Attachment A: Data/Information Security Policy for Contractors

Revised 8/15/2018

Information Technology Security

a. **General Security Statement:** You will implement appropriate administrative, technical, and physical safeguards to ensure the security, privacy, confidentiality, integrity, and availability of Indiana Bureau of Motor Vehicles or the Bureau of Motor Vehicles Commission information, collectively referred to as BMV/C. Whether BMV/C information is stored on, processed on, or transmitted by BMV/C systems, your systems, or third-party provider systems, you (and your third party providers if applicable) will use information security controls to: (1) protect any and all BMV/C information and BMV/C systems you have access to while performing your obligations under any agreement; and (2) protect your systems and your third party provider systems on which BMV/C information is stored, processed, or transmitted.

b. **Access to BMV Systems:** Contract staff and/or subcontractors may not be allowed access to BMV/C data systems without prior individual approval from BMV/C, which may include but is not limited to periodic background checks. BMV/C must be notified immediately each time an approved individual leaves employment or the subcontract for an approved subcontractor is cancelled or when these individuals are reassigned to duties that do not involve access to BMV/C data systems. No agent of a contractor will be permitted access to Social Security Administration (SSA) data until he/she has completed all required forms and executed the required agreements for such access.
    a. Any contractor, and their agents/users, who receives access to SSA data through the Information Exchange Agreement (Agreement) between the BMV/C and SSA through the Social Security On Line Verification (SSOLV) process agrees to be bound by the terms and conditions concerning the access, use or disclosure of SSA data under the Agreement, including the penalties associated with loss or disclosure.
    b. Your access to any BMV/C information and/or BMV/C systems, including but not limited to any BMV/C customer and/or employee information, is subject to your continuing compliance with this Policy. We may immediately, automatically, and unconditionally revoke your access, and all links and interfaces, to BMV/C information and/or BMV/C systems without liability for any reason or no reason.

c. **Minimum Information Security Controls:** You must implement and maintain the minimum information security controls set forth in the State of Indiana IOT's Information Security Framework (ISF) and the BMV Information Security Policy and Standards.
    a. You must reach out to the IOT security team at security@iot.in.gov to request an NDA and subsequent ISF documentation. If implementation of an IOT policy or standard is not possible due to technology differences, naming standards, or the like, you must provide a methodology that meets or exceeds the IOTs minimum standard of security, or request an exception by bmvsecurityteam@bmv.in.gov.
    b. You must reach out to the BMV security team at bmvsecurityteam@bmv.in.gov to request the BMV Security Policy.

d. **Audit of Security Controls:** If we request, you will provide, at your expense, a written description, certified in writing by your authorized representative, of compliance with this Policy (including without limitation how you implement each security control).
    a. In addition, if we request, you will allow us, IOT, and \ or our independent third party, to audit your compliance with this Policy (including without limitation performing penetration testing and vulnerability scans). You will work with us, at your own expense, to remedy any deficiencies the audit identifies to our reasonable satisfaction.

b. Further, BMV/C may require you to obtain a formal audit of your security controls conducted by an unaffiliated third party. If this is required, you must provide BMV/C with the written audit results. Examples of acceptable audits include the following:
    i. An AICPA SSAE 16 SOC 2 Type II audit. You will promptly remediate at your expense any failures or deficiencies found in the SOC 2 Type II report.
    ii. An ISO/IEC 27001:2013 certification.
    iii. Other appropriate audit providing objective assurance of security controls, such as NIST, FedRAMP at FIPS 199 Moderate baseline, or equivalent.
c. Nothing in this section limits our audit or other rights we may have in any other agreement with you or your third party providers.

e. Personal Information (PI) – Definition:

a. "Highly restricted personal information" shall mean the following information that identifies an individual:
    i. Digital photograph or image.
    ii. Social Security number.
    iii. Medical or disability information.
    iv. Bank account and credit card information/numbers.
b. “Personally Identifiable Information”, or PII, shall mean information that identifies a person, including an individual's:
    i. Digital photograph or image;
    ii. Social Security number;
    iii. Driver's license or identification document number;
    iv. Name;
    v. Address (but not the 5-digit zip code);
    vi. Telephone number;
    vii. Medical or disability information; or
    viii. Bank account and/or credit card numbers or other associated identifying information.

