Acceptable Use Policy : Pulsant Group

The Pulsant Group Acceptable Use Policy ("AUP") is as defined in the Conditions and forms part of the Contract.

It has been formulated with the following goals in mind:

- to give our customers a better understanding of what is and what is not acceptable when using Pulsant Services.
- to ensure security, reliability and integrity of Pulsant Group's systems and network, the systems and networks of Pulsant Group's customers and the networks and systems of others
- to avoid situations that may cause Pulsant Group to incur civil liability and to comply with legal requirements concerning the use and/or misuse of a public communication system as defined by the Telecommunications Act
- to maintain the image and reputation of Pulsant Group as a responsible provider
- to preserve the value of Internet resources as a conduit for free expression
- to 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 AUP below defines the actions which Pulsant Group considers to be abusive and unacceptable, and thus, strictly prohibited. The examples named in this list are non-exclusive, and are provided solely for guidance to Pulsant Group customers. If you are unsure whether any contemplated use or action is permitted, please send mail to support@pulsant.com and we will assist you.

We reserve the right to amend, modify or substitute this AUP from time to time. The continued use of the Services provided by Pulsant signifies that the Customer agrees to be bound by this AUP and by any amendments to it.

General

1. Customers are prohibited from transmitting on or through any of the Pulsant Group services, any material that is, in Pulsant Group's sole discretion, unlawful, obscene, threatening, abusive, libellous, hateful, or encourages conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any Applicable Law.
2. Pulsant Group services may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of Applicable Laws is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret or infringement of other Intellectual Property Rights of others or the privacy, publicity or personal rights of others. Pulsant Group reserves the right to remove such illegal material from its servers.
3. Customers are responsible for keeping their billing data with Pulsant Group 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. Customers are responsible for keeping their service contact data with Pulsant Group up-to-date and accurate. Any reduction in service, security threat or security breach brought about directly or indirectly from incorrect or old contact information is the responsibility of the Customer.
5. The resale of Pulsant Group products and services is not permitted, unless specifically authorised and documented in a written agreement.
6. Pulsant Group 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. In all cases relating to this matter Pulsant Group will first engage with the Customer to discuss an appropriate reconfiguration or contracting of new services being provided to match that required by the Customer.
7. Passwords in any environment should consist of at least 8 mixed alpha, numeric and special 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. If you have forgotten a password used for your Pulsant services then contact our support team.
8. Customers are responsible for violations of this AUP by anyone using their services with the Customer's permission or on an unauthorised basis as a result of the Customer's failure to use reasonable security precautions.

Messaging Systems

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. Any intended recipients must have given their consent to receive email by some affirmative means.
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. Users of mailing lists must monitor non-deliveries and cleanse their lists accordingly.
4. Malicious email of any type is prohibited.
5. Forging of header information in any deceitful manner or obscuring the source of an email is not permitted.

6. Pulsant Group accounts or services may not be used to collect replies to messages sent from another Internet Service Provider, where those messages violate this AUP or the Acceptable Use Policy of that other provider.
7. Customers must post an email address for complaints in a conspicuous place on any website associated with the email ad must promptly respond to messages sent to that address.

Systems and Applications

1. Customers may not attempt to circumvent user authentication or security of any host, or related user accounts. 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 authorised to access, probing the security of systems or running scanning tools.
2. Customers may not attempt to interfere with service to any user or host. This includes, but is not limited to deliberate attempts to overload a service, and attempts to make a host unresponsive.
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 system or application security may incur criminal or civil liability. Pulsant Group 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. Pulsant Group reserves the right to run security scanning agents and test mail and web infrastructure connected to the Pulsant Group network for the sole purpose of ensuring system integrity.
6. Customers must not attempt to probe, scan, penetrate or test the vulnerability of Pulsant Group systems and applications, or to breach or attempt to breach the Pulsant Group security or authentication measures, whether by passive or intrusive techniques without prior written agreement from Pulsant Group.
7. Customers must use best efforts to secure any device or network within the Customer's control against being used in breach of the Applicable Laws against spam and unsolicited mail, including where appropriate by the installation of anti-virus software, firewall software, and operating and application software patches and updates.

Network Security

1. Customers may not attempt to circumvent user authentication or security of network. This includes, but is not limited to, accessing data not intended for the Customer, probing the security of other networks or running scanning tools.
2. Customers may not attempt to interfere with service to any network. This includes, but is not limited to deliberate attempts to overload a service.
3. Customers must not use the Pulsant Group network to transmit, distribute or store material that contains a virus, worm, Trojan horse or other harmful component.
4. Users who violate network security may incur criminal or civil liability. Pulsant Group 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. Pulsant Group reserves the right to run security scanning agents and test mail and web infrastructure connected to the Pulsant Group network for the sole purpose of ensuring network integrity.
6. Customers must not attempt to probe, scan, penetrate or test the vulnerability of a Pulsant Group network, or to breach or attempt to breach the Pulsant Group security or authentication measures, whether by passive or intrusive techniques without prior written agreement from Pulsant.
7. Customers must use best efforts to secure any device or network within the Customer's control against being used in breach of the Applicable Laws against spam and unsolicited mail, including where appropriate by the installation of anti-virus software, firewall software, and operating and application software patches and updates.

