Memorandum of Understanding for Remote Access made effective the day of 2016.

BETWEEN:

THE GOVERNMENT OF MANITOBA,
as represented by the
Fire Commissioner
Office of the Fire Commissioner
Manitoba Labour and Immigration,

(called "**Manitoba**")

-and-

Fire Chief
of the Fire Department.
pursuant to the laws of Manitoba

(called the "**Recipient**")

WHEREAS:

A. Manitoba maintains a computer application know as the Fire Department Management (FDM) System ("**System**");

B. The Recipient has requested remote access to Manitoba's System ("**Remote Access**") through either Dial-up or Virtual Private Network access services. For the purposes of this Memorandum of Understanding ("**MOU**"), "**Dial-up**" access refers to a means by which the Recipient and its authorized officers, employees and agents may gain access to Manitoba's System via a public switched network. "**Virtual Private Network**" access refers to a means by which the Recipient and it authorized officers, employees and agents may gain access to Manitoba's System using the internet ;

C. Before providing the Recipient with Remote Access to Manitoba's System, Manitoba requires the Recipient to agree to and be bound by Manitoba's Protection of Personal Information and Security Safeguards and Measures requirements, copies of which are attached hereto as Schedules "A" and "B" respectively.

NOW THEREFORE, this MOU sets out the terms and conditions pursuant to which the Recipient will be entitled to access Manitoba's System using either Dial-up or Virtual Private Network access.

1. This MOU will be effective as of the date noted above and shall continue until terminated by either party in accordance with paragraph 10 hereof, (the "**Term**").

2. Manitoba hereby grants the Recipient and its designated officers, employees and agents (each a "**System User**") access to portions of the System via either Dial-up or Virtual Private Network access.

3. Where the Recipient will be entitled to use Dial-up services in order to access Manitoba's System, then each System User who requires access to the System will require a password and user identification.

4. Where the Recipient will be entitled to use Virtual Private Network services in order to access the System, then each System User will be provided with a security token whose security identification number changes every sixty (60) seconds. In order to gain access to the System, each System User will require a personal identification number (PIN), user identification and security token.

5. System Users will be entitled to access the system 24 hours a day, 7 days a week, however System support will only be available Monday to Friday, from 8:30 a.m. to 4:30 p.m., excluding statutory holidays. It is understood that access during these times may be disrupted due to scheduled system maintenance or due to circumstances beyond the control of Manitoba. While Manitoba will use reasonable efforts to ensure that interruptions of access to the System will be limited, in no event will the Recipient or any System User hold Manitoba responsible for any service disruption.

6. While accessing the System, the Recipient agrees that it will at all times comply with, and will ensure that all System Users will at all times comply with:

    (a) the Protection of Personal Information requirements detailed in Schedule "A";

    (b) the Security Safeguards and Measures detailed in Schedule "B"; and

    (c) such further rules or direction made or given by Manitoba to ensure System security,

    (collectively the "**Security Requirements**").

7. The Recipient will confirm in writing to Manitoba the individual who is responsible for system security for that organization, ("**Security**

Manager"). The Security Manager, working with Manitoba's security contact, will be responsible for ensuring that the Recipient is complying with the Security Requirements. The Recipient must immediately notify Manitoba in the event of change of the Security Manager.

8. The Recipient must immediately notify Manitoba in the event of change of the Fire Chief.

9. The Recipient acknowledges and agrees that access to the System will be given to individual System Users and not to the Recipient itself. Each System User must not disclose any passwords needed to access the System, nor transfer any security hardware or software, including the security tokens, needed to access the System to any person or organization without the prior written approval of Manitoba. Each System User shall not record or share the passwords necessary to access the System, or allow access to any security tokens or passwords, in any manner which may allow unauthorized individuals or organizations to use them.

10. Manitoba shall have the right from time to time and upon reasonable notice, using either internal or external auditors, to inspect and audit the relevant records, premises and equipment of the Recipient to ensure compliance with the Security Requirements and this MOU. In the event of any failure by the Recipient or any System User to comply with the Security Requirements or this MOU, which default is not remedied to the satisfaction of Manitoba, then Manitoba may immediately terminate the Recipient's and each System User's access to the System, without any further notice being required. In addition, either party is entitled to terminate this MOU and all System Users' access to the System upon thirty (30) days' advance written notice to the other party.

11. In addition to Manitoba's rights under paragraph 10 hereof, the Recipient agrees that it will indemnify and hold harmless Manitoba, and its respective officers, employees and agents, from any loss, damage, costs, expenses or liability suffered or sustained by Manitoba or any third parties, relating to the Recipient's or any System User's access to the System pursuant to this MOU. This obligation shall continue notwithstanding the termination of this MOU.

