

At Data Intensity, we value our customers and wish to provide them with a positive experience. Our goal is to offer you the ability to use and enjoy the network, applications and services provided by Data Intensity in order to enrich your business, recreational, and family life. To help Data Intensity offer you the best service possible, all customers need to follow the same rules and guidelines. These policies are intended to make Data Intensity's services available to all our customers as consistently and efficiently as possible.



This policy may be modified from time to time as broader regulations and laws are defined for public and/or private information processing systems and voice and data transmission facilities. The intent of Data Intensity's Acceptable Use Policy is to specify and define acceptable and unacceptable use of the Data Intensity network and/or computer systems and to clearly communicate Data Intensity's absolute requirement for all users of Data Intensity network and/or computer systems to comply.

While Data Intensity does not monitor your use, you are obligated to adhere to these policies. These policies are used in conjunction with the terms of service agreement. Violating any of these policies grants Data Intensity the authority to take the appropriate action to restrict or terminate your access to the Data Intensity systems and/or services.

1. Introduction

This document sets forth the principles, guidelines and requirements of the Acceptable Use Policy of Data Intensity Incorporated governing the use by the customer ("Customer") of Data Intensity's services and products ("Services and Products"). The Acceptable Use Policy has been created to promote the integrity, security, reliability and privacy of Data Intensity's vCenter facility, network, and Customer data contained within. Data Intensity retains the right to modify the Acceptable Use Policy at any time and any such modification shall be automatically effective as to all customers when adopted by Data Intensity.

Questions or comments regarding the Acceptable Use Policy should be forwarded to Data Intensity via:

-  E-mail: <mailto:sshea@dataintensity.com>
-  Telephone: 1-781-541-5913

2. Lawful Use

Customer shall not post, transmit, re-transmit or store material on or through any of Services or Products which, in the sole judgment of Data Intensity

- (i) Is in violation of any local, state, federal or non-United States law or regulation
- (ii) Threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons")
- (iii) Violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer.

Customer shall be responsible for determining what laws or regulations are applicable to its use of the Services and Products.

3. Prohibited Uses of Services and Products

In addition to the other requirements of this Acceptable Use Policy, the Customer may only use the Services and Products in a manner that, in Data Intensity's sole judgment, is consistent with the purposes of

such Services and Products. If the Customer is unsure of whether any contemplated use or action is permitted, please contact Data Intensity as provided above. By way of example, and not limitation, uses described below of the Services and Products are expressly prohibited.

3.1. General

- 3.1.1. Resale of Services and Products, without the prior written consent of Data Intensity or previous e-commerce or other SLA with the company.
- 3.1.2. Deceptive on-line marketing practices.
- 3.1.3. Violations of the rights of any Person protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer.
- 3.1.4. Actions that restrict or inhibit any Person, whether a customer of Data Intensity or otherwise, in its use or enjoyment of any of Data Intensity's Services or Products.
- 3.1.5. Falsification of any information, including sharing passwords or other methods of access with others previously not agreed upon by Data Intensity.

3.2. System and Network

- 3.2.1. Introduction of malicious programs into the network or server (e.g., viruses, trojans and worms).
- 3.2.2. Circumventing user authentication or security of any host, network or account.
- 3.2.3. Executing any form of network monitoring which will intercept data not intended for the Customer's server.
- 3.2.4. Effecting security breaches or disruptions of Internet communication. Security breaches include, but are not limited to, accessing data of which the Customer is not an intended recipient or logging into a server or account that the Customer is not expressly authorized to access. For purposes of this Section 3.2.4. "disruption" includes, but is not limited to, port scans, flood pings, packet spoofing and forged routing information.
- 3.2.5. Interfering with or denying service to any user other than the Customer's host (for example, denial of service attack).
- 3.2.6. Using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable, a user's terminal session, via any means, locally or via the Internet.
- 3.2.7. Creating an "active" full time connection on a Company-provided dial-up account for Internet access by using artificial means involving software, programming or any other method.
- 3.2.8. Utilizing a Company-provided dial-up account for purposes for Internet access other than facilitating connectivity to the Services and Products provided by Data Intensity unless expressly agreed upon. This includes copying or creating files utilizing more than 50MB of disk space on the dial-up account servers.

- 3.2.9. Failing to comply with Data Intensity's procedure relating to the activities of customers on Data Intensity's premises.

3.3. Billing

- 3.3.1. Furnishing false or incorrect data on the order form, contract or online application, including fraudulent use of credit card numbers.
- 3.3.2. Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document "use" of Data Intensity's Services and Products.

3.4. Mail

- 3.4.1. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers of the Customer or with whom the Customer does not have an existing business relationship ("E-mail spam").
- 3.4.2. Harassment, whether through language, frequency or size of messages.
- 3.4.3. Unauthorized use, or forging, of mail header information.
- 3.4.4. Solicitations of mail for any other E-mail address other than that of the poster's account or service with the intent to harass or to collect replies.
- 3.4.5. Creating or forwarding "chain letters" or other "pyramid schemes" of any type.
- 3.4.6. Use of unsolicited E-mail originating from within Data Intensity's network or networks of other Internet Service Providers on behalf of, or to advertise, any service hosted by Data Intensity, or connected via Data Intensity's network.

