

Recipient's Employees Code of Conduct Regarding Access to and Release of Information

PART 1

Preamble

This Code is intended to:

- Support a culture that values professionalism, integrity, honesty, fairness and respect for Information released to **your** Employer by the Registrar of Motor Vehicle Services of Alberta (“Registrar”).
- Educate and promote a secure environment for requesting, releasing, using, maintaining, processing, and destroying confidential Information shared by the Registrar with **your** Employer in accordance with specific legislated authorities.

This Code is distinct from the *Registry Agent Employees Code of Conduct* or other codes of conduct and ethics established by **your** Employer or any professional regulatory body whose member **you** may be. This Code is not intended to substitute for these codes, rather to complement other codes of conduct and ethics **you** must adhere to.

As Employee of a Recipient who has access to Protected Information **you** must read, understand, and commit to this Code by signing the *Code of Conduct Acknowledgement*.

Policy

Protecting the personal information of Albertans is a top priority for the Government of Alberta. To protect the privacy of Albertans and the business interest of entities while permitting authorized entities to continue to access Information, the Registrar regulates the request, release, use, maintenance, processing, and destruction of driving and motor vehicle information.

PART 2

Legislative Framework

Information on the Registrar's motor vehicle information system (MOVES) is collected under the Alberta *Freedom of Information and Protection of Privacy Act* (FOIP) for *Traffic Safety Act* (TSA) purposes. Motor Vehicles Registry information is collected and compiled for the purpose of identifying licensed operators and registered owners of motor vehicles to ensure responsibility and accountability for their actions with respect to motor vehicles. Once in Registrar's Office, the information is exempted under FOIP.

Access to Motor Vehicle Information Regulation (AMVIR)

Personal driving and motor vehicle information is defined in the TSA. Access to and the release of this Information is governed by the Access to Motor Vehicle Information Regulation (AMVIR). Other motor vehicle information may be released under Policies or Registrar's discretion.

Having access to the information of another person **your** Employer must ensure the confidentiality and security of Protected Information from the moment Information was released by the Registrar up to the moment the Protected Information was destroyed. Information is released in a protected environment governed by agreements. Depending on the situation, Protected Information may be disclosed in Court only.

As privacy legislation, AMVIR is purpose driven. To obtain Information directly from the Registrar **your** Employer had to declare a valid purpose (for which it was already pre-approved by the Registrar). Information released by the Registrar for a specific purpose **cannot be used for other purposes**. In addition **your** Employer may have obtained Protected Information indirectly, from a client under the agreement-based Third Party Model (TPM) implemented by the Registrar.

Consequently, **you** should understand the purpose declared by **your** Employer to obtain Information. If **your** Employer receives Protected Information indirectly, under TPM **you** need to know the purpose for which the Information was obtained by the original Recipient and the constraints imposed by the service **your** Employer is authorized to provide to that client under the TPM.

Agreement

Before requesting or being transferred motor vehicle information **your** Employer had to apply for, and sign an Agreement with the Registrar. Depending on the declared type of business and uses of information, **your** Employer has been pre-approved for different motor vehicle information products and AMVIR purposes. Your Employer may be a Valid Purpose Holder (VPH) under AMVIR or act as a Third Party Service Provider (TPSP) to a VPH. The Agreement between **your** Employer and the Registrar regulates the request, release, use, maintenance, processing, and destruction of Protected Information and clarifies the role **your** Employer has under AMVIR. **Your** Employer must provide to you the information **you** require to understand and comply with the Agreement signed with the Registrar.

Code is part of Policies

This Code is published on the Registrar's website. Furthermore, the Code is part of the Policies referred in the Agreement between **your** Employer and the Registrar.

Application of the Code

1. This Code and any subsequent versions published on the Registrar's website come in full force and apply to **you** 30 days after published on Registrar's website. The version and the date the Code was published on the Registrar's website are embedded in the footer of the Code.
2. As an Employee having access to Protected Information, this Code applies to **you** from the moment **you** had access to Protected Information regardless of the role **your** Employer has under AMVIR, if **you** have read or not read this Code, the

applicable legislation, the Agreement, the Policies or if **you** have signed or not the *Code of Conduct Acknowledgement*.