12. In the event of termination of this MOU in accordance with paragraph 10, then the Recipient shall immediately return, and cause each of its System Users to immediately return, all software and hardware provided by Manitoba and which permitted Remote Access to the System, including any and all security tokens. In addition, the Recipient agrees to comply with the Disposal of Records of

Confidential Information as detailed in the attached Security Requirements, which obligations shall survive the termination of this MOU.

13. Any notice or other communication to the Recipient under this MOU shall be in writing and shall be delivered personally to the Recipient or an officer or employee of the Recipient, or sent by registered mail, postage prepaid, or by facsimile transmission to:

Fire Chief
of the Fire Department

Address:

Phone #:
Fax #:

14. Any notice or other communication to Manitoba under this MOU shall be in writing and shall be delivered personally to the Manitoba or an officer or employee of the Manitoba, or sent by registered mail, postage prepaid, or by facsimile transmission to:

Office of the Fire Commissioner
508 – 401 York Avenue
Winnipeg, MB R3C 0P8
(204) 945-3322

15. This MOU shall be interpreted, performed and enforced in accordance with the laws of Manitoba.

16. No amendment or change to, or modification of, this MOU shall be valid unless it is in writing and signed by both parties.

This MOU has been executed by the Assistant Deputy Minister, Immigration and Multiculturalism Division, Manitoba Labour and Immigration on behalf of the Government of Manitoba and by the Recipient (by its duly authorized representative) on the dates noted below.

SIGNED IN THE PRESENCE OF:

FOR THE GOVERNMENT OF MANITOBA

_____
WITNESS

_____
Fire Commissioner
Office of the Fire Commissioner
Manitoba Labour and Immigration
(or designate)

Date: _____

FOR THE RECIPIENT

_____
Per: Fire Chief
of the Fire Dept.

_____
WITNESS

Date: _____

I have the authority to bind the Recipient

SCHEDULE "A"
PROTECTION OF PERSONAL INFORMATION
(with Schedule "B" – Security Safeguards and Measures)

This is Schedule "A" to a Memorandum of Understanding between **the Government of Manitoba ("Manitoba") and Fire Chief [ ] of the [ ] Fire Department. (the "Recipient")** made effective [ ], 2016, (the "MOU").

Definition of personal information

1.01 In this Schedule and in the MOU, "personal information" has the meaning given to that term in *The Freedom of Information and Protection of Privacy Act* of Manitoba (C.C.S.M. c. F175), and includes:

(a) personal information about an identifiable individual which is recorded in any manner, form or medium; and

(b) personal health information about an identifiable individual as defined in *The Personal Health Information Act* of Manitoba (C.C.S.M. c. P33.5).

These statutory definitions are attached at the end of this Schedule.

1.02 The requirements and obligations in this Schedule:

(a) apply to all personal information received, collected or otherwise acquired by the Vendor in the course of carrying out its obligations under the MOU, in whatever manner, form or medium;

(b) apply whether the personal information was received, collected or acquired before or after the commencement of the MOU; and

(c) continue to apply after the termination or expiration of the MOU.

Collection of personal information by the Recipient

1.03 The Recipient recognizes that, in the course of carrying out its obligations under the MOU, the Recipient may receive personal information from Manitoba and may collect, acquire, be given access to and may otherwise come into possession of personal information about individuals.

1.04 Where the Recipient receives, collects, acquires, is given access to or otherwise comes into possession of personal information, the Recipient must collect only as much personal information about an individual as is reasonably necessary to carry out the Recipient's obligations under the MOU.

1.05 Where the Recipient collects or acquires personal information directly from the individual it is about, the Recipient must ensure that the individual is informed of:

(a) the purpose for which the personal information is collected;

(b) how the information is to be used and disclosed;

(c) who in the Recipient's organization can answer questions the individual may have about his or her personal information; and

(d) his or her right of access to the information, as set out in the Recipient's policies under subsection 1.06 of this Schedule.

Access to personal information by the individual it is about

1.06 [Intentionally deleted].

Restrictions respecting use of personal information by the Recipient

1.07 (a) The Recipient must keep the personal information in strict confidence and must use the personal information only for the purpose of properly carrying out the Recipient's obligations under the MOU and not for any other purpose.

(b) The personal information shall be used solely by the Recipient personally, or (where the Recipient is a corporation, business, organization or other entity) by the officers and employees of the Recipient, except as otherwise specifically permitted by Manitoba in writing.

