State of Indiana, Bureau of Motor Vehicles
Electronic Lien (E-Lien)

Program Requirements

Section 1: Overview

These Program Requirements ("Requirements") provide the parameters for [COMPANY NAME] ("Provider") certification and continuing participation in the Indiana Bureau of Motor Vehicles ("BMV") electronic lien and title ("ELT") program (the "Program") pursuant to Contract No. [CONTRACT NO.] ("Contract"). This Agreement is the presiding document governing the systemic functions of the Program and sets forth guidance with regard to services required, implementation plan, and ongoing support for the Program. The goal of the Program is to meet the requirements of Indiana Code ("IC") 9-17-5-6.

The Requirements provide Provider with the information needed to participate in the Program including:

1. Administration, policy, and procedure requirements
2. Technical, system, and installation requirements
3. Roles and responsibilities of Program participants
4. ELT allowed transactions

These Requirements are intended to offer Provider sufficient technical details regarding the Program as they consider the requirements necessary to provide an electronic filing service program.

The Requirements provide the criteria BMV will use to review and evaluate the Program and Provider's performance. BMV will conduct periodic reviews of the Provider to evaluate performance and compliance with the Requirements. Based upon these periodic reviews, or upon request from the Provider, the Requirements may be amended.

Section 2: Definitions

a) **BMV Systems** are any of the databases or other electronic systems owned, operated, or maintained by BMV.

b) **Lienholder** is a lender that holds an encumbrance on an Indiana vehicle certificate of title to secure a debt and records such security through Provider's Systems.

c) **Personal Information** means all data identified by IC 9-14-6-6.

d) **Provider Systems** are any of the databases or other electronic systems owned, operated, or maintained by Provider.

Section 3: High-Level Requirements

a) Provider shall develop and maintain a system that will interface with BMV Systems via an application programming interface. Each transaction will be transmitted to BMV Systems in real time.

b) The Program will allow Providers to:
   1) Make ELT-related inquiries to BMV Systems through a device inquiry function; and
   2) Process ELT-related transactions at their location.

c) Provider Systems shall permit Lienholders to perform the following transactions:
   1) Releasing liens
   2) Requesting a paper title with electronic lien recorded

d) Provider is expected to use the Program to process approved ELT-related transactions only. Providers are not to use the Program as a device to access BMV title and registration records not related to an ELT transaction.

e) Provider Systems must conform the E-Lien Service Provider Technical Specifications Document, set forth in **Attachment A**, which is attached hereto and fully incorporated herein.

Provider must maintain compliance with the Service Provider Technical Specifications as published and updated by BMV.

1) In the event the Service Provider Technical Specifications are updated following execution of the Contract, unless otherwise permitted by BMV, Provider must come into compliance with the updated specifications within sixty (60) calendar days from the publication of the new requirements. Provider shall bear the cost of any enhancements required of their Systems.
2) If a change has been legislatively mandated, Provider shall not process a transaction that would put them in violation of the law.

f) Upon execution of the Contract, BMV shall assign a Service Provider identification number to Provider. This will serve as the unique identifier for Provider's use in the Program.

g) BMV may suspend a Provider's or Lienholder's ability to process a transaction for any violation of the Requirements or the Contract that negatively impacts the nature, quality, or value of the services or products provided under the Requirements or Contract.

h) Provider must be able to temporarily or permanently suspend the ability for Lienholder to process transactions through Provider Systems if required by BMV.

i) Provider may not process transactions if the communication lines between Provider and BMV are down.

<u>Section 4: Communication</u>

a) Provider commits to providing personnel for the BMV to contact regarding all aspects of Provider's participation in the Program. BMV and Provider agree that timely communication is a key factor in the success of the Program. When problems or disputes arise, they will be promptly brought to the attention of the applicable parties. It is the intention that most issues will be resolved through the joint effort of BMV and Provider; however, should staff from BMV or Provider be unable to resolve the issue to the satisfaction of the other, issues can and should be escalated to work toward a resolution.

b) Changes in the Requirements necessitated by legislative changes to statute will be communicated to Provider prior to their implementation.

c) Changes in the Requirements necessitated by changes in data processing requirements or system changes will be communicated to Provider prior to their implementation.

<u>Section 5: Program Onboarding</u>

a) **Provider System Testing and Certification:** Provider shall participate in a BMV onboarding program to ensure system operation.

1) **Development Phase:** following execution of the Contract, BMV will provide the necessary technical information to Provider to begin the testing process to ensure compatibility between BMV and Provider Systems.