3.5. Usenet Newsgroups

- 3.5.1. Posting the same or similar messages to large numbers of Usenet newsgroup ("Newsgroup spam").
- 3.5.2. Posting chain letters of any type.
- 3.5.3. Posting encoded binary files to newsgroups not specifically named for that purpose.
- 3.5.4. Cancellation or superseding of posts other than your own.
- 3.5.5. Forging of header information.
- 3.5.6. Solicitations of mail for any other E-mail address other than that of the poster's account or service, with intent to harass or to collect replies.
- 3.5.7. Use of unsolicited E-mail originating from within Data Intensity's network or networks of other Internet Service Providers on behalf of, or to advertise, any service hosted by Data Intensity, or connected via Data Intensity's network.

3.6. Rules Regarding UNIX Managed Server

- 3.6.1. Customer may not create/update/delete accounts created and maintained by Data Intensity. Specifically, Data Intensity account may not be altered in any manner nor may any account with a UID of less than 1000 be altered.
- 3.6.2. Customer may not change the partitioning or mount points of any drive.
- 3.6.3. Customer may not create/update/delete any file in the /usr directory tree.
- 3.6.4. Customer may not install Microsoft© FrontPage Extensions unless updated on the /usr directory tree.
- 3.6.5. Customer may not create .rhosts or /etc/.host.equiv files.
- 3.6.6. Customer may not implement any procedure or process that would allow one to login as root without using the root password. Customer may not create suid scripts or programs.
- 3.6.7. Customer may not alter the system kernel.
- 3.6.8. Customer may not alter the /sys or /etc/system directory trees or any files contained therein.
- 3.6.9. Customer may not apply operating system and application patches to software not installed and solely maintained by the Customer, unless notification is given to Data Intensity.
- 3.6.10. Customer may not change the root shell.
- 3.6.11. Customer may not alter the contents of /.k5login.
- 3.6.12. Customer may not alter /etc/fstab or /etc/vfstab.
- 3.6.13. Customer may not share or export file systems. This includes modifying /etc/exportfs, /etc/dfs/sharetab, and /etc/netgroup.
- 3.6.14. Customer may not modify, decode or list (catalog) the contents of the root alias in the /etc/aliases file.
- 3.6.15. Customer may not change the "identity" of the system. This includes modifying /etc/hosts, /etc/hostname.*, /etc/defaultrouter, /etc/networks and /etc/ethers.
- 3.6.16. Customer may not modify the system in any manner that restricts or alters access to the system by Data Intensity's employees.
- 3.6.17. Customer may acquire root privileges after successful login of a valid non-root userid and using su to gain access as root.
- 3.6.18. Customer may create/update/delete all aspects of Customer created user accounts. This may include modifying home directory permissions, user passwords, etc.
- 3.6.19. Customer may use FTP to create/update/delete files and directories.
- 3.6.20. Customer may add to, but may not modify, existing data in the following configuration files: /etc/aliases, /etc/group, /etc/rc.local, /etc/sendmail.cf file and root crontab.
- 3.6.21. Customer may install software on the server provided the installation meets all of the criteria detailed above, and Data Intensity is notified of such installation.

3.7. Rules Regarding Windows NT Managed Server

- 3.7.1. Customer may not create/update/delete accounts created and maintained by Data Intensity. Specifically, Data Intensity's account(s) may not be altered in any manner.
- 3.7.2. Customer may not install software that does not execute as a service.
- 3.7.3. Customer may not install software that does not have a remote administration capability.
- 3.7.4. Customer may not install applications that do not run within a logon account different from that of the installing user.
- 3.7.5. Customer may not install applications that must be restarted when one user logs off and another user logs on.
- 3.7.6. Customer may not install applications that do not execute when an individual is not logged on to the server.
- 3.7.7. Customer may not modify the network and system settings of the server.
- 3.7.8. Customer may not apply operating system and application patches to software not installed and solely maintained by the Customer, unless notification is given to Data Intensity.
- 3.7.9. Customer may use FTP to create/update/delete files and directories.
- 3.7.10. Customer may create/update/delete all aspects of Customer created user accounts. This includes modifying home directory permissions, user passwords, etc.
- 3.7.11. Customer may start and stop all Windows NT 4.0 or Windows 2000 Services, including the WWW and FTP services.
- 3.7.12. Customer may install software on the server provided the installation meets all of the criteria detailed above, and Data Intensity is notified of such installation.

3.8. Website Bandwidth Abuse

Abuse of bandwidth during a Web Site Management Pilot Period will result in termination of applicable network discounts and commencement of billing based upon normal network recurring charges.

4. Exploitable or Abuse-capable Resources

Upon notification of the existence of an exploitable resource, for example, and without limitation, an open news server, an unsecured mail relay or a smurf amplifier, Customer shall immediately take all necessary steps to avoid any further abuse of such resource. Any abuse of an open resource that occurs after Customer has received such notification shall be considered a violation of this Acceptable Use Policy and enforced as such.












