

CONFIDENTIALITY OF AGENCY INFORMATION:

1. Contractor shall take all precautions and measures necessary to ensure the integrity, nondisclosure, confidentiality and protection of all data and information obtained from SCC or derived there from, including but not limited to all original reporting forms and data in any other form, and agrees to comply with all Federal and state guidelines including but not limited to the COV ITRM Standard SEC501-01 and the Data Protection Guideline SEC507-00 concerning the protection of sensitive data.
2. Prior to the commencement of any work for SCC, the contractor shall declare in writing that he or she understands that all data and information obtained from SCC or derived there from is sensitive and will be held in the strictest confidence by Contractor, its officers, directors, agents, and employees and that Contractor, its officers, directors, agents, and employees shall be governed by and comply with Federal and State laws prohibiting the disclosure of information obtained or compiled during the course of their work for SCC.
3. All information obtained and work performed under this SCC contract/order is considered sensitive, requires use of sensitive and personal data and information and falls under one or more categories of information that is subject to protection from disclosure and misuse, including but not limited to: personal information and highly restricted personal information in connection with motor vehicle records under the Federal Drivers Privacy Protection Act, (18 USC 2721 et seq.) law enforcement sensitive data and information, the Privacy Act, personal, vehicle and driver information as defined under and governed by Va. Code §46.2-208 et seq. and personal information as defined under and governed by the Virginia Government Data Collection and Dissemination Practices Act (VA Code §2.2-3800 et seq.).
4. All source materials/data/information and resultant work products compiled or created and any information or portion of information derived there from are the property of SCC and must not be used by the contractor for any purpose other than the purpose outlined by this agreement.
5. The contractor, its officers, directors, agents and employees shall hold all information obtained under a SCC contract/order in the strictest confidence. All information obtained shall be used only for the purpose of performing this contract/order and shall not be divulged nor made known in any manner to any person except as necessary to perform this contract/order. Neither Contractor, nor its officers, directors, agents, or employees shall divulge, sell, or distribute any information obtained from SCC or derived there from at any point in time, even after termination or expiration of a contract/order.
6. Except as specifically authorized by the contract/order, Contractor, its officers, directors, agents, and employees are prohibited from reproducing SCC source media, written products, or any portion thereof.
7. The contractor shall notify in writing, each of its officers, directors, agents, and employees having access to SCC information that such information may be used only for the purpose and to the extent authorized in this contract.
8. The Contractor shall provide a security plan outlining the steps and methods taken to secure and protect the information provided by SCC to address the following points:
 - Security of Files and/or Copies of Records (for Hardcopy).
 - Security of on-line Computer Terminals (On-Line Users Only).

- Designation of Authorized Users/Assignment of Access Codes.
- For automated interfaces/electronic extraction and storage of data, if applicable:
- Security of Records, Files, and Systems, use of encryption for storage.
- Names and addresses of data extraction method and software creators/vendors,
- Network Diagrams and descriptions of Data Extraction methods and software,
- Descriptions of system support processes including backup methods and frequencies.
- Proposed Audit/Management Controls Over Access and Dissemination of Requested Information.

9. Contractor agrees to comply with all federal and state statutes, rules and regulations and understands that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, shall be grounds for immediate termination of this agreement may subject the offender to criminal sanctions.

10. Contractor shall indemnify, defend, and hold harmless the Commonwealth, SCC, its officers, directors, employees and agents from and against all losses, liabilities, damages and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties), incurred in connection with any action or proceeding arising directly or indirectly from unauthorized use or disclosure by Contractor, its agents, directors, officers or employees, of any data or information obtained from SCC pursuant to this agreement, or derived therefrom. Contractor shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Contractor shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification required may be delayed if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

- Notice may be provided by one of the following methods:
 - (1) written notice to the most recent available address the person or business has in its records;
 - (2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or
 - (3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

(i) e-mail notice when the person or business has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification ~~by major statewide media, including newspaper, radio and television.~~

Deleted: to

- If a person discovers circumstances requiring notification of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

- Notification must include:

(1) a general description of what occurred and when:

(2) the type of PII that was involved

(3) what actions have been taken to protect the individuals personal information from further unauthorized disclosure.

(4) what if anything, the contractor will do to assist affected individuals, including contact information for more information and assistance; and

(5) what actions the contractor recommends that the individual take.

Formatted: Indent: Left: 108 pt,
No bullets or numbering