Medweb Telemedicine
667 Folsom Street,
San Francisco, CA 94107
Phone: 415.541.9980 Fax: 415.541.9984
www.medweb.com

Medweb Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and data transmission of clients and partners of Medweb.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Scope

In addition to named clients and partners, of Medweb this policy applies to all employees, contractors, consultants and temporary employees of such clients and partners, and other personnel affiliated with third parties. This policy applies to all equipment that is owned by Medweb or leased by Medweb, as well as software licenses provided by Medweb. The rules of this policy are in place to protect both Medweb and their clients and partners from compromise of network systems and services, and legal issues.

Network Security Guidelines

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
3. All hosts used by the employee that are connected to the Medweb Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database.
4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of any partner or client of Medweb authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Medweb owned, leased or licensed resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company 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 Medweb.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and the installation of any copyrighted software for which Medweb or their client or partner does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Using a Medweb computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any Medweb account.
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to Medweb is made.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Use of unsolicited email originating from within Medweb’s networks or of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Medweb or connected via Medweb’s 's network.
6. Any activities undertaken with the intent to harm, including:
    a. to access, upload, download, or distribute pornographic material
    b. to transmit obscene, abusive, sexually explicit, or threatening language;
    c. to violate any local, state, or federal statute;
    d. to vandalize, damage, or disable the property of another individual or organization
    e. to access another individual's materials, information, or files without permission
    f. to violate copyright or otherwise use the intellectual property of Medweb