3. By signing the *Code of Conduct Acknowledgement* you agree to consult Registrar's website at least one time per month, to read and comply with any changes in the Code, applicable legislation, or Policies, and to be bound by the current version of the Code published on the Registrar's website.

PART 3

Definitions

In this Code:

“Administrative Suspension” means “Administrative Suspension” as defined in the Agreement between **your** Employer and the Registrar.

“Agreement” means a contractual relationship established between the Registrar and **your** Employer related to the request, release, use, maintenance, and destruction of Alberta Motor Vehicles Registry information.

“Authorized Officer” (AO) means an officer of the Recipient that was properly authorized under a specific AMVIR file and includes the “Authorized Signing Officer (ASO)” and the “Contact Person (CP)” as these are defined under the AMVIR Agreement between **your** Employer and the Registrar.

“Code” means this Code of Conduct.

“Employee” means an individual that is subject to the will and control of the Recipient for whom the services are performed, both as to what is to be done and the manner in which it is to be accomplished, and who has agreed by contract to perform specified services for the Recipient in exchange for money but does not include a contractor, consultant, permatemp, agent, or the employees of a Third Party Service Provider (TPSP).

“Employer” means a Recipient that pays a wage or fixed payment to an individual (Employee) in exchange for the services of such individual and has legal control of the payment of wages of the individual.

“Information” means Information as defined in the Agreement between **your** Employer and the Registrar.

“Policies” means the policies, policy directives, pre-approved forms, and user guides (including this Code of Conduct) related to Employer's Agreement that the Registrar may adopt and publish on the Registrar's website. Notice of any change in the Policies will be deemed to be given 30 days after it has been published on the Registrar's website.

“Protected Information” means information in any electronic, written or other form that may include, but is not limited to:

- (i) Information released by the Registrar following a Request from **your** Employer
- (ii) information obtained by **your** Employer using Information released by the Registrar that could not have been obtained without Information released by

the Registrar (e.g. a phone number obtained using the physical address released by the Registrar) and which if released may:

- (A) be harmful to business interests of a third party;
- (B) affect the privacy of an individual; or
- (C) permit the identification of an individual.

(iii) information obtained by **your** Employer indirectly, from another Recipient under the Third Party Model (TPM).

“Recipient” means a party that has entered in an Agreement with the Registrar for the purpose of obtaining Alberta Motor Vehicles Registry information. This Code applies to **you** if **your** Employer has entered into an Agreement with the Registrar.

“Registrar” means the Alberta Registrar of Motor Vehicle Services in accordance with Part 5, Division 1.1 of the *Freedom of Information and Protection of Privacy Act*.

“Request” means the request for release of Information made by the Recipient as defined in the Agreement between the Recipient and the Registrar.

“Third Party” means Third Party as defined in the Agreement between the Recipient and the Registrar.

“Third Party Model” (TPM) means a process implemented by the Registrar ensuring that any organization that uses Protected Information to providing a specialized services to a Valid Purpose Holder can be hold accountable for the use, maintenance, and destruction of the Protected Information.

“Third Party Service Provider” (TPSP) means a Third Party having a valid Agreement with the Registrar, an active Personal Unique Access Number (PUAN), and that provides specialized services to original Recipients (services the TPSP had declared to the Registrar when they have applied for an Agreement).

“Valid Purpose Holder” (VPH) means a person who has a valid purpose under legislation to request Information under AMVIR.

“**You**” and “**your**” means all individuals employed by the Recipient who have access to Protected Information.

PART 4

Recipient Employee Responsibilities under the Code

A. Understanding the regulatory framework

Depending on situation, **your** Employer may be governed by specific privacy legislation that **you** should be aware of. In addition, when **you** use Alberta motor vehicle information **you** must understand how AMVIR applies to **your** specific situation.

Before **you** make a Request for Information or before **you** use Protected Information **you** must understand the regulatory framework that applies to **your** specific situation. The AMVIR legislative framework is created by Alberta *Freedom of Information and Protection of Privacy Act* (FOIP), Alberta *Traffic Safety Act* (TSA) and the Access to Motor Vehicle Information Regulation (AMVIR). Other acts, enactments or arrangements of Canada or Alberta may apply in specific situations (for example, Alberta

Operator Licensing and Vehicle Control Regulation or Alberta Civil Enforcement Regulation). **You** can access and read AMVIR directly from Registrar's website or from Alberta Queen's Printer.

