

Acceptable Use Policy, AUP

Xdev Information Systems Ltd

This AUP is a description of types of activities that are not allowed on the Xdev Information Systems network. The Internet is still evolving, and the ways in which the Internet may be abused are also still evolving. Therefore, we may from time to time amend this AUP as set out below to further detail or describe reasonable restrictions on your use of our services. Your continued use of the services will be an acceptance of the AUP as it is changed from time to time.

We may change the AUP to reflect changes in law, regulation or accepted industry practice by posting any changes on our website at www.xdev.net to take effect 15 days from the date of posting provided that we inform you at least 15 days in advance via the online ticketing system. In the event that the change materially adversely affects your ability to use the Services, then you can terminate the Agreement by 30 days formal written notice. This AUP forms part of the terms of your Agreement with us and your Services may be suspended or terminated for breach of this AUP in accordance with the MSA. You are responsible for violations of this policy by you or anyone using your service, whether authorised by you or not. If you have any questions, please contact us at abuse@xdev.net

1. Internet Abuse

You may not use our network to engage in illegal, abusive, or irresponsible behaviour, including:

- 1.1 unauthorised access to or use of data, services, 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 authorisation of the owner of the system or network;
- 1.2 monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;
- 1.3 interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- 1.4 use of an Internet account or computer without the owner's authorisation;
- 1.5 collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
- 1.6 use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting;
- 1.7 use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- 1.8 any activity or conduct that is likely to result in retaliation against our network;

- 1.9 any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including data protection;
- 1.10 introducing intentionally or knowingly into the Service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Services;
- 1.11 is used to send unsolicited e-mails ("spam");
- 1.12 misrepresenting yourself as other computer networks and users; or
- 1.13 any activity or conduct that unreasonably interferes with our other customers' use of our services.

2. Security

- 2.1 You must take reasonable security precautions.
- 2.2 Passwords should consist of at least 8 mixed alpha and numeric characters with case variations. You should not permit a common word to be used as a password. You must protect the confidentiality of your password, and you should change your password regularly.

3. Bulk Commercial E-Mail

- 3.1 Under the European Directive 2002/58/CE of 12 July 2002 on privacy and electronic communications, the use of e-mail for direct marketing is only allowed to recipients who have given their prior consent. We acknowledge that market research is not considered as direct marketing within the meaning of the Directive above, and therefore, the requirements set out below don't apply to bulk e-mails for market research purposes. You must obtain our advance approval for any bulk commercial e-mail other than for market research purposes, for which you must be able to demonstrate the following to our reasonable satisfaction:
 - 3.1.1 Your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure;
 - 3.1.2 Your procedures for soliciting consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given;
 - 3.1.3 You retain evidence of the recipient's consent in a form that may be promptly produced within 72 hours of receipt of recipient's or our requests to produce such evidence;
 - 3.1.4 The body of the e-mail must include information about where the e-mail address was obtained, for example, "You opted in to receive this e-mail promotion from our Web site or from one of partner sites," and information on how to request evidence of the consent, for example, "If you would like to learn more about how we received your email address please contact us at abuse@yourdomain.com;

- 3.1.5 You have procedures in place that allow a recipient to revoke their consent – such as a link in the body of the e-mail, or instructions to reply with the word “Remove” in the subject line and such revocations of consent are implemented within 72 hours;
- 3.1.6 You must post an abuse@yourdomain.com e-mail address on the first page of any Web site associated with the e-mail, you must register that address at abuse.net, and you must promptly respond to messages sent to that address;
- 3.1.7 You must have a Privacy Policy posted for each domain associated with the mailing;
- 3.1.8 You have the means to track anonymous complaints;
- 3.1.9 You may not obscure the source of your e-mail in any manner. Your e-mail must include the recipients e-mail address in the body of the message or in the “TO” line of the e-mail.
- 3.2 These policies apply to messages sent using your Xdev Information Systems service or network, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site hosted via your Xdev Information Systems service. You may not use third party e-mail services that do not have similar procedures for all its customers.
- 3.3 We may test and monitor your compliance with these requirements, including requesting opt-in information from a random sample of your list at any time.

4. Unsolicited E-Mail

You may not send any unsolicited e-mail, whether commercial or non-commercial in nature, to any person who has indicated that they do not wish to receive it.

5. Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a Xdev Information Systems system or network or to breach our security or authentication measures, whether by passive or intrusive techniques without our prior written consent.

6. Newsgroup, Chat Forums, Other Networks

- 6.1 You must comply with the rules and conventions for postings to any bulletin board, chat group or other forum in which you participate, such as IRC and USENET groups including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic commercial messages, or mass postings to multiple forums.
- 6.2 You must comply with the rules of any other network you access or participate in using your our services.

7. Offensive Content

- 7.1 You may not publish, display or transmit via our network and equipment any content that we reasonably believe:

- 7.1.1 constitutes or encourages child pornography or is otherwise obscene, sexually explicit or morally repugnant;
 - 7.1.2 is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
 - 7.1.3 is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
 - 7.1.4 is defamatory or violates a person's privacy;
 - 7.1.5 creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement bodies;
 - 7.1.6 improperly exposes trade secrets or other confidential or proprietary information of another person;
 - 7.1.7 is intended to assist others in defeating technical copyright protections;
 - 7.1.8 infringes another person's trade or service mark, patent, or other property right;
 - 7.1.9 is discriminatory in any way, including by way of sex, race, or age discrimination;
 - 7.1.10 facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;
 - 7.1.11 involves theft, fraud, drug-trafficking, money laundering or terrorism;
 - 7.1.12 is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to us; and
 - 7.1.13 is otherwise malicious, fraudulent, or may result in retaliation against us by offended viewers.
- 7.2 Content "published or transmitted" via our network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting, display or transmission that relies on the Internet.

8. Export Control

The Services may not be used by persons, organisations, companies or any such other legal entity or unincorporated body, including any affiliate or group company, which violates export control laws and/or is:

- 8.1 located in Iran, Cuba, Sudan, Syria, North Korea, and Libya; and/or
- 8.2 involved with or suspected of involvement in activities or causes relating to:
 - 8.2.1 illegal gambling;
 - 8.2.2 terrorism;

8.2.3 narcotics trafficking;

8.2.4 arms trafficking or the proliferation of weapons of mass destruction; including any affiliation with others whatsoever who sponsor or support the above such activities or causes.

9. Copyrighted Material

9.1 You may not use our network or equipment to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless:

9.1.1 you have been expressly authorised by the owner of the copyright for the work to copy the work in that manner; and

9.1.2 you are otherwise permitted by copyright law to copy the work in that manner.

9.2 We will terminate the Service of copyright infringers in accordance with the MSA.

10. Cooperation with Investigations and Legal Proceedings

10.1 We may monitor any content or traffic belonging to you or to users for the purposes of ensuring that the Services are used lawfully. We may intercept or block any content or traffic belonging to you or to users where Services are being used unlawfully or not in accordance with this AUP and you do not stop or provide us with an acceptable reason within 7 days of receipt of a formal written notice from us.

10.2 We may, without notice to you:

10.2.1 report to the appropriate authorities any conduct by you that we believe violates applicable law, and

10.2.2 provide any information we have about you, or your users or your traffic and cooperate in response to a formal or informal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil action that on its face meets the requirements for such a request.

10.3 If we are legally required to permit any relevant authority to inspect your content or traffic, you agree we can provided however that where possible without breaching any legal or regulatory requirement we give you reasonable prior notice of such requirement and an opportunity to oppose and/or attempt to limit such inspection in each case to the extent reasonably practicable.

11. Other

11.1 You must have valid and current information on file with your domain name registrar for any domain hosted on our network.

11.2 You may only use IP addresses assigned to you by our staff.

11.3 You may not take any action which directly or indirectly results in any of our IP space being listed on any abuse database

12. Consequences of Violation of AUP

You are strictly responsible for the use of your Xdev Information Systems service in breach of this AUP, including use by your customers, and including unauthorised use that you could not have prevented. We will charge you our standard hourly rate for work on any breach of the AUP together with the cost of equipment and material needed to:

12.1 investigate or otherwise respond to any suspected violation of this AUP;

12.2 remedy any harm caused to us or any of our customers by the use of your service in violation of this AUP;

12.3 respond to complaints; and

12.4 have our Internet Protocol numbers removed from any "blacklist".

13. Disclaimer

We are under no duty, and by this AUP are not deemed to undertake a duty, to monitor or police our customers' activities and we disclaim any responsibility for any misuse of our network.