This Acceptable Use Policy is part of our overall effort to provide quality, reliable service to Atomic Data's customers; to protect the privacy and security of our customers, systems, and networks; to encourage responsible use of Atomic Data's and other providers' resources; and to comply with applicable laws. Atomic Data may in its sole discretion determine whether a use is a violation of this Policy. While it is not Atomic Data's intent to monitor, control, or censor communications on and over Atomic Data's facilities, when we become aware of a violation of this Policy, we may take such action as we deem appropriate to address the violation, as referenced below. This Policy applies to all customers and to all users of Atomic Data's facilities. This Policy supplements, but does not supersede, the contracts that customers have with Atomic Data; if such a contract restricts a use of Atomic Data that is not addressed in this Policy, the contract will govern with respect to such use. The Atomic Data customers, or other users, persons and organizations, who publish materials and information which are accessible through Atomic Data facilities are solely responsible for the content of such materials and information and to know and to comply with all laws applicable to the publication of such materials and information. Atomic Data does not accept responsibility for the content of the materials and information published by others that are accessible through our facilities and does not accept responsibility for the violation of any laws resulting from such publication.

Illegal/Prohibited Uses

Atomic Data facilities may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, license, or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

Security Violations

Atomic Data facilities may not be used in connection with attempts, whether or not successful, to violate the security of a network, service, or other system. Examples of prohibited activities include vulnerability scanning, monitoring, or using systems without authorization; scanning ports; conducting denial of service attacks; hacking; and distributing or propagating viruses, worms, or other harmful software. Atomic Data's customers are responsible for maintaining the basic security of their systems to prevent their use by others in a manner that violates this Policy. Examples include improperly securing a mail server so that it may be used by others to distribute spam, and improperly securing an FTP server so that it may be used by others to illegally distribute licensed software. Customers are responsible for taking corrective actions on vulnerable or exploited systems to prevent continued abuse.

Email/Spam

Sending unsolicited mail messages, including, without limitation, commercial advertising and informational announcements, is explicitly prohibited. A user shall not use another site's mail server to relay mail without the express permission of the site. Posting the same or similar message to one or more newsgroups (excessive cross--posting or multiple posting) is explicitly prohibited.

Indirect Access

A violation of this Policy by someone having only indirect access to the Atomic Data facilities through a customer or other user will be considered a violation by the customer or other user, whether or not with the knowledge or consent of the customer or other user. It is the responsibility of each Atomic Data customer to distribute, publicize, and enforce this Policy on their colocated equipment. Each customer shall provide this Policy to appropriate administrative authorities at all sites connected to theirs via connections not directly supported by Atomic Data.

Enforcement

Violations of this Policy may result in a demand for immediate removal of offending material, immediate temporary or permanent filtering, blocked access, suspension or termination of service, or other action appropriate to the violation, as determined by Atomic Data in its sole discretion. Atomic Data may involve, and will cooperate with, law enforcement if illegal or prohibited activity is suspected. Violators may also be subject to civil or criminal liability under applicable law. Refunds or credits are not issued in connection with actions taken for violations of this Policy.

Incident Reporting

Complaints regarding violations of this Policy, illegal use, system or security issues, or complaints regarding email abuse or USENET abuse or SPAM should be sent to: abuse@atomicdata.com.

Modifications

Atomic Data reserves the right to modify this policy at any time, effective upon posting of the modified Policy to this URL: atomicdata.com/aup