

## **DATA DOCTORS ACCEPTABLE USE POLICY**

This is Data Doctors Acceptable Use Policy. This document contains information about what type of behavior is and is not allowed on the Data Doctors Network. If you have any questions, please email us at [websupport@doc1.datadoctors.com](mailto:websupport@doc1.datadoctors.com).

### **Background**

From time to time Data Doctors may impose reasonable rules and regulations regarding the use of its services. Such rules and regulations are called Acceptable Use Policies (AUPs) and are posted on the Internet at <http://doc1.datadoctors.com/datadr/legal/>. The AUPs are not exhaustive and Data Doctors reserves the right to modify the AUPs at any time, effective upon either the posting of the modified AUPs to <http://doc1.datadoctors.com/datadr/legal/aup.html> or notification of the modified AUPs. By registering for and using the services, and thereby accepting the terms and conditions of the Services Agreement or its equivalent, you agree to abide by the AUPs as modified from time to time. Any violation of the AUPs may result in the suspension or termination of your account or such other action as Data Doctors deems appropriate. An unlisted activity may also be a violation of the AUPs if it is illegal, irresponsible, or disruptive use of the Internet. No credits will be issued for any interruption in service resulting from policy violations.

VIOLATION OF ANY AUP IS STRICTLY PROHIBITED AND MAY RESULT IN THE IMMEDIATE TERMINATION OR SUSPENSION OF THE SERVICES YOU RECEIVE FROM DATA DOCTORS. YOU SHALL REMAIN SOLELY LIABLE AND RESPONSIBLE FOR YOUR USE OF THE SERVICES AND ANY AND ALL CONTENT THAT YOU DISPLAY, UPLOAD, DOWNLOAD OR TRANSMIT THROUGH THE USE OF THE SERVICES. "CONTENT" INCLUDES, WITHOUT LIMITATION, YOUR E-MAIL, WEB PAGES, PERSONAL HOME PAGES, AND DOMAIN NAMES. IT IS DATA DOCTORS' POLICY TO TERMINATE REPEAT INFRINGERS. DATA DOCTORS RESERVES THE RIGHT TO REFUSE SERVICE TO ANYONE AT ANY TIME.

### **System And Network Security**

Violations of system or network security are prohibited, and may result in criminal and civil liability. Data Doctors may investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- Unauthorized access to or use of data, 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 authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting.

Violators of the policy are responsible, without limitations, for the cost of labor to clean up and correct any damage done to the operation of the network and business operations supported by the network, and to respond to complaints incurred by Data Doctors. Such labor is categorized as emergency security breach recovery and is currently charged at \$250 USD per hour required. Data Doctors is concerned with the privacy of online communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, Data Doctors urges its customers to assume that all of their online communications are insecure. Data Doctors cannot take responsibility for the security of information transmitted over Data Doctors' facilities.

### **Password Protection**

The customer is responsible for protecting customer's password and for any authorized or unauthorized use made of customer's password. The customer will not use or permit anyone to use Data Doctors' service to guess passwords or to access other systems or networks without authorization. Data Doctors will fully cooperate with law enforcement authorities in the detection and prosecution of illegal activity.

### **Internet Etiquette**

The customer is expected to be familiar with and to practice good Internet etiquette (Netiquette). The customer will comply with the rules appropriate to any network to which Data Doctors may provide access. The customer should not post, transmit, or permit Internet access to information the customer desires to keep confidential. The customer is not permitted to post any material that is illegal, libelous, tortuous, indecently depicts children or is likely to result in retaliation against Data Doctors by offended users. Data Doctors reserves the right to refuse or terminate service at any time for violation of

this section. This includes advertising services or sites via IRC or USENET in clear violation of the policies of the IRC channel or USENET group.

### **Copyright Infringement - Software Piracy Policy**

The Data Doctors network may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of United States or state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights.

Making unauthorized copies of software is a violation of the law, no matter how many copies you are making. If you copy, distribute or install the software in ways that the license does not allow, you are violating federal copyright law. If caught with pirated software, you or your company may be liable under both civil and criminal law, and you may be fined up to \$250,000 and/or receive up to 5 years in jail.

In compliance with the Digital Millenium Copyright Act (the "DMCA"), please send DMCA notifications of claimed copyright infringements to:  
[websupport@doc1.datadoctors.com](mailto:websupport@doc1.datadoctors.com)

Data Doctors will cooperate fully with any civil and/or criminal litigation arising from the violation of this policy.

### **Network Responsibility**

Customers have a responsibility to use the Data Doctors network responsibly. This includes respecting the other customers of Data Doctors. Data Doctors reserves the right to suspend and or cancel service with any Customer who uses the Data Doctors network in such a way that adversely affects other Data Doctors customers. This includes but is not limited to:

- Attacking or attempting to gain unauthorized access to servers and services that belong to Data Doctors or its customers (i.e. computer hacking), and/or
- Participating in behavior which result in reprisals that adversely effect the Data Doctors network or other customers' access to the Data Doctors network.

