
(name of company)

INFORMATION TECHNOLOGY POLICY



INFORMATION TECHNOLOGY POLICY

OVERVIEW OF TECHNOLOGIES



The following are examples of technologies governed by this policy. As new technologies gain in popularity and use, they too will be governed by this policy. You should understand that each of these technologies creates an electronic record. This is what separates these from other forms of communications such as a telephone conversation. An electronic record is reproducible and therefore deserves special recognition.

1.1 Email

Email offers an efficient method of conducting Station business. Email consists not only of the Station-provided Email system, but also the act of sending and receiving Email through the Internet.

There are a number of characteristics that distinguish Email from other means of communication, such as paper records, telephones and information stored on electronic media such as diskettes. Awareness of these characteristics should guide your use of Email.

- (a) **Backups.** As part of standard computing and telecommunications practices to prevent loss of data, Email systems and the systems involved in the transmission and storage of Email messages usually are “backed up” on a routine basis. This process results in copying data, such as the content of an Email message, onto storage media that may be retained for periods of time and in locations unknown to the sender or recipient of a message. While it may be difficult and time consuming, it should be assumed backup copies of Email messages exist and can be retrieved, even though the sender or recipient has discarded his/her copy of a message.
- (b) **Special Status.** While password protecting your Email account is beyond usual measures taken to protect access to paper records and telephones, it does not confer a special status on Email records with respect to applicability of laws, policies and practices.
- (c) **Monitoring.** In the course of their work, Station managers or other personnel may monitor the network or Email system. It should be assumed that the content of Email messages may be seen by these authorized individuals during the performance of their duties.
- (d) **Forgeries.** No system of communication is completely secure, including Email. Just as with paper communications, an Email message can be forged and it can be distributed beyond the address list originally defined by its author.

David A. Barnette
dbarnette@jacksonkelly.com

Vivian H. Basdekis
vhbasdekis@jacksonkelly.com

(e) Viruses. Executable files (e.g., *.exe, *.com) can be transmitted via Email. You must always check executable files attached to Email messages for viruses before they are executed on Station-provided IT resources. This is performed in most instances automatically; however, if in doubt call IT.



(f) Legal implications. Email and other electronic files may be accessible through the discovery process in the event of litigation.

1.2 Facsimile (Fax)

In the past, fax machines simply created a paper copy of the original message. This is becoming less and less true; an electronic copy may be created. The same rules governing acceptable use of other Station-provided IT resources also apply to the use of fax technology. The faxed message may be “backed up” onto other storage media.

Use of fax technology does not always require a password for access. Recipients should not assume that the sender is always as reported. A fax should always be perceived as a non-private communication method. Remember, anyone at the other end may read your fax.

1.3 Internet

Even if you are able to encrypt data, anything you transmit over the Internet is subject to interception, reading, and copying by others. This includes Email, personal information and passwords that are transmitted when you log into an account or log into another computer.

1.4 Voice Mail

Voice mail is a means of communication that is similar to a telephone conversation, but it creates a “record”. The sender must remember that the message can also be saved, replayed and shared with others that the sender did not intend. The same rules of password protection and confidentiality that concern other technologies also apply here.

1.5 Emerging Technologies

This policy should allow you to determine the acceptable use of any new or emerging technology. If you have any questions regarding appropriate use of a particular technology not specifically covered in this policy, please contact the appropriate individual in IT.)

David A. Barnette
dbarnette@jacksonkelly.com

Vivian H. Basdekis
vhbasdekis@jacksonkelly.com

UNACCEPTABLE USES OF IT RESOURCES

The first and foremost rule for using these technologies is: ***Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records were laid bare.*** Any use of Station-provided IT resources for inappropriate purposes, or in support of such activities, is prohibited (unless authorized through job responsibilities). The following list includes uses considered unacceptable (list is not all inclusive):

2.1 Illegal Use. Any use of Station-provided IT resources for illegal purposes, or in support of such activities. Illegal activities include any violation of local, state or federal laws.

2.2 Personal Use. Any personal use for commercial, political or religious purposes, product solicitations or advertisements or "for profit" personal activity.

2.3 Sexually Explicit. Any sexually explicit use, whether visual or textual. You should not view, transmit, retrieve, save or print any electronic files which may be deemed as sexually explicit. Accessing child pornography is a federal crime and will result in seizure of the Station's computers or other IT resources used to access such materials.

2.4 Copyright Infringement. Duplicating, transmitting, or using software not in compliance with software license agreements. Unauthorized use of copyrighted materials or another persons' original writings.

2.5 Unnecessary Use of IT Resources. Wasting IT resources by intentionally:


- (1) Placing a program in an endless loop;
- (2) Printing unnecessary amounts of paper;
- (3) Disrupting the use or performance of Station-provided IT resources or any other computer system or network (for example, unauthorized world wide web pages, recurrent mass communications); or
- (4) Storing any information or software on Station-provided IT resources which are not authorized by the Station.

2.6 Security Violations.

- (1) Accessing accounts within or outside the Station's computers and communications facilities for which you are not authorized or do not have a business need;

David A. Barnette
dbarnette@jacksonkelly.com

Vivian H. Basdekis
vhbasdekis@jacksonkelly.com



(2) Copying, disclosing, transferring, examining, renaming or changing information or programs belonging to another user unless you are given express permission to do so by the user responsible for the information or programs;



(3) Violating the privacy of individual users by reading Email or private communications unless you are specifically authorized to maintain and support the system; or

(4) Representing yourself as someone else, fictional or real.

2.7 Viruses. Knowingly or inadvertently spreading computer viruses. “Computer viruses” are programs that can destroy valuable programs and data. To reduce the risk of spreading computer viruses, do not import files from unknown or disreputable sources. If you obtain software or files from remote sources, follow proper procedures to check for viruses before use. You should adhere to any Station-specific policy in this area.

2.8 Junk Mail. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations.

2.9 Confidential Information. Transmitting confidential or privileged information without proper security.

David A. Barnette
dbarnette@jacksonkelly.com

Vivian H. Basdekis
vhbasdekis@jacksonkelly.com