Personnel Files

Keep employment records in individual personnel files where access is restricted. Personnel files have confidential information about employees and should be kept in a locked cabinet with access restricted to one individual or a department from whom authorization must be gained before others can view the files.

Most employee information will be kept in the personnel file, but certain documents must be kept in a separate file. These documents include:

- **Medical Records-** Under California law, you must establish a procedure to ensure all employee medical records and information will remain confidential and will be protected from unauthorized use. Failing to establish a procedure will result in a misdemeanor.

- **Equal Employment Opportunity Classification Information-** Companies with 15 or more employees must attempt to recruit and develop a workforce reflective of the community's profile. Therefore, you must maintain a record of the sex, race, and national origin of applicants and employees. Keep the records in a common file rather than in each employee's personnel file.

- **Employment Eligibility Verification (Form I-9)-** Keep forms and information verifying employment eligibility (I-9 form, photocopies of verification documents) in a common file rather than in the personnel file. This makes it easy to access the documents if you are audited by the immigration or labor officials and also makes the documents available to check for expiration dates.

Disposing of Employment Records

Because employment records contain personal information, they need to be disposed of properly. There are two options that are acceptable: shredding and burning. This applies to all companies regardless of size. If you use an outside company to shred your materials, you must use due diligence in choosing a company. The components of due diligence include:

- Reviewing an independent audit of the disposal company's operations and/or its compliance with this rule;
- Obtaining information about the disposal company from several references;
- Requiring that the disposal company be certified by a recognized trade association; and
- Reviewing and evaluating the disposal company's information security policies or procedures.

This applies to all information that is on electronic media as well. If the information is on disks or other recordable media, then it must be destroyed before being discarded. If it is on a computer, they must be erased in a way that makes it unrecoverable. Failure to do so may result in a class-action lawsuit.