   A) Provider shall use data provided by BMV comprising of, at minimum, vehicle identification number, title number, and Service Provider identification number, (collectively, "Test Data") to be used for testing purposes. Provider shall utilize only the Test Data prior to acceptance into the Program to aid in development of Provider systems.

   B) Provider must be able to connect and send Test Data to a test environment provided by BMV. Test records will be processed and will require BMV approval before changes are implemented to production.

      i. Provider must send a transaction (update BMV Systems) through the processes outlined in the Service Provider Technical Specifications.

ii. If no response is received from BMV Systems on the transaction sent, Provider must submit the transaction again. Lienholders cannot continue with the transaction if there is no response from BMV Systems.

iii. Provider must check for a transaction acknowledgment message that confirms the transaction was accepted. If an acknowledgement from BMV Systems is not received, Provider must resubmit the transaction.

C) Upon BMV's request, Provider shall provide information on program interfaces that will interact with the BMV system.

D) Provider shall provide a sandbox/test environment to conduct joint testing with BMV.

E) Provider shall provide access to Provider's development team personnel (including but not limited to coders, testers, and business analysts) to ensure efficient and effective development.

F) Provider shall ensure appropriate development team personnel are available for and attend meetings scheduled by BMV necessary to collaboratively develop Program functionality.

G) Provider shall timely remediate Provider system defects identified during testing and production.

H) Provider may participate in optional Live Onboarding Q&A Sessions that will include BMV IT and line-of-business resources.

2) **Certification Phase:** following the Development Phase, Provider must demonstrate system operation to BMV's satisfaction.

A) Provider shall demonstrate functionality of Provider systems as requested by BMV through use of virtual desktop or similar technology in a test environment.

B) When ready, Provider shall participate in a Certification Session, during which Provider shall demonstrate the required transactions (both inbound and outbound) in a test environment.

C) Upon passage of the Certification Session, Provider will receive new access credentials to the production system.

b) **Initial Lienholder Onboarding:** Upon acceptance into the Program, Provider shall provide lienholder-specific information in a format specified by BMV to enable bulk loading of lienholder information into the appropriate BMV Systems and for assignment of lienholder identification numbers.

Section 6: Continuing Participation

a) Provider shall maintain, at its own expense, Provider Systems. This includes all equipment, devices, telephone and data lines, and the associated communications facilities, wiring, and other components necessary to effectuate the Requirements.

b) Provider shall maintain information related to each Lienholder that includes, at a minimum:

1) The type of financial institution; and

2) A physical or electronic copy of the financial institution's federal or state charter or license.

c) Provider shall participate in Provider System testing of future development efforts in a manner similar to the testing, development, and certification outlined in Section 5.

d) Ensure adequate staff for routine support needs post-implementation for both BMV and Lienholders, including but not limited to:

1) General maintenance;

2) Issue resolution; and
3) Building out enhanced functionality alongside BMV.

e) Continuing lienholder onboarding: Provider shall provide new Lienholder information in a format specified by BMV. BMV will load that information into its system and assign a lienholder identification number within thirty (30) calendar days of receipt from Provider.

f) Provider shall provide status updates for service interruptions/outages to BMV via the ELT Help Desk when such interruptions/outages occur.

g) If Provider's system is down for a period of more than four (4) hours, Provider must notify BMV via the ELT Help Desk.
   1) In the event BMV Systems are unavailable or otherwise down, Provider's system should allow a Lienholder to complete and save transactions and then retrieve and transmit them when BMV Systems are available.

h) Provider Training Responsibilities: Provider training responsibilities include, at a minimum, the following:
   1) Design and development of training courses for Lienholders on:
      A) Program standards;
      B) Data Security (e.g., passwords, account-sharing);
      C) Driver Privacy Protection Act (DPPA) restrictions;
      D) Permitted ELT transactions and BMV policies and procedures concerning the processing of transactions; and
      E) Provider's system hardware and software.
   2) Providing follow-up training to Lienholders as needed or requested by BMV.
   3) Ensuring new Lienholders receive training before utilizing the ELT system.
   4) Providing ongoing training as BMV provides changes in procedures.
   5) Ensuring all Provider staff, contractors, and Lienholders with access to BMV Systems or data understand the Data Security requirements set forth in Section 12.
   6) Ensuring all Provider staff, contractors, and Lienholders understand that they are prohibited from using information concerning vehicle titles for any commercial, marketing, business, or other purpose not specifically contemplated by the Program.

