

Atlas World Group, Inc. Information Systems Code of Conduct

As a user of the Atlas World Group, Inc. (the "Company") Information System (the "System"), which includes its computers, e-mail, and Internet/intranet access through those computers and voice mail, I understand that:

1. **General Policy.** The System is the property of and/or is provided for the benefit of the Company and is intended to be used for the Company's business (which includes the business of its affiliated companies). I am responsible for using the System in an effective, ethical, and lawful manner that complies with this Code of Conduct.
2. **Confidentiality.** I must not disclose any Company confidential or proprietary information to anyone outside of the Company, including but not limited to personal information of customers, employees and other individuals. To protect Company property and the privacy of customers, employees and other individuals, all personal information including, but not limited to PII and SPI (both defined below) obtained by the Company, its affiliates and their agents shall be considered confidential and for the exclusive use by such parties for Company business.

Personally Identifiable Information (PII) - Information that identifies or can be used to identify, contact or locate the individual to whom such information pertains, including, but not limited to, name, address, phone number, fax number and email address. To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information or IP address is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information. Personally Identifiable Information does not include information that is collected anonymously (i.e., without identification of an individual) or demographic information not connected to an identified individual.

Sensitive Personal Information (SPI) - Consists of more private data that provides a link to an individual's identity and includes information that an individual would not want disclosed publicly, including the individual's Social Security number (or other similar unique identifier provided by a government), bank account numbers, credit card numbers (particularly when accompanied by the expiration date and card member ID) and driver's license number.

3. **Access.** The User ID assigned to me and passwords used by me provide me the capability to access and use the System. Access may be approved with restrictions that limit the sites available to me and the type of service allowed. I am responsible for protecting the System by:
 - a. Not knowingly sharing my User ID with or disclosing my passwords to another person.
 - b. Changing my password whenever I know or suspect that it has been disclosed to another person.
 - c. Not using or attempting to use any other person's User ID or passwords to obtain access to the System.
 - d. Only accessing data for which I have a specific authorization.
 - e. Reporting security violations that I observe or that otherwise come to my attention. These

are to be reported to the IT Security Officer, Director of IT Network Services or VP/CTO of Atlas World Group, Inc.

4. **Content Restrictions.** All communications and use of the System should be for the Company's business purposes. I am responsible for:
 - a. The content of all text audio or images (together referred to as "Messages") that I place on or send or forward over the System (including specifically both e-mail and the Internet/intranet).
 - b. Ensuring that my use of the System, including Messages that I send, are not for my personal gain, including soliciting non-Company business, or advancement of my individual views, for which I will use my own user name on another Internet/intranet system.
 - c. Not sending or forwarding fraudulent or obscene Messages, including Messages with abusive, profane or offensive language, or Messages that would violate the Atlas World Group, Inc. Anti-Harassment Policy prohibitions against unlawful harassment on the basis of race, national origin, religion, sex, gender, age, or disability.
 - d. Using only my own name and not any assumed name to send Messages and not obscuring the origin of any Message.
 - e. Ensuring that materials that I obtain or transmit through the System do not infringe the property rights of others, including those arising under licenses and copyrights, and are not copyrighted materials belonging to other entities, although I may download one copy of copyrighted material for my own personal use.
 - f. Any security violation traceable to my User ID.

5. **Other User Rules.** In order to ensure the use of the System efficiently and consistent with this Code of Conduct, I may or shall:
 - a. Use the System only for authorized business activities.
 - b. Use Internet/intranet relay chat channels to conduct official Company business, including obtaining technical or analytical advice.
 - c. Access databases that I am authorized to access for information as needed for business purposes and use e-mail for business contacts.
 - d. Observe all copyright and license agreements.
 - e. Abide by the generally accept rules of computer and network etiquette, including appropriate use of computer sound volume, being polite, using appropriate language and not revealing the residence addresses or phone numbers of others, with the understanding that providing my own residence address and phone number is a personal choice.

I shall not:

- f. Disrupt the operation of the Company network or the networks of other users or use the System in such a way that it disrupts its use by others, including having the sound volume too high and sending large files needlessly consuming network resources.
- g. Download any software from the Internet/intranet, with the understanding that all software downloads will be done through the MIS Department. Not allow my use of the System and, in particular, the Internet/intranet, to interfere with my productivity.
- h. Copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner.

6. **Company Rights.** All Messages, files and information, whether created, sent, received or stored on or through the System, are the property of the Company and should be considered public information. The Company reserves the right, whether or not it exercises such right, to access and monitor all Messages, files and information on the System and to disclose such Messages, files and information to persons within or without the Company, including third parties, law enforcement and government officials. The Company will monitor and record the Internet/intranet sites accessed and other services used by me and this information will be available for enforcement of this Code of Conduct and any other purpose. I acknowledge that:
 - a. I DO NOT and CANNOT have any expectation of privacy with respect to my use of the System, or any Message, file or information on the System.
 - b. I have been assigned a User ID and have passwords to limit the access of others to the System, but this does not restrict the Company from accessing any Message, file, or information on the System.
 - c. E-mail and Internet/intranet transmissions coming from or going to persons outside the Company are not guaranteed to be private. E-mail can be easily monitored and intercepted by others and can be altered en route.

6. **Entity Authorizations.** The Company may authorize limited access to the System by another entity (an "Entity User") and may elect to assign a single User ID to an Entity User, which will then have a single password to access the System. The Entity User is responsible for ensuring compliance with this policy by all individuals accessing the System using the User ID assigned to the Entity User, provided that the use and sharing of a common Entity User ID and password will not violate this policy. The Entity User is also responsible for ensuring that its User ID and password will only be made available to individuals within its organization who are authorized by it and have a need to access the information available to the Entity User through the System and for changing its password to limit such access whenever any individual with access to the User ID and password is no longer authorized to have such access. The Entity User will be responsible to the Company for any damages resulting from a breach of these provisions. Use of the System by the Entity User is an acknowledgment of acceptance of these terms.

7. **Violations.** Violations of this policy may result in disciplinary action up to and including termination and/or, with respect to non-employee users, termination of access to the system. In addition, the Company may advise appropriate legal authorities of any illegal actions.