Schedule D – Employee's Pledge of Confidentiality

Pursuant to an Information Sharing Agreement between Manitoba Trucking Association and The Manitoba Public Insurance Corporation ("**Manitoba Public Insurance**"), dated the ___ day of _____, 2021 (the "**Agreement**").

I UNDERSTAND THAT:

A1. As an employee of _____ (my "employer"), I may have access to Information provided by Manitoba Public Insurance for the purpose of checking the licence status of an individual in accordance with Paragraph E of the Agreement (the "**Authorized Purpose**").

A2. "**Information**", for the purposes of the Agreement and this Pledge of Confidentiality, means "personal information" as defined by *The Freedom of Information and Protection of Privacy Act* (C.C.S.M. c. F175), as amended, which is provided by Manitoba Public Insurance to the Recipient under the Agreement.

I UNDERTAKE AND AGREE THAT:

A3. I will not collect, use, disclose, alter, retain or destroy the Information for any purpose except for the Authorized Purpose and in accordance with the requirements in the Agreement and any applicable policies and procedures of my employer.

A4. I will treat all Information to which I have access under the Agreement as strictly confidential and will use the Information solely for the Authorized Purpose and for no other purpose.

A5. I will limit my access to and use of the Information to information that I am authorized by my employer to use and that I need to know to carry out my employment responsibilities.

A6. I will not remove any Information, or any copy of the Information, in any form or medium, from the premises of my employer.

A7. I will not retain or make unauthorized copies of any Information, in any form or medium.

A8. I will not modify or alter any of the Information in any manner.

A9. I will not disclose any Information, in any form or medium, to any person, corporation, organization or entity, except as specifically authorized in Section 5.1 of the Agreement (a copy of this section is attached to this Pledge of Confidentiality).

A10. I will not sell or disclose any Information for consideration or exchange any Information for any goods, services or benefits.

A11. I will comply with the requirements respecting protection of information and the security arrangements contained in Article 9.0 of the Agreement (a copy of that article is attached to this Pledge of Confidentiality) as directed by my employer through its policies or procedures.

I acknowledge that failure to comply with the undertakings in this Pledge of Confidentiality may result in my no longer having access to the Information, my being prohibited from providing services with respect to the Authorized Purpose, and in other disciplinary action or proceedings being taken against me by my employer.

_____	_____
Name (Printed)	Position
_____	_____
Signature	Date

The following provisions of the Agreement are attached to the Employee's Pledge of Confidentiality:

5.1 The Recipient shall take reasonable steps to ensure that their Authorized Employees keep the Information confidential. They shall not give access to or disclose, and shall not permit anyone to give access to or disclose, the Information in any manner, form or medium to any person, corporation, business, agency, organization or entity except as follows:

a) to Manitoba Public Insurance or its Representatives for the purposes of this Agreement, including for the purpose of monitoring compliance with this Agreement and for audits, investigations and reviews respecting this Agreement;

b) to an external auditor with the consent of Manitoba Public Insurance;

c) where disclosure is required by legislation;

d) where disclosure is required by an order of a court, person or body with jurisdiction to compel production of the Information; and

e) where disclosure is required to comply with a rule of court that relates to the production of the Information.

9.1 The Recipient shall adequately protect the Information from risks, including risks of use, access, disclosure and destruction which are not authorized by this Agreement.

9.2 In addition to complying with the requirements and obligations in this Agreement, the Recipient shall comply with any additional reasonable requirements established by Manitoba Public Insurance from time to time to protect the Information.

9.3 The Recipient shall put in place sufficient security arrangements, including administrative, technical and physical safeguards that ensure the continued confidentiality and security of the Information, and that protect the Information against risks of cyberattacks and against risks of use, access, disclosure or destruction which are not authorized under this Agreement. These security arrangements shall take into account the sensitivity of the Information and the medium in which the Information is stored, handled, transmitted or transferred.

9.4 Without limiting Section 9.3 of this Agreement, the security arrangements which the Recipient puts in place shall, at a minimum, include the following:

a) The Recipient may maintain the Information in electronic form on its computer network provided that:

(i) the computer network is a secured against cybersecurity attacks and is accessible only to the Recipient and it’s Authorized Employees. In

particular, the Recipient shall not allow access to the database even for demonstration purposes;

(ii) the Information is protected by user access credentials and strong passwords to prevent unauthorized access;

(iii) access to the user access credentials and strong passwords is limited to: (1) Authorized Employees who are physically present in the offices of the Recipient and who need access to the Information to carry out the Authorized Purpose, and (2) personnel or contractors of the Recipient who provide technical support services to the Authorized Employees, including its Information Security Service Provider, in compliance with Section 8.0;

(iv) the Recipient keeps an electronic record of every successful and unsuccessful attempt to gain access to the Information, and whether authorized or not;

(v) the Recipient regularly reviews the electronic record to detect any security breaches; and

(vi) the Information is protected via encryption when in transit and at rest.

(vii) the computers on which the Information is stored must have encryption at rest enabled.

b) An established and formalized best practices in operating and managing its infrastructure and services that includes asset management, backup and restore processes and procedures, change management, configuration management, and release management processes;

c) Reasonable security practices and protections in place to protect against internal and external threats, in ways that will not impact the confidentiality, integrity, and the availability of the Information. Such protections must be augmented with timely patching of systems, conducting vulnerability assessments and penetration testing on a regular basis, and timely remediation of identified vulnerabilities as per industry best practices;

d) No other collection or database of the Information, in any form or medium, shall be maintained or created by the Recipient; and

e) When disposing of any media containing a record of the Information, the Recipient shall erase or destroy any Information contained on the media in a manner which adequately protects the confidentiality of the Information and in accordance to Section 10.

f) A formal security and background screening process for all its Representatives (including the requirement for its Representatives to sign confidentiality agreements);

9.5 The Recipient has established written information security policies and standards respecting the use of, access to, and disclosure, protection and destruction of the Information as well as identifying, recording, protecting against and correcting security breaches which are consistent with and reflect the requirements of this Agreement. Such information security policies and standards will be communicated to its Authorized Employees. The Recipient shall diligently enforce these policies and standards through Technical, administrative, organization and / or physical mechanisms.

a) The Recipient shall provide a copy of their written policies or procedures if requested by Manitoba Public Insurance.

b) The Recipient shall provide training to its Authorized Employees on its information security, privacy and other relevant policies and standards for handling the Information.