<u>Section 7: Audits</u>

a) BMV may perform audits, at any time, to evaluate compliance with the Requirements, including but not limited to, reviewing controls and activities related to the Program.

b) Provider agrees to provide access to all information necessary to the scope of an audit by the BMV.

c) BMV may require Provider to engage an independent third party to perform a Service Organization Controls (SOC) 2, Type II review pursuant to the AICPA's Attestations (AT) section 101, Attest Engagements professional standard. The SOC 2, Type II review should be based on control requirements presented in the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy.
   1) If requested by BMV, Provider must provide an updated SSAE 16 SOC 2 Type 2 audit report to the State within ninety (90) days after Provider's receipt of such request. The SOC 2 audit must have been completed within the prior twelve (12) months. Provider must provide copies of such audit reports covering controls on its own organization as well as controls on its subservice organizations. Any such audit reports will be recognized as Provider's Confidential Information.

2) Any deficiencies detected in subsequent evaluations related to ELT must be immediately reported to BMV along with corrective action plans that must be approved by BMV before they are implemented.

d) Provider shall establish a plan of action to remediate any deficiencies identified in an audit. This plan shall be submitted to BMV within fourteen (14) days from identification of the deficiency.

Section 8: Reporting

a) Each quarter, Provider shall be required to submit, in form and manner prescribed by BMV, a report on all the lien transactions conducted during the previous quarter. The report shall be submitted to the ELT Help Desk.

b) Provider must produce any other reports as deemed necessary by BMV, including, but not limited to, Lienholder invoicing under Section 9 or data security pursuant to Section 12.

c) Any reports generated must be made available upon request from BMV. Electronic copies of reports requested by BMV must be maintained for seven (7) years.

Section 9: Fees

a) Provider may not assess a per-transaction fee to Lienholders that exceeds the total of:

1) The fee for use of Provider Systems consistent with market pricing in accordance with IC 9-17-5-6(g)(6); and

2) The fee assessed to Provider by BMV pursuant to IC 9-17-5-6(g)(4).

Section 10: Termination from Program and Annual Review

a) The following are prohibited under the terms of this Agreement and may result in Provider's termination from the Program upon written notice from BMV:

1) Using BMV data for any purpose not associated with the Program;

2) Providing access to the Program to a lienholder or other person not authorized by the BMV;

3) Willful misrepresentation of Program policies, procedures, contractual terms, or other information;

4) Failure to correct errors or resolve outstanding erroneous transactions as requested by BMV;

5) Failure to comply with the Requirements or technical specifications of the Program.

6) Failure to remain in good standing with government entities in terms of conduct and performance, including lapse or sanction by any state or federal agency;

7) Intentionally entering false information into BMV Systems;

8) Referencing BMV in marketing or advertising without the express written consent of BMV;

9) Failing to inform BMV of circumstances in the business that could impact the Program, including intent to file bankruptcy, change of business entity, ownership, or legal judgments;

10) Any violation of Indiana or federal law.

b) Nothing in this Section shall prohibit BMV from exercising any other termination rights set forth in the Contract.

c) BMV may perform a formal review of Provider after Provider Systems are operational. Factors that will be considered in the evaluation include, but are not limited to:

1) Increases in detection of Lienholder violations.

2) Incidents of improper use of BMV record data.

3) Number of Lienholder phone calls to the ELT Help Desk.

4) Incidents of Lienholder errors/issues.
5) High levels of errors when processing transactions.
6) Timeliness of programming changes requested by BMV to correct problems with Provider Systems or to address legislatively mandated changes.
7) Timeliness of response to requests to the Provider for information or assistance with resolving Provider errors.
8) Failure to provide annual assessment of the Provider's internal control processes of Provider Systems.
9) Provider System performance and uptime
10) Connectivity issues

Section 11: ELT Help Desk

BMV has created a dedicated Help Desk to assist with Program-specific issues. Provider shall contact ELTHelpdesk@bmv.IN.gov as a first point of contact with any questions related to the Program.

Section 12: Data Security

a) **General Security Statement:** Provider shall implement appropriate administrative, technical, and physical safeguards to ensure the security, privacy, confidentiality, integrity, and availability of BMV information. Whether BMV information is stored on, processed on, or transmitted by BMV Systems, Provider Systems, or third-party provider systems, Provider (and Provider's third-party vendors, if applicable) will use information security controls to:
1) protect any and all BMV information and BMV Systems Provider has access to while performing the obligations under these Requirements; and
2) protect Provider systems on which BMV information is stored, processed, or transmitted.

b) **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 IC 9-14-13. Except as agreed to between BMV and Provider and as permitted by and in accordance with the DPPA and IC 9-14-13, a person with access to Personal Information shall not knowingly or accidentally disclose or otherwise make available any Personal Information obtained in connection with a BMV record. No data under this Agreement shall include Social Security number or any other Social Security data.

