www.oxi.net
info@oxi.net
01865 598790

Acceptable Use Policy

Oxinet Hosted Applications and Services

Gordon Buxton
3-25-2015

The Oxinet Acceptable Use Policy has been formulated with the following goals in mind:

- to ensure security, reliability and integrity of Oxinet's systems and network, the systems and networks of Oxinet's customers and the networks and systems of others
- to avoid situations that may cause Oxinet to incur civil liability
- to maintain the image and reputation of Oxinet as a responsible provider
- to preserve the value of Internet resources as a conduit for free expression
- τo encourage the responsible use of net resources, discouraging practices which degrade the usability of network resources and thus the value of Internet services
- to preserve the privacy and security of individual users

The Acceptable Use Policy below defines the actions which Oxinet considers to be abusive, and thus, strictly prohibited. The examples named in this list are non-exclusive, and are provided solely for guidance to Oxinet customers. If you are unsure whether any contemplated use or action is permitted, please send mail to support@oxi.net and we will assist you.

Please note that the actions listed below are also not permitted from the Oxinet Ltd network or remotely to the Oxinet network from any other network.

General conduct

1. Customers are prohibited from transmitting on or through any of the Oxinet services, any material that is, in Oxinet's sole discretion, unlawful, threatening, abusive, libellous, hateful, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, national or international law.
2. Oxinet services may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of United Kingdom laws, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or any other statute. Oxinet reserves the right to remove such illegal material from its servers.
3. The customer is responsible for keeping his billing data with Oxinet up-to-date and accurate. Furnishing false data upon signup, contract, or online application, including fraudulent use of credit card numbers, is grounds for immediate termination, and may subject the offender to civil or criminal liability.
4. The resale of Oxinet products and services is not permitted, unless specifically authorized and documented in a written agreement.

System and network security

1. Customers may not attempt to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the Customer, logging into a server or account the customer is not expressly authorized to access, or probing the security of other networks (such as running a SATAN scan or similar tool).
2. Customers may not attempt to interfere with service to any user, host, or network ("denial of service attacks"). This includes, but is not limited to, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
3. Customers may not use any kind of program/script/command, or send messages of any kind, designed to interfere with a user's terminal session, via any means, locally or by the Internet.
4. Users who violate systems or network security may incur criminal or civil liability. Oxinet will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.
5. Oxinet reserves the right to monitor network traffic, run security scanning agents and test mail and web infrastructure connected to the Oxinet network for the sole purpose of ensuring system and network integrity.
6. 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

Email

1. Harassment, whether through language, frequency, or size of messages, is prohibited.
2. Customers may not send email to any person who does not wish to receive it. If a recipient asks to stop receiving email, the customer must not send that person any further email.
3. Customers are explicitly prohibited from sending unsolicited bulk mail messages ("junk mail" or "spam"). This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements, and political tracts. Such material may only be sent to those who have explicitly requested it.
4. Malicious email, including but not limited to "mailbombing" (flooding a user or site with very large or numerous pieces of email), is prohibited.
5. Forging of header information in any deceitful manner is not permitted.

6. Oxinet accounts or services may not be used to collect replies to messages sent from another Internet Service Provider, where those messages violate this Acceptable Use Policy or the Acceptable Use Policy of that other provider.

Colocation, Managed and Virtual Hosting

1. Any and all material hosted on any hosted servers, or servers co-hosted on Oxinet premises and network facilities remain the responsibility of the webmasters of those respective sites. If there are any queries regarding those sites, please get in touch with the owners and maintainers in charge.
2. Oxinet reserves the right to remove or suspend web sites, hosted servers co-hosted servers at our premises which contain material offensive or deemed unacceptable by Oxinet, ISOC, NHTCU, SOCA or Scotland Yard.
3. The virtual hosting resources allocated for CGI scripts are made available on a shared hardware platform. Oxinet reserves the right to remove any scripts deemed to solicit an unacceptable load on those resources. Also, customers should not run their own server processes (or daemons) on any managed server (e.g. database servers, chat servers, etc). For further advice on this or any other issues, please contact us at support@oxi.net
4. Oxinet reserves the right to restrict support access to the customer where it is deemed to be in excess of the supplier average support requests for similar customer contracts.
    1. Managed Hosting – 10 requests per month per server
    2. Managed+Applications – 15 requests per month per server

    In all cases relating to this matter Oxinet will first engage with the customer to discuss an appropriate re-configuration or contracting of new services being provided to match that required by the customer.

