Nviron Telecom Services: Acceptable Usage Policy

This Acceptable Use Policy (AUP) is intended to help protect Nviron customers, and the Internet community, from the inappropriate use of the Internet. A Customer's use of relevant Nviron services constitutes acceptance of this AUP. Nviron reserves the right to revise and update this AUP from time to time. Nviron expects Customers must cooperate with Nviron when requested to assist in its investigations.

This AUP is divided into two sections:

SECTION 1. Violations and Descriptions of Appropriate Use

SECTION 2. Reporting to Nviron's TOS/Abuse Department

SECTION 1. Violations and Descriptions of Acceptable Use

GENERAL VIOLATIONS

Our AUP prohibits the following:

IMPERSONATION/FORGERY

Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous re-mailers and nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting. Privacy Violations Attempts, whether successful or unsuccessful, to gain access to any electronic systems, networks or data, without proper consent, are prohibited. Threats of bodily harm or destruction of property are prohibited. Threatening or harassing activity is prohibited. The use of any Nviron service for illegal purposes is prohibited. The resale of any Nviron service without proper authorisation from Nviron Ltd. is prohibited.

COPYRIGHT INFRINGEMENT

All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing. Nviron will co-operate with all agencies attempting to assert their rights in these matters.

NETWORK DISRUPTIONS AND NETWORK-UNFRIENDLY ACTIVITY

Any activities, which adversely affect the ability of other people or systems to use Nviron services or the Internet, are prohibited. This includes "denial of service" (DoS) attacks against another network host or individual user.

Interference with, or disruption of, use of the network by others, network services or network equipment is prohibited.

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.

FACILITATING A VIOLATION OF THIS AUP

Advertising, transmitting, or otherwise making available any software, programme, product, or service that is designed to violate this AUP, or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to spam.

NEWS

Customers should use their best judgment when posting to any newsgroup. Many groups have charters, published guidelines, FAQs, or ‘community standards' describing what is and is not considered appropriate. Usenet can be a valuable resource if used properly. The continued posting of off-topic articles is prohibited. Commercial advertisements are off-topic in most newsgroups, especially non-commercial regional groups. The presence of such articles in a group is not indicative of the group's intended use. Customers must familiarise themselves with basic USENET netiquette before posting to a newsgroup.

Newsgroup spamming: Spam is, first and foremost, a numerical metric-posting of substantively similar articles to multiple newsgroups. This form of spam is sometimes referred to as "excessive multi-posting" (EMP). Nviron considers ‘multi-posting' to 10 or more groups within a two-week period to be excessive.

Hostile attacks or invectives (flames) aimed at a group or an individual poster are generally considered inappropriate in Nviron service groups. Flames in the non-service groups are discouraged. Many newsreaders offer filtering capabilities that will bring certain messages to a person’s attention or skip over them altogether (kill files).

Customers must not cancel messages other than their own messages. A Customer may cancel posts forged in that Customer's name. Nviron may cancel any postings that violate this AUP.

WEB

Using a Web-site address or hosted Web account provided by or on behalf of Nviron for the purpose of distributing illegal material is prohibited. Nviron will co-operate with authorities to remedy breaches of this AUP.

Using a Web-site address or hosted Web account provided by or on behalf of Nviron to collect responses from unsolicited commercial e-mail is also prohibited.

SECTION 2. Reporting to Nviron's TOS/Abuse Department

Anyone who believes that there is a violation of this AUP must direct the information to the AUP Abuse Staff at this address: abuse@nviron.co.uk

Customers who wish to report ‘spam' from a non-Nviron source should send copies of the e-mail they received along with full header information. Some messages may not receive a response, but Nviron may use the information received at this address to aid in the development of filter lists.

All issues involving other e-mail abuse originating from Nviron e-mail or network addresses should also be sent to the above address, as should:

All issues regarding USENET ‘news' abuse issues originating from Nviron customers.

Other suspicious activity such as port scans or attempts to penetrate network resources and virus distribution.

Copyright infringement:

Nviron may take any one or more of the following actions in response to complaints:

- Issue warnings: written or verbal
- Suspend the Customer's newsgroup posting privileges
- Suspend the Customer's services
- Terminate the Customer's agreement
- Invoice the customer for administrative costs and/or reactivation charges

What information should be submitted?

1. The IP address used to commit the alleged violation
2. The date and time of the alleged violation, including the time zone or offset from GMT
3. Evidence of the alleged violation
4. Copies of e-mail with full header information provide all the required information, as do syslog files and firewall logs. Other situations will require different methods.