Chief Justice Directive 97-03

SUPREME COURT OF COLORADO
Office of the Chief Justice

CONCERNING COMPUTER SECURITY IN THE COLORADO JUDICIAL BRANCH

The information management systems of the Judicial Branch contain vast amounts of data that are vital to the business of the Branch. It is imperative that these data be preserved and protected from any unlawful or inappropriate tampering. The issue of data security must be a paramount concern for all Judicial Branch personnel. Accordingly, all Branch personnel must adhere at all times to the following:

User IDs and Passwords

User IDs and passwords are a critical level of defense in protecting computers from non-authorized access and use. All personnel must be diligent in protecting their user IDs and passwords. Personnel must not let any other person use their assigned user ID/password, nor shall they use another person's user ID/password.

Each level of password protection reduces the chances that someone can gain unauthorized access to the AS/400 network. Authorized users should have a different password for each part of the system. For example, at a minimum, each user should have one password for Windows, another for the AS/400, and another still for communications software.

In addition to the password standards that are enforced by the AS/400 system itself, users must also adhere to the following practices:

(1) Names of family members or other terms that could be "attributed" to a user should not be used.

(2) Passwords must not be posted on or near a terminal or PC.

(3) User IDs and passwords must not be recorded in a record key or macro. It is appropriate to record a sequence of keystrokes to get into an application; but the record key sequence must begin only after a user has manually entered the user ID and password.

Use of Communications Software on PCs

Communications software which allows a user to communicate directly with a personal computer from a remote site (e.g., PC Anywhere, Carbon Copy, etc.) **should not be used routinely**. On those occasions when it is necessary to use this sort of software, it must be left in a "waiting state" only when the authorized user knows he or she will be attempting to log in from a remote site; otherwise "waiting state" must be disabled. Further, whenever the host PC is in a "waiting state," the user must have signed off of any active AS/400 sessions and end the AS/400 emulation. If available, "callback" features of the communications software must always be used.

Use of Perle Box

When the Perle Box is used, access to Perletalk must at all times be available only through the use of a password.

System-enforced Standards

Various standards and procedures relating to data security have been programmed into the computer system and are mandatory. Such standards and procedures may be augmented or amended from time to time as approved by the IIS Standing Committee.

Viruses

Sneaker-net floppy disks must be routinely checked for viruses. This includes disks used to load software. Under no circumstances may software be loaded from "copied" disks without first scanning the disks for viruses and loading the software only as it is allowed by the licensing agreement with the vendor. Viruses can also be transmitted via e-mail on the internet. Therefore, e-mail should be read only when the sender is known. Under no circumstances may a file be downloaded from the internet unless the user has confidence in the source of the file to be downloaded. A virus check must be run on any downloaded file.

DONE this _____ day of March 1997, effective immediately.

_____

Anthony F. Vollack
Chief Justice