(c) The Recipient must:

(i) limit access to and use of the personal information to those of the Recipient's officers and employees who need to know the information to carry out the obligations of the Recipient under the MOU;

(ii) ensure that every use of and access to the personal information by the Recipient and by the authorized officers and employees of the Recipient is limited to the minimum amount necessary to carry out the obligations of the Recipient under the MOU;

(iii) ensure that each officer and employee of the Recipient who has access to the personal information is aware of and complies with the requirements, obligations and fair information practices in this Schedule; and

(iv) ensure that each officer and employee who has access to the personal information signs a pledge of confidentiality, satisfactory in form and content to Manitoba, that includes an acknowledgement that he or she is bound by the requirements, obligations and fair information practices in this Schedule and by the Recipient's security policies and procedures and is aware of the consequences of breaching any of them.

1.08 The Recipient must ensure that:

(a) no person can make unauthorized copies of the personal information;

(b) no person shall disclose the personal information except as unauthorized under subsection 1.10 of this Schedule; and

(c) no person can modify or alter the personal information in a manner which is not authorized.

1.09 The Recipient must not link or match the personal information with any other personal information, except where necessary to carry out the obligations of the Recipient under the MOU.

Restrictions respecting disclosure of personal information by the Recipient

1.10 The Recipient must not give access to, reveal, disclose or publish, and must not permit anyone to give access to, reveal, disclose or publish, the personal information to any person, corporation, business, organization or entity outside the Recipient's organization, except as follows:

(a) to Manitoba, and to Manitoba's officers, employees and agents, for the purposes of the MOU;

(b) to any person, corporation, business, organization or entity with the voluntary, informed consent of the individual the information is about;

(c) where the individual the information is about is a child under the age of 18 years, to the custodial parent or parents or to the legal guardian of the child, upon satisfactory proof of identity and authority, provided that the Recipient is of the opinion the disclosure would not be an unreasonable invasion of the child's privacy;

(d) where disclosure is required or authorized by legislation;

(e) where disclosure is required by an order of a court, person or body with jurisdiction to compel production of the personal information or disclosure is required to comply with a rule of court that relates to the production of the personal information; or

(f) where disclosure is necessary to prevent or lessen a serious and immediate threat to the health or safety of the individual the information is about or of any other individual or individuals.

1.11 Without limiting subsection 1.10 of this Schedule, the Recipient shall not:

(a) sell or disclose the personal information, or any part of the personal information, for consideration; or

(b) exchange the personal information for any goods, services or benefits; or

(c) give the personal information to any individual, corporation, business, agency, organization or entity for any purpose, including (but not limited to) solicitation for charitable or other purposes;

and shall not permit any of these activities to take place.

Protection of the personal information by the Recipient

1.12 The Recipient must protect the personal information by putting in place reasonable security arrangements, including administrative, technical and physical safeguards, which ensure the confidentiality and security of the personal information against such risks as use, access, disclosure or destruction which are not authorized under this Schedule. These security arrangements must take into account the sensitivity of the personal information and the medium in which the information of the personal information and the medium in which the information is stored, handled, transmitted or transferred.

1.13 Without limiting subsection 1.12 of this Schedule:

(a) the Recipient must ensure that:

(i) the personal information is accessible only to those of the Recipient's officers and employees who need to know the personal information to carry out the obligations of the Recipient under the MOU; and

(ii) the personal information is protected by a series of passwords to prevent unauthorized access and that access to and use of these passwords is limited to those of the Recipient's officers and employees who need to know the personal information to carryout the obligations of the Recipient under the MOU;

(b) the Recipient must comply with any regulations made, policies issued and reasonable requirements established by Manitoba respecting the protection, retention or destruction of the personal information, including, without limitation, the Security Safeguards and Measures identified in Schedule "B"; and

(c) the Recipient must provide training for its officers, employees, agents and subcontractors regarding the requirements in this Schedule and the Recipient's security policies and procedures.

****

Statutory definitions of personal information and personal health information

1. "**personal information**" means recorded information about an identifiable individual, including

    (a) the individual's name,
    (b) the individual's home address, or home telephone, facsimile or e-mail number,
    (c) information about the individual's age, sex, sexual orientation, marital or family status,
    (d) information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,
    (e) information about the individual's religion or creed, or religious belief, association or activity,
    (f) personal health information about the individual,
    (g) the individual's blood type, fingerprints or other hereditary characteristics,
    (h) information about the individual's political belief, association or activity,
    (i) information about the individual's education, employment or occupation, or educational, employment or occupational history,
    (j) information about the individual's source of income or financial circumstances, activities or history,
    (k) information about the individual's criminal history, including regulatory offences,
    (l) the individual's own personal views or opinions, except if they are about another person,
    (m) the views or opinions expressed about the individual by another person, and
    (n) an identifying number, symbol or other particular assigned to the individual.