Under AMVIR, the Registrar publishes *Registrar's Decisions: Notifications* (RDNs). These are incremental decisions. **You** must read RDN 01/2004 and any subsequent RDN that would apply to **your** specific situation. **You** can access all RDNs from Registrar's website.

The [Access and Release of Motor Vehicle Information Policy](#) governs the request, release, use, maintenance, destruction, and disclosure of personal driving and motor vehicle information. It applies to all recipients of Information and is published on the Registrar's website. **You** must read and understand this policy.

The Registrar may publish, on the Registrar's website, pre-approved forms, guides, manuals, or interpretative notices. These forms, manuals, guides, and interpretative notices are reviewed for compliance under FOIP, TSA, and AMVIR and become mandatory and part of the Policies 30 days after being published. **You** must use the mandatory forms published and read and understand the guides and interpretative notices that would apply to **your** specific situation.

From time to time, the Registrar may publish Tip Sheets and Frequently Asked Questions (FAQs). **You** must read and understand the Tip Sheets and FAQs that would apply to **your** specific situation.

When **you** receive service through Alberta Registry Agents, **you** need to be aware that they are restricted in the type of service they can provide to **you**. Registry Agents act as both service providers and gate keepers. They protect the security and confidentiality of the information collected and maintained in MOVES. Consequently, they are governed by Registry Agent agreements, the *Registry Agent Motor Vehicles Policy*, and *User Guides*. **You** need to understand and respect their limitations and responsibilities, provide the supporting documents they may request, and avoid making unreasonable requests.

Under AMVIR **your** Employer may be authorized to request Information under one or multiple AMVIR Agreements. **You** need to know the file number of the specific Agreement under which **you** request Information and **you** must provide this number in **your** Request for Information.

You need to be aware that under AMVIR, **your** Employer is responsible for the validity of each and every Request made to the Registrar. Consequently, before **you** make a Request to the Registrar **you** must understand the AMVIR purpose under which the Request is made. **You** must ensure that any intended use is consistent with the declared purpose and that all documents required to support the Request are in compliance with the requirements of AMVIR, RDNs, the Agreement between **your** Employer and the Registrar, and all Policies.

If **you** are transferring information to a TPSP or **you** obtain motor vehicle information from the original Recipient **you** need to understand TPM and **your** duties and responsibilities under this model.

Information should be requested from the Registrar as near as possible to the moment in time when **you** require such information. A new Request for Information is required if

you need to make a decision or take action using Information (for example serve documents on a defendant) if more than 60 days have passed from the moment the Information was first released by the Registrar.

If **you** have difficulties understanding the regulatory framework or **you** are uncomfortable with **your** specific role under AMVIR **you** should request further clarifications from **your** Employer.

Each Recipient must provide to the Registrar the name and contact information of an Authorized Signing Officer and of a Contact Person. These individuals are encouraged to contact Data Access and Contract Management Unit (DACMU) to obtain any information **you** require for compliance under AMVIR. **You** need to know who are the Contact Person and the Authorized Signing Officer for **your** Employer.

If **you** are the Contact Person, **Authorized Officer** and/or the Authorized Signing Officer of **your** Employer **you** need to ensure that the Registrar has correct information about **your** Employer. Under Agreement, **you** are responsible to keep the Registrar informed about any change in contact information or status of **your** Employer. Using the Administrative Suspension, the Registrar could suspend access if it is not informed about changes relevant to the Agreement.

B. Disclosure vs. Release

You need to be aware about the meaning of disclosure and release under AMVIR. Normally the Registrar **releases** Information to the Recipient in a secure environment that is controlled by Agreement. Under AMVIR the Registrar agrees to share the Information for specific purposes and uses only. **You** cannot use Protected Information for any other purposes than those declared when the Information was requested.

A Recipient may request Information specifically for court purposes. The Information could be requested to serve documents, in preparation for court proceedings, or to be disclosed in Court. Only printed reports and Confirmation Letters released through an Alberta Registries agent can be used to disclose information in Court. If **you** need to disclose Information in Court, **you** must request a product that discloses only the Information required for that case.