5. Enforcement

Data Intensity may immediately suspend and/or terminate the Customer's service for violation of any provision of the Acceptable Use Policy upon verbal or written notice, which notice may be provided by voicemail or E-mail. However, Data Intensity will make good-faith attempts to work with the Customer to

diHost Acceptable Use Policy

cure violations of this Acceptable Use Policy, and to ensure that there is no re-occurrence of violations prior to suspension and/or termination.

GLOSSARY

-  **Acceptable Use Policy:** Guidelines for services and products for Web Hosting and Internet Connectivity.
-  **Address/IP Spoofing:** Inserting forged routing information into network packet(s) such that the origin of the packet is misreported, which causes return packets to be misrouted.
-  **Binary Files:** A file containing bits or bytes that do not necessarily represent printable text. The term *binary file* usually denotes any file that is not a text file, such as executable machine language code. Special software is required to print a binary file or view it on the screen.
-  **Bulk E-mail:** Any group of messages sent via E-mail, with substantially identical content, to a large number of addresses at once. Many ISPs specify a threshold for bulk E-mail (e.g., 25 or more recipients within a 24-hour period). Taken by itself, bulk E-mail is not necessarily abuse of the electronic mail system. For example, there are legitimate mailing lists, some with hundreds or thousands of willing recipients.
-  **Commercial E-mail:** Any E-mail message sent for the purposes of distributing information about a for-profit institution, soliciting purchase of products or services, or soliciting any transfer of funds. It also includes commercial activities by not-for-profit institutions.
-  **Cracks:** Distribution of registration codes for software in violation of the software license, or distribution of any software intended to defeat copy protection.
-  **Deceptive On-Line Marketing Practices:** Marketing practices that present a false image of the advertised product (or of the advertiser). One example of a deceptive on-line marketing practice would be an E-mail that purports to originate from the recipient's ISP or from a well-known company. Other examples include fraud, multi-level marketing, or any commercial or non-commercial activity that is conducted for the purpose of confusing, misleading or misinforming the E-mail and/or Internet users.
-  **Electronic mail (E-mail) Spam:** Unsolicited E-mail from which a recipient cannot unsubscribe, or unsolicited E-mail to a recipient who does not have a previous business or other relationship with the sender.
-  **Forged Routing Information:** Routing information which is misleading or incorrect or which would tend to disguise the origin of the routed material. Usually refers to information that is not generated by any routing device (such as a mail server), but is inserted by a party using software, which is designed to produce false routing information (headers in the case of E-mail).
-  **FTP:** File Transfer Protocol. A standard way of transferring files from one computer to another on the Internet and on other TCP/IP networks. FTP is also the name of any of various computer programs that implement the file transfer protocol. Customers can also retrieve files by FTP using a web browser.
-  **MMF:** Make Money Fast Schemes: Messages that "guarantee immediate, incredible profits!," including such schemes as chain letters.

- 📖 **Mail bomb:** Delivery of enough E-mail to an electronic mailbox to overload the mailbox or potentially overload the system that the mailbox is hosted on.
- 📖 **Newsgroup Spams:** A public forum or discussion area on a computer network. All users of the network can post messages, and every user can read all messages distributed worldwide by the Usenet system, covering thousands of topics.
- 📖 **Packet Spoofing:** Emitting a network packet with a source address you do not have permission from the owner to use.
- 📖 **Ping Flood:** Intentionally flooding a system's pipeline with ICMP EchoRequests. This can reduce the bandwidth available for legitimate use and, if severe enough, can bring a pipe down.
- 📖 **Pirated:** Any copy written material, commercial or noncommercial, that is used, transmitted and/or stored without authorization.
- 📖 **Pyramid Schemes:** A get-rich scheme in which you receive a message containing a list of names. Recipients are expected to send money to the first person on the list, cross the first name off, add their name at the bottom and distribute copies of the message.
- 📖 **Smurf / Fraggle:** <http://users.quadrunner.com/chuegen/smurf.txt> - The "smurf" attack, named after its exploit program, is one of the most recent types of network-level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of which have a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer-2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet. The "smurf" attack's cousin is called "fraggle," which uses UDP echo packets in the same fashion as the ICMP echo packets. A "fraggle" is a simple re-write of "smurf."
- 📖 **System Kernel:** The central part of an operating system. In many operating systems, only the kernel can access hardware directly. (Also spelled "kernal.")
- 📖 **Unsolicited E-mail:** Unsolicited E-mail is any E-mail message received where the recipient did not specifically ask to receive it. Taken by itself, unsolicited E-mail does not constitute abuse, and not all unsolicited E-mail is undesired E-mail. For example, receiving "unsolicited" E-mail from a long-lost friend or relative is certainly not abuse.
- 📖 **Unsolicited Bulk E-mail (UBE):** E-mail with substantially identical content sent to many recipients who did not ask to receive it.
- 📖 **Unsolicited Commercial E-mail (UCE):** E-mail containing commercial information that has been sent to a recipient who did not ask to receive it.
- 📖 **Worms:** An automated computer program that probes, breaks into, interferes with or disrupts service for one or more computers, networks or services. Computer worms are similar to a computer virus, Trojan horse or other disabling device.