data via the internet which has forged addresses or which is deliberately constructed to adversely affect remote machines.

You must not configure your pc as an open relay system.

Port Scanning

You must not run "port scanning" software which accesses remote machines or networks, except with the explicit prior permission of the administrator or owner of such remote machines or networks. This includes using applications capable of scanning the ports of other internet users. If you intend to run a port scanning application, you must provide Alncom with a copy of either a contract with or the written consent authorising the activity received from the target of the scan. This must be supplied to Alncom prior to the application being run.

Spam or Unsolicited Email

You must not send or allow a third party to send anonymous bulk e-mailings through either action or inaction.

If we receive any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, we may take further action to stop this happening again. This may involve the termination specific ports that are being used by the sender and may occur without notice.

In the event that we are alerted to anyone sending bulk e-mails, we will generally attempt to make contact with the senders to discuss appropriate actions but we reserve the right to suspend without notice or terminate the accounts of any clients involved in these activities.

We recommend that anybody undertaking any kind of bulk mail has a data protection statement on their Website explaining how the company fulfils their obligations in terms of the Data Protection Act.

Trolling

Alncom is committed to making the internet a safer and friendlier place for all users. Customers who engage in abusive behaviour; “Trolling” will be notified that their behaviour is unacceptable and may have their accounts suspended or terminated.

Due Diligence

We strongly recommend against, and additional care must be taken, if running an "Open Proxy Server" as this can allow other users of the internet to exploit your internet connection, and use it as if it were their own. For example, an external user could access your local network and send unsolicited e-mails that would appear to come from you.

In severe cases, including "denial of service" (DoS) attacks originating from your network, against another network host or individual user, your service may be suspended without prior notice and if repetitions occur through actions or inactions may be terminated.

What actions will Alncom Take?

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended without prior notice or terminated. Alncom may operate systems to ensure compliance with this AUP, including without limitation port scanning and testing of open servers and mail relays.

Account Restoration

A suspended account may be restored at Alncom discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by Alncom on their individual merits.

It is your responsibility to protect your local network from access or infection through adequate passwords, firewalls and antivirus. You must not allow any activities, which adversely affect the ability of other people or systems to use Alncom’s services or the internet, from a device connected to your network.

You must not use Open DNS resolvers; these can be used to amplify attacks within Alncom’s network.