f. **Disclosure of Personal Information**: The disclosure of personal information collected and/or obtained by the BMV/C is subject to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.) (“DPPA”) as implemented under state law at Indiana Code (“**IC**”) §9-14-13. Except as agreed to between BMV/C and Contractor and as permitted by and in accordance with the DPPA and IC §9-14-13, a Contractor of the BMV/C, or an officer or employee or subcontractor of the Contractor, shall not knowingly, accidentally disclose or otherwise make available any personal information obtained in connection with a motor vehicle record.
    a. "Disclose" shall mean to engage in a practice or conduct to make available and make known personal information contained in a motor vehicle record about a person to another person by any means of communication.
    b. "Record" shall mean means any information, books, papers, photographs, photostats, cards, films, tapes, recordings, electronic data, printouts, or other documentary materials, regardless of medium, that are created or maintained by the BMV.

g. **Confidentiality of BMV/C Information:**
    a. Contractors of the BMV/C shall follow all requirements of IOT Information Security Framework (ISF) and the BMV Security Policy and Standards regarding the protection of all personal information (“PI”).
    b. It is the Contractor’s responsibility to ensure all Contract staff and/or subcontractors with any access to BMV/C data systems and/or PI understand these policies and that access to and/or use of BMV/C data systems and/or PI is limited only to those staff/subcontractors whose access to and/or use of this information is essential for the purpose of carrying out the Contractor’s or subcontractor’s obligations governed by this Contract.

h. **Information Retention and Disposal:**
    a. Pursuant to 18 U.S.C. §2721(c) of the DPPA and IC §9-14-13-10, upon termination of a contract, a Contractor who resells or re-discloses PI pursuant to its contract with the BMV/C shall maintain for a period of five (5) years all records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make these records available to the BMV/C upon request.

b. At the end of five (5) years, a Contractor who resells or re-discloses PI pursuant to its contract with the BMV/C shall securely return or destroy any PI in a commercially reasonable manner, including contracting with a third party for destruction of said PI, and provide to the BMV/C a certificate of destruction.
c. This means you will shred paper copies of BMV/C information and you will destroy electronic copies in a confidential manner so that they are no longer usable, readable, or decipherable, and the information on them is not retrievable.
d. If any PI is stored in a data format proprietary to the Contractor, the Contractor shall provide the BMV/C with a copy of the PI in a standardized format (e.g. PDF, TIF, JPG, GIF, etc.).
e. The Contractor will ensure that any subcontractor shall promptly securely return any PI upon termination of the Contract.
f. Those Contractors that are NOT AUTHORIZED to resell or re-disclose PI pursuant to their contract with the BMV/C shall either securely return or destroy any PI in a commercially reasonable manner and provide to the BMV/C a certificate of destruction upon termination or expiration of their Contract.
g. Nothing in this Policy will prevent you from maintaining information still subject to confidentiality obligations as required by law or any regulatory authority to which you are subject.

i. **Data Breaches:** Unless subject to IC §24-4.9, Contract staff members and/or subcontractors shall complete the Contractor's Personal Information Disclosure Report below each time an unauthorized disclosure of a customer's personal information occurs. The process to follow is based on the type of data breached:
   a. **Social Security Administration ("SSA")-Provided Personal Information Disclosure Incident Report:**
      i. Contract staff and/or subcontractors who experience or suspect a breach or loss of PI that contains SSA-provided personally identifiable information shall immediately (within 24 hours of the incident) complete the online Personal Information Disclosure Report at **https://secure.in.gov/BMV/SecurityIncidentReporting/default.aspx** .
      ii. The Contractor and/or subcontractor acknowledges that time is of the essence in reporting suspected breaches or loss of PI that contains SSA-provided PI and shall not delay the reporting thereof.
      iii. The Contractor must also immediately notify the BMV by direct telephone contact **within one (1) hour of discovery.**

William Woolsey
Information Security Director
Telephone: (317) 499-3988
E-mail: wwoolsey@bmv.in.gov

Joe Fewell
Telephone: 317-416-5144
Email: jfewell@bmv.in.gov

Steve Leak
Telephone: 317-691-3896
Email: sleak@bmv.in.gov

      iv. Upon receipt of the Report, the BMV/C Legal Department will review, investigate and make any necessary reports to the appropriate state and/or federal agencies.
   b. **All other Personal information:**
      i. Contract staff and/or subcontractors who experience or suspect a breach or loss of all other personal information shall immediately complete the online Personal Information Disclosure Report at: **https://secure.in.gov/BMV/SecurityIncidentReporting/default.aspx** .
      ii. Upon receipt of the Report, the BMV/C Legal Department will review, investigate and make any necessary reports to the appropriate state and/or federal agencies.