Unless disclosed in Court, the Registrar continues to be the custodian of the Information shared with a Recipient. The Registrar may monitor the use of Protected Information or conduct audits and investigations to ensure that the Protected Information continues to be stored, used, maintained, released, disclosed, or destroyed appropriately.

C. Confidentiality of Protected Information

As Recipient's Employee, **you** must understand and comply with any confidentiality clause in the TSA, AMVIR, the Policies, and the Agreement between **your** Employer and the Registrar.

As a general approach, **you** are not to discuss, release, transfer, or disclose any Information or Protected Information obtained directly from the Registrar or indirectly from an original Recipient except to:

- An Alberta Registries officer or Registry Agent clerk on a need to know, file-related base when that individual is providing service to **you**;

Access to Motor Vehicle Information Regulation (AMVIR)

- An Alberta Registries auditor or investigator conducting a specific audit or investigation;
- Another Employee of **your** Employer on a need to know, file-related base if that Employee has been authorized and trained appropriately by **your** Employer and has signed a *Code of Conduct Acknowledgement*;
- An Employee of a TPSP providing service to **your** Employer under TPM if the TPSP has a valid AMVIR Agreement with the Registrar and that Employee of the TPSP has been authorized by **your** Employer;
- An Employee of the original Recipient if **your** Employer uses the TPM to provide service as a TPSP to the original Recipient and that Employee of the original Recipient has been authorized by their Employer;
- A Law Enforcement Agency in Canada if that Law Enforcement Agency is conducting a specific investigation and **you** have notified **your** Employer and the Registrar before Protected Information is released, or as soon as practicable;
- Any party if the Protected Information is required to be disclosed under court order or other lawful compulsory process compelling disclosure to such party if **you** have notified **your** Employer and the Registrar before Protected Information is released, or as soon as practicable, of a court order or other lawful compulsory process compelling such disclosure.

If **you** have been approved for Direct Access in MOVES **you** are not permitted to use the display features to browse for information except on a need to know, file-based approach. **You** should know the restrictions imposed on **your** access and **you** must comply with all rules about browsing and printing information.

You must take all reasonable steps to safeguard personal information to ensure that unauthorized persons will not make any unauthorized copies of personal information.

You must notify the Registrar immediately of any unauthorized or inappropriate form of disclosure, use or possession of Information or Protected Information by any person and promptly furnish the Registrar with full details of such unauthorized collection, disclosure, use or possession to the extent known.

If **you** have difficulties to understand the specific confidentiality conditions **you** are required to comply with or **you** are uncomfortable with the way Protected Information is handled **you** should seek further clarifications from **your** Employer.

D. Confidentiality of Personal IDs and Passwords

Your Employer may have been approved for different purposes, different release channels, and different products under specific agreements. Each release channel has different delivery models and specific IDs, and or passwords. To request information **you** need to be aware about the specifics of the release channel **you** are using and comply with all requirements.

Personal Unique Access Number (PUAN)

The Personal Unique Access Number (PUAN) is a confidential unique ID assigned to **your** Employer for a specific Agreement. Only authorized Employees should know and use the PUAN to request Information in the office of a Registry Agent. **You** should not

use the PUAN without appropriate delegation from **your** Employer. **You** are not permitted to use the PUAN after **your** employment is terminated or **your** role changes.

You must maintain the confidentiality of the PUAN. To further protect the confidentiality of the PUAN **you** need to know the Agreement file number. Use the Agreement file number instead of the PUAN when **you** contact DACMU or in any Request. When **you** request information as a 'walk-in' client through a Registry Agent **you** need to know the PUAN and provide it to the Registry Agent clerk with a letter of authorization from **your** Employer. If **you** have a billing account with one Registry Agent, they are permitted to store the PUAN associated to the relevant file number. This is necessary to permit them to conduct searches when they provide service by fax.

Other System User IDs

You may have been assigned other System User IDs depending on the type of access your Employer has been approved for. These IDs are managed by Alberta Registries and/or our IT Service Providers. The System User ID may be associated to an Agreement or may be directly associated to **you**. **You** are not permitted to use any System User ID and/or associated password after **your** employment is terminated or **your** role changes.

