Eagle Technology Associates
Guidelines for Preserving Computer Evidence

These guidelines have been developed to assist you in preserving the integrity of the computer that is to be examined for any issues involved with criminal, civil litigation as well as personal or internal company actions. These do not encompass all aspects but are merely to be used as a guide. Please consult your local law enforcement agency or certified computer examiner for any additional steps that may be needed for your case.

1. Proper seizure and recovery of computer evidence requires the use of non-invasive advanced computer software specifically designed for the task. Such software recovers, searches, authenticates and documents relevant electronic evidence during the course of internal investigations or for use in civil or criminal litigation without compromising the integrity of the original evidence.
2. Digital evidence is volatile by nature and can easily be altered without proper handing.

Do not use or search any computer that contains digital evidence – Even the simple action of turning on the computer will alter date and time stamps, computer swap files and other dynamic references contained in temporary files. It's extremely important that the suspected computer, floppy disk, external hard drive or other digital equipment suspected of containing evidence is not used for any purpose and is removed to a secure area under properly designated supervision to await examination by a certified computer examiner.

If the computer or digital device is not currently in your possession, promptly send a certified/registered letter requesting preservation of the evidence - Often times, involved parties lack access to computer evidence in possession of other people or companies. In these cases, a formal letter asking that the computer in question be removed from service and secured along with all relevant computer data immediately until analysis can be conducted through appropriate and approved litigation discovery procedures.

Immediately consult an experienced certified computer examiner – By using any internal or external Information Technology staff untrained in Computer Forensics, the evidence is often spoiled and no longer can be presented in a criminal civil or other litigated proceedings in a manner that can withstand close scrutiny.

Ensure that current recognized forensic software and hardware is utilized – Although there are many software programs that claim to do forensics, only a few are recognized by the courts. The most common programs are EnCase by Guidance Software and Forensic Ultimate Toolkit by Access Data.

For additional information please contact your local law enforcement agency or Eagle Technology Associates at (818) 926-6925 or on-line at www.forensic-computer.net.