Data Doctors will react strongly to any use or attempted use of an Internet account or computer without the owner's authorization. Such attempts include, but are not limited to, "Internet Scanning" (tricking other people into releasing their passwords), password robbery, security hole scanning, port scanning, etc. Any unauthorized use of accounts or computers by a Data Doctors customer, whether or not the attacked account or computer

belongs to Data Doctors, will result in severe action taken against the attacker. Possible actions include warnings, account suspension or cancellation, and civil or criminal legal action, depending on the seriousness of the attack. Any attempt to undermine or cause harm to a server, or customer, of Data Doctors is strictly prohibited.

Violations of this policy may be reported directly to the FBI's Infrastructure Protection & Computer Intrusion Squad at <http://www.fbi.gov/programs/pcis/pcis.htm>. Data Doctors will cooperate fully with any civil and/or criminal litigation arising from the violation of this policy.

### **Lawful Purpose**

All services may be used for lawful purposes only. Transmission, storage, or presentation of any information, data or material in violation of any applicable law, regulation, or AUP is prohibited. This includes, but is not limited to: copyrighted material or material protected by trade secret and other statute or dissemination of harmful or fraudulent content.

Using any Data Doctors service or product for the purpose of participating in any activity dealing with subject matters that are prohibited under applicable law is prohibited.

Any conduct that constitutes harassment, fraud, stalking, abuse, or a violation of federal export restriction in connection with use of Data Doctors services or products is prohibited. Using the Data Doctors network to solicit the performance of any illegal activity is also prohibited, even if the activity itself is not performed. In addition, knowingly receiving or downloading a file that cannot be legally distributed, even without the act of distribution, is prohibited.

Servers hosted within Data Doctors network are open to the public. You are solely responsible for your usage of the Data Doctors network and servers and any statement you make on servers hosted within the Data Doctors network may be deemed "publication" of the information entered. Acknowledging the foregoing, you specifically agree not to use our service in any manner that is illegal or libelous.

### **Child Pornography on the Internet**

Data Doctors will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for the actions of their clients over the Data Doctors network, and will be liable for illegal material posted by their clients.

According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years or any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years.

Violations of the Child Protection Act may be reported to the U.S. Customs Agency at 1-800-BEALERT

### **Unsolicited Commercial Email/Unsolicited Bulk Email (UCE/UBE)**

Unsolicited commercial email (UCE) is defined by Data Doctors as any electronic communication (e-mail, ICQ, IRC, Instant Messenger, etc...) sent for purposes of distributing commercial information of any kind, soliciting the purchase or sale of products or services or soliciting any transfer of funds to a recipient who has not agreed to receive such communication.

Unsolicited bulk e-mail (UBE) is defined by Data Doctors as any electronic communication (e-mail, ICQ, IRC, Instant Messenger, etc...) to multiple recipients who have not agreed to receive such communication.

Use of the Data Doctors network, servers or services to transmit any unsolicited commercial or unsolicited bulk-e-mail is expressly prohibited, as is hosting web sites or services on a server which are advertised in any UCE/UBE. Data Doctors also prohibits the sending of any fraudulent, malicious, harassing, false or misleading electronic communications, including, without limitation, chain letters, pyramid schemes, or e-mails with forged headers. Posting off-topic advertisements to Usenet discussion groups, ICQ, Instant Messenger, etc., is also expressly prohibited. Additionally, Data Doctors customers are expressly prohibited from sending any UCE/UBE from our network or any email from another network that in any way references a document, image, or Web site that resides on the Data Doctors network or in one of our data centers. Violations of this type may result in the termination of the offending Data Doctors account. Our customers are ultimately responsible for any violations of the AUP by their clients, and any violation of the AUP by a client of a Data Doctors customer shall be deemed a violation of the AUP by such Data Doctors customer.

Customers whose actions directly or indirectly result in Data Doctors IP space being listed in any of the various abuse databases may be subject to having the offending domain(s), server(s), or user(s) immediately removed from our network. In addition, if Data Doctors in its sole discretion determines that a customer is in violation of our AUP, Data Doctors may, at its sole discretion, restrict, suspend or terminate a customer's account. Data Doctors will, in most cases, attempt to contact a customer prior to

suspension or termination of a server(s), but can not guarantee prior notification. Any server suspended or terminated for AUP violations will be reconnected only after the customer agrees to cease all activities that violate the Data Doctors AUP and pays all applicable reconnect fees and related charges. Any server suspended a second time for AUP violations WILL be immediately and permanently removed from our network.

Customers that Data Doctors determines in its sole discretion to be in violation of the Data Doctors AUP may be subject to additional fees or fines including, without limitation, any applicable reconnect fees.

Violation of Data Doctors' UCE/UBE policy may be reported to [abuse@doc1.datadoctors.com](mailto:abuse@doc1.datadoctors.com).

