

E-MAIL, FACSIMILE, AND INTERNET ACCESS

Future In Sight ("Organization") provides computers, E-mail, Internet, and facsimile communications equipment as essential tools to support the Organization's business. It is the responsibility of each employee to ensure that this technology is used solely for proper business purposes and in a manner that does not compromise the confidentiality of the Organization's secret, proprietary or other sensitive information. This policy applies to each and every employee of Future In Sight, and to any other person who uses the Organization's computers, E-mail, voice-mail or facsimile systems. For brevity, these will be referred to collectively as the Organization's Communications Systems.

E-mail and Voice-mail Procedures and Policies

When used below, wherever the context permits, a reference to E-mail shall be deemed to include voice-mail.

1. All E-mail correspondence in the Organization's Communications Systems is the property of the Organization, regardless of where it may have originated.
2. Employee/contractor E-mail communications are not considered private despite any such designations either by the sender or the recipient.
3. Employees/contractors should be aware that messages sent to recipients outside of the Organization, if sent over the Internet and not encrypted, are not secure. Accordingly, no Association or client confidential information should be sent over the Internet except by approved means to be determined by the President. If in doubt, ask your Supervisor.
4. Future In Sight reserves the right to monitor and examine the contents of the Organization's Communications System, including E-mail and voice mail and facsimiles, and including an employee/contractor's mailbox - at the Organization's discretion and for any purpose. Future In Sight reserves the right to disclose the contents of any such material for any purpose and to any person the Organization deems appropriate or desirable. If you wish to communicate privately, do not use the Organization Communications Systems.
5. The existence of passwords and "message delete" functions do not restrict or eliminate Future In Sight's ability or right to access electronic communications. Even deleted messages may be recovered and reviewed.

6. Employees/contractors shall not share passwords, or provide E-mail access to an unauthorized user, or access another user's E-mail box without authorization.
7. Employees/contractors who use their own equipment to connect to Future In Sight from outside the Organization's premises or from home should know that any communications that are delivered to or sent through the Organization Communications Systems may leave copies behind on the company system, are not private, and are subject to all of the terms and provisions of this policy statement.
8. Employees/contractors shall not post, display or make easily available any access information, including, but not limited to, passwords.
9. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the Organization's policies concerning equal employment opportunity and sexual and other unlawful harassment.
10. Messages sent to "All Employees/contractors" and other broadcast messages should be used sparingly, and only for the Organization and Client business.

Internet Procedures

1. Future In Sight's network, including its connection to the Internet, is to be used primarily for business and client related matters. Unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to:

I. Unauthorized entry or attempted unauthorized entry into other computer systems or areas of the Organization computer systems which you are not authorized to view;

II. Attempting to disable or compromise the security of information contained on Future In Sight computers;

III. Intentionally introducing a virus or other mischievous software onto any Organization computer;

IV. Downloading or posting of pornographic or sexually explicit material;

V. Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be

compromised at any point along the way, unless the messages are encrypted. No messages or files are to be shared with any outside individual or organization without the prior approval of the President – such arrangements with outside agencies will be developed cooperatively at the CEO level.

6. Because postings placed on the Internet may display the Organization's address, make certain before posting information on the Internet that the information reflects the standards and policies of the Organization. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the Internet except as specifically authorized by The President.

7. Subscriptions to news groups and mailing lists are permitted when the subscription is for a work-related purpose and must be approved in advance by your supervisor. Any other subscriptions are prohibited.

8. Information posted or viewed on the Internet may constitute material subject to copyright. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.

9. Unless the prior approval of management has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to the Organization's systems and information. These connections include the establishment of hosts with public modem dial-ins, World Wide Web home pages and File Transfer Protocol (FTP) servers.

10. All files downloaded from the Internet must be checked for possible computer viruses. If uncertain whether your virus-checking software is current, you must check with the President before downloading.

Any employee/contractor who violates any technology-related policy shall be subject to discipline, up to and including discharge.

5/21/99

S:\Public\Onboarding Employees\Business Office Forms\Email Fax Internet Policy.doc

ACKNOWLEDGMENT OF E-MAIL AND INTERNET ACCESS POLICY

As an employee of Future In Sight ("Organization"), I understand that the confidentiality and protection of the Organization's information is of the utmost importance. I have read and understand the Organization's Policy on acceptable use of E-mail and Internet access. These policies are in addition to Organization's policies on technology published in the Employee Handbook. Specific technology-related policies are found in Section XVII, part H titled, Technology: Policies and Practices Concerning Agency Computer Systems. Please note the following addition to these policies in part H.

- *"Employees carrying out agency business may only use agency-owned hardware and fully licensed software. Exceptions must be authorized in writing by the President for users of assistive technology at his discretion. All such approved hardware will be covered by the Organization's Service Maintenance Contract."*

If I receive a password for access to E-mail, the Internet or any other system of electronically-stored computer information, I will use it only for authorized purposes. I agree not to use a code, access a file or retrieve any stored communication other than where explicitly authorized unless there has been prior clearance by an authorized representative of the Organization. I will notify my supervisor immediately if I believe that another person may have unauthorized access to my password.

I understand that all information stored in, transmitted or received through the Organization's systems of printed or computer information is the property of the Organization, and is to be used only for job-related purposes. I further understand that authorized representatives of the Organization may monitor the use of the Organization's systems of printed or computer information from time to time to ensure that such use is consistent with the Organization's policies and interests. Further, I am aware that use of the Organization-provided password or code does not in any way restrict the Organization's right or ability to access electronic communications.

I am aware that any violation of the Organization's E-mail or Internet Access Policy may subject me to disciplinary action, up to and including discharge from employment.

5/21/99

(Name)

Date

(Signature)