REMOTE ACCESS PRIVACY POLICY

OVERVIEW

Increasingly, the firm's systems are being connected to external networks in an effort to gather and share information more effectively and efficiently. While the use of external networks benefits the firm, it also increases our exposure, as network connections are susceptible to eavesdropping, interception and illegal acquisition of information. Although the firm has taken steps to secure our data and information resources from unauthorized access, all users are responsible for complying with the policies set forth in this document when accessing the external networks.

The following guidelines can be found through the Weil Portal. For more information, please refer to the firm's Electronic Security Policy.

USER RESPONSIBILITIES

If you access the Weil network through one of the firm's remote access solutions, you must follow proper login and remote access security procedures to sign in. Failure to follow these procedures is in violation of the firm policy. See the Information Services page on the Weil Portal for instruction on remote access.

Access to external networks, including the Internet, is a privilege and requires users to act responsibly. Users must respect the rights of others, respect the integrity of the firm's systems and should understand that they are waiving any right of privacy in anything they create, view, send or receive via e-mail or the Internet and observe all relevant laws including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

UNACCEPTABLE USE STANDARDS

The following behaviors are examples of actions or activities that violate firm policy with respect to computer systems and their use. This list is not meant to be all inclusive, but rather to serve as an aid in determining appropriate behavior. Examples of misuse include, but are not limited, to the following:

- Accessing the firm's network through a means that does not follow the firm's remote access security procedures;
- Providing others with access to one's personal computer account(s), or gaining or attempting to gain access to the personal computer accounts, files, or electronic information of others or to accounts, files or systems to which authorized access (e.g. by secretaries, IT, etc.) has not been granted;
- Sending harassing, intimidating and/or threatening messages through electronic mail or other means;

- Intentionally intercepting, disclosing or using any electronic communication to which authorized access is not explicitly provided (including firm authorized monitoring of electronic communications). Authorized access includes mail directed to or from an individual, and those messages intended for public consumption (news groups, bulletin boards, broadcast messages);
- Accessing or distributing pornographic or degrading images or other inappropriate material located on the Internet is both unacceptable and is strictly prohibited while using firm equipment and software;
- Initiating or encouraging the promulgation of chain letters, unauthorized automated or mass postings, or other types of unauthorized large-scale distributions;
- "Hacking" or related behavior attempting to compromise firm computer security or the security of remote systems accessed through firm equipment or systems;
- Creating or releasing computer viruses or engaging in other destructive or potentially destructive programming activities.
- Copying for oneself or distributing to others commercial or other copyrighted software or proprietary data which has not been placed in the public domain or been distributed as freeware. This includes, but is not limited to, music, visual files and books or other printed material. Under no circumstances should the firm's computers or systems be used - inside or outside of the office - to connect to Internet sites that are known to allow or facilitate the unauthorized exchange of copyrighted materials (such as "Napster", "Gnuttella", etc.);
- Use of firm computers, systems and/or services to perpetrate fraud, misrepresentation or illegal activity;
- Use of firm computers, systems and/or services for commercial purposes or unauthorized financial gain;
- Use of firm computers, systems and/or services for political activities.
- Violation of any criminal laws, e.g., obscene or child pornography statutes, defamation, libel, etc.

These prohibitions are not just a matter of etiquette. When there are reasonable grounds to believe that a user is abusing computing resources, his or her computing privileges may be suspended immediately to protect the firm's computing environment. Abuse of the e-mail or Internet systems, through excessive personal use, or in violation of the law or firm policies, may result in disciplinary action, up to and including termination of employment.

BROWSING THE INTERNET - A FEW WORDS OF CAUTION

The firm's internal and external networks are intended to be used for business purposes only; use for informal or personal purposes is permissible only within reasonable limits. All Internet traffic is considered part of firm records. Additionally, as firm records, e-mail/Internet usage and traffic records are subject to disclosure to law enforcement or government official or to other third parties through subpoena or other process.

The firm has the right, but not the duty, to monitor any and all aspect of its computer system, including, but not limited to, monitoring the sites employees visit on the Internet, monitoring chat groups and news groups, reviewing materials downloaded or uploaded by employees and reviewing e-mails sent and received by employees. While the firm does not intend to regularly review individual e-mail/Internet records, the firm routinely monitors usage patterns for its e-mail/Internet communications and will proactively monitor situations where the firm has been alerted to a potential problem. The reasons for this monitoring are many, including cost analysis/allocation and the management of the firm's gateway to the Internet. The firm owns the computer and software making up the Internet access/browsing system and permits employees to use them in the performance of their duties. All information created, sent, or retrieved over the firm's Internet connection are the property of the firm. Internet records are to be treated like shared paper files, with the exception that anything in them is available for review by authorized representatives.

Downloading and/or distributing copyrighted, public domain or "freeware" software applications or operating systems to a firm computer is prohibited. Information Services reserves the right to delete any such files without notice or to reset any computer exhibiting a problem.