c) **Provider System Maintenance:** Provider warrants that all systems, media, network connections used for BMV information access and services meet all security requirements set forth in the Contract. All changes to the systems, storage, media, and network used for access, storage, maintenance, or any other purpose of State-provided information must be disclosed to BMV. Provider shall maintain on-site (in a physical or electronic format), review, and abide by the Indiana Office of Technology (IOT) Security Framework and BMV Information Security Policy and Standards. Provider must visit https://www.in.gov/iot/security/information-security-framework2/ to request an NDA and subsequent ISF documentation.

d) **Sale and Redisclosure:** Provider agrees that neither it nor any of its agents shall sell, assign, redisclose, or otherwise transfer any information or portions of information or data obtained pursuant to the Contract to any other party. Provider shall not use any record information so obtained pursuant to this Contract for any purpose other than those as specifically authorized by this Contract.

e) **Internal Controls:**
   1) Provider shall establish internal procedures designed to:
      A) Prohibit access to BMV data by unapproved individuals; and
      B) Immediately delete any data or information received from BMV after the purposes for which it was requested is complete.
   2) Any agreement entered into between Provider and a Lienholder to become a part of the Program must include procedures and practices designed to:
      A) Prohibit access to BMV Systems or data by unapproved individuals; and
      B) Prohibit Lienholders from retaining any data or information received from BMV after the purposes for which it was requested is complete.

f) **User Identification:** A logon is needed to identify the person responsible for processing each ELT transaction. Provider shall ensure this is accomplished by assigning and controlling individual User IDs and requiring each individual to use the User ID authentication method provided to them to access each session. Individuals shall not share the same User ID and password. Beginning six (6) months following execution of this Agreement, Provider must ensure that at the start of a user's logon attempt, a message to the user will appear and remain on the ID/password screen until the user takes explicit actions to log on or further access the information system. The affirmation must provide the following:

> "I certify that I am the individual registered under this account and that the information provided is mine. I understand that the willful unauthorized disclosure of information obtained by accessing this account for a purpose other than what is permitted usage related with this account, or sale or other redisclosure of personal information to a person or organization not identified in this request, is prohibited and may result in criminal and civil penalties imposed under the provisions of state and federal laws, including state and federal Driver Privacy and Protection Acts (DPPA). I understand that I am accessing an information system where individual that usage may be monitored, recorded and subject to audit. Use of the system indicates consent to monitoring and recording."

With approval from BMV, Provider may substitute substantively similar language.

Passwords must consist of a minimum of fifteen (15) characters with a combination of upper- and lower-case letters, numbers, or special symbols. Passwords will automatically expire every 90 days and require the user to change it if not changed sooner. New passwords cannot be any password that has been used within the last ten (10) generations. Provider Systems must provide the user the capability to change their password any time they believe their password security has been compromised.

Provider will suspend the User ID and revoke the password for any individual who does not enter their correct User ID and password within three attempts. Each logon attempt must be captured in a log. When a user's ID has been suspended, they must contact the Provider's support center to have it re-enabled.

Provider must sign a security and disclosure statement acknowledging that Provider understands the BMV security and confidentiality requirements and their responsibility to ensure their staff adheres to these requirements.

A representative of each Lienholder must also complete and sign an Information Access Agreement (**Attachment B**) acknowledging that all Lienholder's users understand and agree to abide by BMV security and confidentiality requirements. Provider must retain a signed copy. An authenticated electronic version of each signed agreement is acceptable. These agreements must be kept on file by Provider for as long as the Lienholder is using Provider's system and emailed to the ELT Help Desk during Lienholder onboarding.

g) **User Authentication:** Before a logon access session may be initiated, Provider must require Lienholder to validate and accept the individual's user authentication method. Lienholder shall require a user to enter their password using a password known only to the user. If an individual is not an authorized user, Provider shall not allow access to Provider Systems. Provider shall also require entry of a Multi-Factor Authentication ("MFA") passcode for each user upon logon if it has been more than twenty-four (24) hours since the user's last MFA passcode entry. The passcode shall be displayed via out-of-band device such as a hard token, SMS to a cell phone, or software token on the user's machine, or email.

Provider shall assign an electronically enforced unique default user authentication to each individual upon initial access. The default user authentication shall be used if a user has forgotten their password or a user has incorrectly attempted a logon access session three (3) times and has had their access suspended. Provider shall ensure the new password is used for the next access only, and the default user authentication shall not be capable of being used for subsequent access by any user.

h) **User Authorization:** Provider staff may not be allowed access to BMV Systems without prior individual approval from BMV. BMV must be notified immediately each time an approved individual leaves Provider employment or when these individuals are reassigned to duties that do not involve access to BMV Systems. Notice under this section must be sent to ELT Help Desk.