Broadband services

1. Pulsant Group broadband (ADSL) services are intended for use to provide unlimited, moderate usage, high speed internet access for an individual, small or home office user in the case of singleADSL, and a multi-user office up to typically 15 people, with perhaps heavier usage requirements in the case of businessADSL.
2. Given the asymmetric nature of broadband ADSL services, they are not intended for the provision of hosting of applications, data or services to the wider Internet. Pulsant Group broadband is specifically aimed at the provision of Internet access. Any Pulsant Group customer wishing to run services or applications, should speak to their account manager about our application hosting, datacentre co-location, or EFM and WAN (leased line, metro ethernet or MPLS) services.
3. Use of a contended network or services (as the broadband network indeed is) relies upon reasonable usage by all subscribers to that service. If there is heavy, excessive or inappropriate usage by a small number of subscribers, then it is possible that network performance for the majority may deteriorate. As such Pulsant Group will monitor and manage traffic levels to ensure that bandwidth is being consumed in line with what is generally considered a "reasonable usage" pattern. Pulsant Group will base this upon current "best internet industry practice" and draw on the collective experience of other similar business-class service providers across the UK internet community.
4. Any broadband Customer who transfers more than contracted limit in total during a calendar month (the total of uploaded and downloaded materials) may be contacted by their account manager to discuss whether their broadband service is still appropriate for their usage requirements. Options include upgrading to a more appropriate service type or moving in an orderly fashion to another broadband provider.
5. During any discussion regarding the bandwidth usage and requirements of a broadband service, Pulsant Group reserves the right to consider rate limiting the broadband service in order to protect other users on the network from unreasonable usage patterns.

Colocation Services

1. Customers must not attempt to probe, scan, penetrate or test the vulnerability of Pulsant Group sites and physical security controls, or to breach or attempt to breach the Pulsant Group security or authentication measures, whether by passive or intrusive techniques without prior written agreement from Pulsant Group.
2. Customers must use best efforts to cable and managed collocated environments to ensure efficient cooling of the devices housed within the service racks. All new deployed cabling must comply with the Pulsant defined cabling standard.
3. Customers must not introduce or store cardboard products within the data halls.
4. Customers will remain liable for any impact or liability with regard to the continuity of services housed in collocated environments where redundant power capability is not used symmetrically between the separate power feeds where they are available.
5. Pulsant Group reserves the right to reject physical access requests to sites and services.
6. Customers are not permitted to bring auditors onto site without declaring at least two weeks in advance of the visit. Any resource required to support a Customer audit will be chargeable at standard day rates.
7. Customers must not attempt to operate or interfere with any infrastructure equipment in the data halls. Pulsant reserves the right to recover cost of any outage resulting from unauthorised operation of critical infrastructure.

Cloud and Managed Hosting Services

1. Any and all material hosted on any hosted servers, or servers co-hosted on Pulsant Group 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. Pulsant Group reserves the right to remove or suspend web sites, hosted servers and co-hosted servers at our premises which contain material offensive or are deemed unacceptable by Pulsant Group and such other organisations including ISOC, NHTCU, SOCA or Scotland Yard.
3. The virtual hosting resources allocated for CGI scripts are made available on a shared hardware platform. Pulsant Group reserves the right to remove any scripts deemed to solicit an unacceptable load on those resources. Customers must 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@pulsant.com
4. Pulsant Group 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. In all cases relating to this matter Pulsant Group will firstly engage with the Customer to discuss an appropriate reconfiguration or contracting of new services being provided to match that required by the Customer.
5. Pulsant Group 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.
6. Pulsant Group 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 Pulsant Group systems or networks is prohibited, and Pulsant Group staff may take action to limit or terminate such programs. If you have requirements to use high resource utilization programs, please contact support@pulsant.com for assistance on how Pulsant Group can accommodate your requirement, without degradation of service.
7. Customers must not attempt to book physical access for virtualised or wholly managed services. Any audit visit for a cloud or wholly managed service is chargeable at standard day rate.

AUP Breach Investigations

1. We have in place a procedure for handling 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@pulsant.com. If you do not use this facility we cannot guarantee that your complaint will be dealt with promptly.
2. Pulsant Group 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 reflects acts that may constitute breaches of Applicable Law and may in some cases carry criminal liability. It is our policy to assist police and law enforcement bodies in any practicable way when required by Applicable Law.
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 Pulsant Group may be required by current or future law or regulation 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, the Customer, 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. Pulsant Group reserves the right to suspend or terminate the Service with immediate effect and without further obligation or liability to the Customers as required by any law enforcement organisation.

Disclaimer

Pulsant Group 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 Pulsant Group service, please contact our technical support team on 0845 1199 999 or by email at support@pulsant.com