Only authorized Employees should know and use the IDs associated to an Agreement. **You** should not use these IDs without appropriate delegation from **your** Employer. **You** must protect the confidentiality of the password.

If **your** Employer has been approved for Direct Access and **you** have been issued an individual MOVES ID, **you** are not permitted to share this ID with other individuals. **You** must protect the confidentiality of **your** password.

E. Maintaining Information and Supporting Documents

Your Employer must preserve supporting documents for auditing and investigation purposes. Furthermore, **your** Employer must respect specific conditions about databasing, maintaining logs, destruction of information. **You** must understand and apply consistently these rules.

Specifically, **your** Employer must maintain logs listing all employees, collaborators, or subcontractors having access to Protected Information, the type of Information, the purpose, use, and type of access.

If **you** have difficulties to understand the specific requirements **you** are required to comply with or if **you** are uncomfortable with the way relevant documents are handled **you** should seek further clarifications from **your** Employer.

F. Electronic Exchange of Information

More and more processes move towards electronic storage, processing, and exchange of information. However, technology solutions are not always secure and could even represent a breach under Agreement. Consequently before storing, processing, and exchanging Protected Information in electronic form **your** Employer is required to contact the Registrar and ask for clarifications, understand the limitations and risks associated, and clarify any potential conflicts or risks.

Access to Motor Vehicle Information Regulation (AMVIR)

E-mail has become a pervasive way of exchanging information. However, to protect privacy and the security of data **you** cannot use e-mail to request or receive Information from Alberta Registry Agents or a TPSP.

If **you** use electronic exchange of information (for example, if **your** Employer has been approved for Direct Access or Batch Access) **you** need to comply with all technical requirements imposed by the Registrar. Furthermore, **you** need to clarify and comply with any technical issues before making any access if **your** Employer has been approved for mobile access.

Under AMVIR, **your** Employer is responsible for any security or privacy breach regardless if this is due to a service provider failure.

If **you** have difficulties in understanding the specific requirements **you** are required to comply with or if **you** are uncomfortable with the way electronic information is handled **you** should seek further clarifications from **your** Employer.

G. Telephone Communication

You should never communicate Protected Information over the phone when **you** cannot establish the identity of the other party. Furthermore, **you** must take any necessary precaution to avoid the risk that unauthorized persons may overhear **you** when Protected Information is referred during telephone conversations.

H. Using Fax Machines

When faxing, **you** must ensure that the fax is situated in a secure area where **you** can preserve the confidentiality of the Protected Information. If **you** make requests and receive Information by fax from an Alberta Registry Agent, **your** Employer is required to enter into a billing agreement with the Registry Agent. With this occasion **you** must exchange the secure fax numbers that can be used to fax Information.

When you send or receive Protected Information by fax, **you** need to ensure that the fax is directed to the correct person and fax number.

You need to read, understand, and comply with the *OIPC Guidelines for Facsimile Transmission* published on the website of the Office of the Information and Privacy Commissioner of Alberta.

I. Storing and Using Protected Information

Your Employer must inform the Registrar about any physical location where Protected Information is stored and used. **You** cannot use a TPSP to store Protected Information.

When **you** use a TPSP under the TPM, they may use or store Protected Information only at a location they have declared in their Agreement with the Registrar.

If there are changes in the physical addresses where **you** store or use Protected Information, your Employer must communicate this information immediately to the Registrar by preparing and submitting an updated Schedule E to the Agreement.

To minimize the risk of any security and privacy breach **you** are required to ensure that Protected Information and supporting documents are stored in a secure environment. If

you are uncomfortable with the way Protected Information is stored, **you** should seek further clarifications from **your** Employer.

J. Transporting Protected Information

You must take precautions to avoid the risk of unauthorized disclosure when transporting Protected Information. Protected Information should be kept in sealed envelopes and safeguarded at all times.

PART 5

Penalties and Consequences

Your Employer is responsible to the Registrar for any breach under the Agreement including any lack of compliance with this Code. However **you** must read understand and comply with this Code.

Recipient's Employees that do not comply with this Code may be subject to disciplinary action by the Employer as well as temporary or permanent suspension of access to Alberta Registries information. Finally, for significant breaches or fraudulent activities the Registrar could seek legal action against the Employer and/or the Employee for such breaches or activities.