Permission for proper authority to access the information being requested will be verified by Provider as part of the access control administrator function. If Provider receives a request to access the system or process a transaction from an unauthorized user, Provider shall terminate the transaction and create a log of the unauthorized attempt. Provider shall also check for patterns that might indicate to BMV when unauthorized attempts to access information are suspected and assist BMV in any investigation that may occur.

Provider will maintain an employment record of all employees who have access to BMV or Provider Systems for at least two (2) years after the employee has their access terminated. Access to BMV Systems must be terminated immediately upon separation of employment or reassignment to a non-BMV project. Provider shall provide a quarterly report to ELT Help Desk of user access terminations.

i) **Provider System Security:** Provider Systems shall be located in a secure facility. The computer room shall be restricted with access only to authorized Provider staff and never out of Provider's control. Provider's service personnel shall be restricted to an application shell that allows customer set-up, password management, and customer support. Service personnel shall not access the operating system from outside that shell. Access codes and operator manuals shall be restricted to authorized users only.
   1) Provider is responsible for incorporating security measures into the host system and other components of the system to preserve the security of BMV records and BMV database. Security provisions shall include user IDs and passwords.
   2) Access from only an authorized user device which are appropriately identified.
   3) Provider must remain compliant with FISMA and the NIST Special Publication 800.53 (most recent version) MODERATE controls using minimum control values as established in the applicable PSP. An equivalent security standard may be accepted if approved by BMV.
   4) If Provider Systems are hosted by a cloud provider, Service Provider must provide evidence of Provider's FedRAMP certification.

j) **File Retention:** Provider Systems shall create and maintain logs for each user that BMV can use for auditing, troubleshooting and record keeping. Provider shall also maintain electronic transaction history records. Records shall include the following:
   1) Transaction Log: This file shall contain the complete history of every transaction and associated BMV interaction including physical or logical device number and user identification. Records shall be maintained for at least seven years from the date of transaction.
   2) Security Log: This file shall contain a security record for each transaction attempted. The log shall also contain a record for each security violation. A security violation is a non-authorized attempt to use Provider Systems (including, at a minimum, invalid passwords and user IDs). Records shall be maintained for at least five years from the date of the attempted access or transaction.

k) **Data Breaches:** If Provider experiences a data breach or other breach of its system security, Provider must notify BMV within twenty-four (24) hours by emailing BMVSecurityTeam@bmv.in.gov. Provider must provide BMV with any information related to the breach requested by BMV.
   1) For purposes of this Agreement, "data breach" means any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

Attachment A

State of Indiana, Bureau of Motor Vehicles
Electronic Lien (E-Lien)

Service Provider System Specification Document

BMV ELT Program – Service Provider System Specification Document

Provider Systems must conform to the E-Lien Service Provider Technical Specifications Document. These specifications are published and updated by the BMV. To ensure the most updated copy is used, please download the current version utilizing the link above.

Attachment B

State of Indiana, Bureau of Motor Vehicles
Electronic Lien (E-Lien)

Service Provider System Specification Document

BMV ELT Program – DPPA Information Access Agreement

Indiana Bureau of Motor Vehicles

Vehicle and driver information shall be accessed and used to process transactions in relation to entities lien and titling interests by ______________________________ (“Lienholder”)

Information and records obtained from the Indiana Bureau of Motor Vehicles (“BMV”) are subject to the restrictions imposed by federal and state privacy protection laws. BMV records involving personal information (as defined by IC 9-14-6-6) are protected under Indiana law and the federal Driver Privacy Protection Act (DPPA), 18 USC § 2721 et seq.

Lienholder understands that misuse of BMV records for non-permitted purposes may result in termination of Lienholder’s access to BMV systems. At its discretion, BMV may terminate or cause to be terminated individual user access in the event an agent, employee, contractor, or any other Lienholder representative accesses or uses BMV data for any reason outside the scope of Lienholder’s business operations or for any other reason it deems necessary. Lienholder acknowledges that BMV, at any time and without advance notice, may revoke any information access and use privileges.

Lienholder shall indemnify and hold harmless BMV and its officers, agents, and employees from any and all claims, actions, damages, or losses which may be brought or alleged against BMV, its officers, agents, or employees for unauthorized disclosure of information, errors or omissions, or delays, or from equipment, software or communication failures which result solely from actions of such party under this agreement. Lienholder certifies that users will only access and use records obtained from BMV in full compliance with the law.

______________________________________ ____________________
Representative Signature Position

______________________________________ ____________________
Print name Date