**Employee Records Confidentiality Policy**

The company philosophy is to safeguard personal employee information in its possession to ensure the confidentiality of the information. Additionally, the company will only collect personal information that is required to pursue its business operations and to comply with government reporting and disclosure requirements.

Personal employee information is considered confidential and as such will be shared only as required and with those who have a need to have access to such information. Personal information collected by the company includes, but is not limited to, employee names, addresses, telephone numbers, e-mail addresses, emergency contact information, equal employment opportunity (EEO) demographic data, medical information, social security numbers, date of birth, employment eligibility data, benefits plan enrollment information, which may include dependent personal information, and school/college or certification credentials. Participants in company benefit plans should be aware that personal information will be shared with plan providers as required for their claims handling or record keeping needs.

All hard copy records will be maintained in locked, secure areas with access limited to those who have a need for such access. Personal employee information maintained electronically will be safeguarded under company proprietary electronic transmission and intranet policies and security systems, with access granted only to those with a legitimate need. Certain records, such as I-9 forms and medical records, will be maintained separate from general personnel records whether maintained electronically or hard copy.

Company-assigned information, which may include organizational charts, department titles and staff charts, job titles, department budgets, company coding and recording systems, telephone directories, e-mail lists, company facility or location information and addresses, is considered by the company to be proprietary company information to be used for internal purposes only. The company maintains the right to communicate and distribute such company information as it deems necessary to conduct business operations.

If an employee becomes aware of a material breach in maintaining the confidentiality of employee personal information, the employee should report the incident to a representative of the human resources department. The human resources department has the responsibility to investigate the incident and take corrective action. Please be aware that a standard of reasonableness will apply in these circumstances. Examples of the release of employee information that will *not* be considered a breach include the following:

* Release of partial employee birth dates, i.e., day and month is not considered confidential and may be shared with department heads who elect to recognize employees on such dates.
* Personal telephone numbers or e-mail addresses may be distributed to department heads in order to facilitate company work schedules or business operations.
* Employee identifier information used in salary or budget planning, review processes and for timekeeping purposes will be shared with department heads.
* Employee’s company anniversary or service recognition information will be distributed to appropriate department heads periodically.