Gary Eikenberry Consulting
122-1010 Polytek Drive, Ottawa, ON, Canada K1J 9J1
Phone: 613-878-7485; E-mail: garyeik@geconsult.com; Web site: http://www.geconsult.ca

File name rules

Please note:
Although various operating systems and file systems have different rules and tolerances regarding file names, the rules below are drawn from a draft for a proposed international standard aimed at resolving issues which arise around moving (usually as e-mail attachments) files between systems. These rules are strongly recommended for internal network use. When you require compatibility with other operating systems (including earlier versions of Windows and Windows Server).

File name length: Although the sky's the limit as far as what your operating system and software may allow, it is strongly recommended that you develop a naming convention that limits the total length of the file name to 128 characters: 124-dot-3, which is to say, one hundred and twenty four characters to the left of the period or dot with a three character extension (usually supplied by the software with which you are saving the file) to the right of the period or dot (on, in the case of four character extensions such as html or docx that would be 123-dot-4).

File name plus path length: Keep in mind that when a file is written to a disk the actual file name has the file path added to it. Some types of media (CDs, DVDs, flash memory many external drives, etc.) and file systems are not able to deal with path/name strings (eg. "C:\Documents and Settings\Default User\My Documents\Letters to Customers\ 2005\February\Wilson and Leblanc\Follow-up to data entry clerk position enquiry.doc") longer than 512 characters. Other media and file systems may "top out" at 1023 characters. On a Windows based network you may be able to save a file with a longer path\name, but not be able to access, copy, move or delete the file. As a general rule it is advisable to try to keep subfolder depths and file names within the 512 character limit.

"Illegal" characters in path/file names: Although some of the characters specified in this rule may not be disallowed by your operating system or application software, they should be avoided, especially when files are to be saved to network locations or may be sent as e-mail attachments.

Accented characters should be avoided in file and path names since different code page (regional and character) settings on different machines may interpret them differently.

The only truly safe **punctuation characters** are the period (.) the hyphen (-) and the underscore (_) character. Space characters and commas are generally acceptable except where "web safe" names are required. Brackets, braces and parentheses ([,], {, }, (,))may or may not be allowed, but are best to avoid. Asterisks (*), colons (:), semi-colons (;), question marks (?), ampersands (&) and slashes or backslashes (/, \ ) should never be used.

An additional note concerning access and permission errors:

With an increasing number of organizations using non-Windows systems and software and with the advent of more aggressive security configurations we are seeing an increasing number of security or ACL (access control list) errors when files are moved around as email attachments or transferred from one device to another via a network connection, FTP, etc. A typical example is an email attachment which you can open but not save after editing or which you can save on your local hard drive but then can't move or delete because of a permission or access rights error. One way to avoid this error is to strip off the security or ACL data when dealing with files from a source outside your own network. The easiest way to accomplish this in a Windows environment is to first save the file to a device formatted with the file system. This includes most flash media (memory cards, USB "thumb drives," etc.) and some external hard drives. Keep in mind that FAT32 is very strict about the above file naming rules. Once a file has been saved to a FAT32 device it can be safely copied or moved to your local hard drive or a network location, at which time it will take on the ACL properties associated with the user doing the copying or moving