Customers seeking to send any permission-based email marketing should read Guidelines for Permission-Based Email to see our guidelines for sending this type of communication.

### **Guidelines for Permission-Based Email**

While Data Doctors prohibits the use of its systems or network to send unsolicited email (UCE/UBE) as described above, customers may send permission-based email marketing, subject to the guidelines provided herein. Permission-based marketing is defined as electronic marketing that an end user agrees to receive. This is often referred to as 'opt-in' electronic marketing. All recipient information for such marketing conducted by Data Doctors customers must be documented and cataloged by the customer. This information is to include date, time, originating IP and the location from which the email address or other recipient information was obtained. Additionally, a customer must at a minimum comply with the following guidelines, and any additional guidelines established by Data Doctors from time to time in its sole discretion, to engage in permission-based email marketing without violating the AUP:

- All commercial or bulk email originating from a Data Doctors customer on the Data Doctors network must have a working unsubscribe link. The customer must honor all requests to unsubscribe within 72 hours.
- All commercial or bulk email originating from a Data Doctors customer on the Data Doctors network must clearly list the email address to which the email was originally sent (the intended recipient's email address) in the body of the message OR in the 'TO:' line of the email.
- All Data Doctors customers sending commercial or bulk email must have a working [abuse@domain.com](mailto:abuse@domain.com) address from EVERY domain associated with the email campaign. Customers must regularly answer any messages sent to the [abuse@](mailto:abuse@) address.

- All Data Doctors customers sending commercial or bulk email must register the abuse@ address for every domain associated with commercial email they send at <http://www.abuse.net/addnew.html>.
- All Data Doctors customers sending commercial or bulk email must have a Privacy Policy/AUP posted for each domain associated with the email campaign.
- All Data Doctors customers sending commercial or bulk email must answer all complainants' requests for details regarding where the complainant "opted-in" to receive electronic marketing within 72 hours. This information must include the date, time, and the location from which the email address or other recipient information was obtained.
- All customers of Data Doctors are required to have up-to-date and valid contact information on file with their registrar for any domain hosted on the Data Doctors network.

#### Disclaimer:

- Data Doctors reserves the right to determine in its sole discretion the validity of any customer's email list. Any list Data Doctors determines in its sole discretion to be in violation of this AUP must be removed immediately or the customer will be subject to immediate suspension or termination. Repeated violations will result in permanent suspension.
- Data Doctors reserves the right to test and otherwise monitor customer's compliance with the above guidelines and requirements at any time during the customer's term of service at Data Doctors.
- If Data Doctors determines in its sole discretion that the customer is not in strict compliance with the guidelines for permission-based e-mail marketing, then Data Doctors may immediately suspend or terminate the customer's service.

#### **Billing**

The customer understands that the customer is responsible for paying for any network resources that are used to connect the customer's server to the Internet.

#### **Suspension**

If Data Doctors in its sole discretion determines that a customer's server has become the source or target of any violation concerning the Data Doctors Acceptable Use Policy (AUP), Data Doctors reserves the right to suspend network access to that server. While Data Doctors will attempt to contact the customer before suspending network access to the customer's server(s), prior notification to the customer is not assured. In certain cases, Data Doctors will contact law enforcement and other agencies regarding these activities. Customers are responsible for all charges, as well as any fees relating to the investigation,

suspension, administration and handling of their servers before, during and after the suspension period.

### **Cancellation**

Data Doctors reserves the right to cancel service at any time. If inappropriate activity is detected, all accounts of the customer in question will be deactivated until an investigation is complete. Prior notification to the Customer is not assured. In extreme cases, law enforcement will be contacted regarding the activity. All fees paid in advance of cancellation will be prorated and paid by Data Doctors if Data Doctors institutes its right of cancellation. Any violation of policies which results in extra costs will be billed to the customer (i.e. transfer, space etc.).

### **Indemnification**

Data Doctors wishes to emphasize that in signing the Services Agreement or its equivalent, customer indemnifies Data Doctors for any violation of the Services Agreement or its equivalent, law or AUP that results in loss to Data Doctors or the bringing of any claim against Data Doctors by any third-party. This means that if Data Doctors is sued because of a customer's or a customer of a customer's activity, the customer will pay any damages awarded against Data Doctors, plus costs and reasonable attorney's fees.

### **Disclaimer of Responsibility**

Data Doctors is under no duty to look at each customer's or user's activities to determine if a violation of the AUPs has occurred, nor do we assume any responsibility through our AUPs to monitor or police Internet-related activities. Data Doctors disclaims any responsibility for any such inappropriate use and any liability to any person or party for any other person's or party's violation of this policy.

All Sub-Networks, resellers and managed servers of Data Doctors must adhere to the above policies. Failure to follow any term or condition will be grounds for immediate Cancellation.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUPs AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON YOUR BEHALF, SHALL BE CONSIDERED VIOLATIONS OF THESE AUPs BY YOU.