**Record-Keeping Policy: Safeguarding Social Security Numbers**

 **Purpose**

It is the policy of [Company Name] to protect the confidentiality of its employees’ and applicants’ Social Security numbers (SSNs) obtained and used in the course of business. All executives, managers and employees are expected to adhere to this policy. Any employee violating the provisions of this policy will be disciplined in accordance with company rules.

**Procedures**

***Collection of SSNs***

SSNs will be collected from applicants and employees as required to meet federal or state reporting requirements. These purposes include:

* To conduct pre-employment background checks.
* To verify eligibility for employment.
* To withhold federal and state taxes.
* To comply with state new-hire reporting.
* To facilitate enrollment in company benefits plans.

SSNs may also be collected from creditors, suppliers or independent contractors where no tax identification or employer identification number is accessible. SSNs so obtained will be subject to the same provisions of the privacy policy as those for applicants and employees.

***Use of SSNs***

Except for verification and reporting uses for the above-referenced reasons, no SSN or portion of an SSN will be used in the conduct of the company’s business. In addition:

* No SSN or portion of an SSN will be permitted to be used for identification badges, parking permits, timecards, employee rosters, employee identification records, computer passwords, company account records, licenses, agreements or contracts.
* No SSN or portion of an SSN will be used in open computer transmissions or company distributions or through the company intranet except where such transmission of information is by secure connection or is encrypted. As examples, reporting of payroll withholding taxes and benefits plan participation require such data; thus, such transmissions of data will be handled through secured computer transmission only.

***Storage of SSNs***

All documents containing SSNs should be stored in locked, secured areas. All computer applications containing SSNs should be maintained on secured, authorized-access computer stations only.

***Access to SSNs***

Only persons who have a legitimate business reason will have access to SSNs. Such access will be granted through department heads responsible for functions with reporting or transporting of such data responsibilities. Department heads and employees granted such access must take all necessary precautions to ensure the integrity of records that include such numbers when the records are not being used.

***Destruction of SSNs***

Records that include SSNs will be maintained in accordance with federal and state law. When such documents are released for destruction, the records will be destroyed by shredding.

**State Laws**

If this policy, or any part thereof, conflicts with a state law in any state in which the company operates, the state law should supersede this policy, or the relevant portion thereof.