Shell accounts

1. Oxinet shell accounts are intended for interactive use. Attempts to circumvent the 'idle daemon' or time charges accounting, or attempts to run programs while not logged in by any method, are prohibited.
2. Oxinet shell accounts operate on shared resources. Customers are prohibited from excessive consumption of resources, including CPU time, memory, disk space, and session time. The use of resource-intensive programs which negatively impact other system users or the performance of Oxinet systems or networks is prohibited, and Oxinet staff may take action to limit or terminate such programs. If you have requirements to use high resource utilization programs, please contact support@oxi.net for assistance on how Oxinet can accommodate you requirement, without degradation of service.
3. Password security is the responsibility of the individual user. Good passwords should be a minimum of eight characters long, contain at least one number or symbol, and are not based on any dictionary word or common name. Customers may not share passwords or accounts with others. If you have forgotten your password or wish to have it changed, Oxinet can reassign/reset your password.

IRC (Internet Relay Chat)

1. Oxinet is not liable for the content of any communications made on IRC. Oxinet reserves the right to ban from IRC usage any user whose conduct is, in Oxinet's sole judgement, inappropriate or disruptive.
2. IRC robots ("bots" or "clones") may not be run from Oxinet shell accounts, or on the Oxinet server.
3. Customers are prohibited from using IRC scripts or programs that interfere with or deny service to other users on any server or host. Customers are also prohibited from engaging in activities which harass other users. This includes, but is not limited to, "flooding" (rapidly entering text with the intent to fill the screens of others), "flashing" (disrupting terminal emulation), "takeovers" (forcibly seizing operator privileges), attempting to send private messages to those who do not wish to see them (via "ignore"), attempting to return to a channel after being banned from it, and other disruptive behaviours. Reports of activity in violation of this policy may be sent in e-mail to support@oxi.net

Investigation

1. We have in place a procedure for handling your complaints about material stored and/or accessed via our service. If you wish to make such a complaint, please ensure that you make your complaint by email to abuse@oxi.net. If you do not use this facility we cannot guarantee that your complaint will be dealt with promptly.
2. Oxinet reserves the right to investigate suspected violations of the AUP. When we become aware of possible violations, we may initiate an investigation, which may include gathering information from the user involved and the complaining party, if any, and examination of material on our servers. Much of the AUP reflect acts that may constitute breaches of United Kingdom legislation or regulations and may in some cases carry criminal liability.
3. During an investigation, we may suspend the account involved and/or remove the material involved from our servers. Such action may include temporary or permanent removal of material from our servers, the cancellation of newsgroup postings, warnings to the user responsible, and the suspension or termination of the account responsible. We will determine what action will be taken in response to a violation on a case-by-case basis.
4. The customer acknowledges that Oxinet may be required by current or future law or regulation, including but not limited to the Regulatory of Investigatory Powers Act 2000, to access, monitor, store, take copies of, or otherwise deal with the Customer's data stored on or transmitted by the Service. Without limitation, you

expressly authorise us to use your personal data and other account information in connection with any such investigation, including by disclosing it to any third party authority that we consider has a legitimate interest in any such investigation or its outcome.

5. Oxinet reserves the right to terminate the Service with immediate effect and without further obligation or liability to the Customers as required by any law enforcement organisation, or for breaching this AUP in any way.

Disclaimer

Oxinet do not have any contractual responsibility to monitor any customer activity and we hereby disclaim any responsibility for any misuse of our network.

If you have further questions or need help with any part of your Oxinet service, please contact our technical support team on 01865 598790 or by email at support@oxi.net