5180-R Unauthorized Release of Information (Cf. 5185) 5180-R

Employee Competence

1. The District will take steps, through the interview, selection, assignment, and hiring process, to see that any employee, or data processing Subcontractor employee, if any, who is authorized to access driver, vehicle and related records, or who has access to information regarding criminal background checks or unprofessional conduct checks and related records will:
    1.) Be adequately trained to access such records,
    2.) Be competent to perform that task, and
    3.) Conduct each record inquiry in accordance with the standards of technical competency that are generally recognized in the data service industry.

Security of Data

The District will implement the following security requirements whenever and wherever records and/or information obtained through any means, electronic or otherwise, is accessed, stored or disseminated:

1. Use software and hardware that is technologically adequate to prevent unauthorized access to the information.
2. Establish operational programs to prohibit unauthorized inquiries from any terminal or other access site.
3. Institute operational programs to detect unauthorized attempts to penetrate the District's system of electronic records.
4. Provide for the physical security of the District's computer system, with procedures and devices designed to protect against the theft of records and information.
5. Secure from each employee (or Subcontractor employee) a signed and approved System Access Request form (or other equivalent form) that grants authority and permission to access driver, vehicle, criminal, or related records directly.

Rules Accepted: June 29, 2009