2. "**personal health information**" means recorded information about an identifiable individual that relates to

    (a) the individual's health, or health care history, including genetic information about the individual,
    (b) the provision of health care to the individual, or
    (c) payment for health care provided to the individual,

    and includes

    (d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and
    (e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care for payment for health care.

    "**health care**" means any care, service or procedure

(a) provided to diagnose, treat or maintain an individual's physical or mental condition,
(b) provided to prevent disease or injury or promote health, or
(c) that affects the structure or function of the body,

and includes the sale or dispensing of a drug, device, equipment or other item pursuant to a prescription.

"**PHIN**" means the personal health identification number assigned to an individual by the Minister to uniquely identify the individual for health care purposes.

SCHEDULE "B"

SECURITY SAFEGUARDS AND MEASURES

This is Schedule "B" to a Memorandum of Understanding between **the Government of Manitoba ("Manitoba") and Fire Chief [ ] of the [ ] Fire Department. (the "Recipient")** made effective [ ], 2016, (the "MOU").

This Schedule contains the requirements and obligations of the Recipient and of the Recipient's Representatives to safeguard Manitoba's assets and Confidential Information.

For the purposes of this Schedule:

"Confidential Information" includes Personal Information and Personal Health Information as defined in Schedule "A" to the Services MOU, along with any 3rd party proprietary information or any other information that Manitoba identifies as confidential.

"Representatives" includes the Recipient's officers, employees, agents, business partners and subcontractors.

"Record" means a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records.

1. Technical Security

1.1. General System

The Recipient's information and communications systems must include reasonable hardware, software and procedural security control measures, acceptable to Manitoba, acting reasonably, designed to prevent the following:

(a) unauthorized access and systematic attempts to disrupt service;

(b) unauthorized changes to software and hardware components;

(c) propagation and execution of harmful code, including but not limited to computer viruses and worms; and

(d) unauthorized access to and disclosure of Confidential Information.

1.2. Individual Workstation

The Recipient's Representatives must have installed and operational the following security controls on their personal workstations:

(a) operating system and optional hard disk encryption password settings;

(b) a password protected keyboard/screen lock that is automatically activated by a period of inactivity of no more than twenty (20) minutes;

(c) encryption software acceptable to Manitoba capable of encrypting Confidential Information stored on the workstation; and

(d) a personal firewall and anti-virus program, acceptable to Manitoba, if the workstation is directly connected to any Manitoba network, the internet or to any external wireless local area network.

1.3. Encryption of Confidential Information

The Recipient's Representatives must encrypt all Confidential Information when:

(a) leaving the work area for the balance of the day;

(b) the Confidential Information is in transit; and/or

(c) the Confidential Information is being sent electronically (including, but not limited to, internet, email, FTP).

2. Physical Security

2.1. Offices and Work Areas

If the MOU permits the Recipient or its Representatives to maintain Confidential Information on the Recipient's or its Representatives' premises, then at all times access to such premises must be controlled. In addition:

(a) the individual in possession of the records must lock their office when they leave for the balance of the day; and

(b) where the individual in possession of the records cannot lock their office, when leaving for the balance of the day they must:

(i.) activate the password protected keyboard/screen lock;

(ii.) lock all records of Confidential Information that are being left on the premises in a secure desk, filing cabinet or room to which only authorized Representatives have access; and lock up their laptop in a similar manner or secure to a fixed object with a cable lock.

3. Disposal of Records of Confidential Information

3.1. Once the records of Confidential Information have been used for the purpose described in the MOU, or if requested by Manitoba or required by the MOU, then the Recipient must immediately destroy any and all copies of the Confidential Information, in all forms and mediums, and

must confirm in writing to Manitoba that such Confidential Information has been destroyed.

3.2. All records of Confidential Information must be destroyed in a manner that makes it impossible to read or reconstruct the information.

3.3. Paper Records

All paper records of Confidential Information must be shredded or otherwise destroyed in a manner acceptable to Manitoba. If the records are shredded, they must be cut in strips of one (1) centimetre wide or less, unless they are also cross-cut, re-shredded or mixed.

3.4. Electronic Records

3.4.1. Microfilm, microfiche, magnetic computer tapes, compact disks, diskettes, and other forms of electronic media must be incinerated or shredded using a commercial shredding operation acceptable to Manitoba.

3.4.2. Before disposal hard drives must be erased with a commercial disk eraser tool, acceptable to Manitoba, capable of writing to each sector a minimum of three (3) times. Drive formatting is not considered an acceptable method of disk erasure. Hard drives that fail and are not accessible must be physically destroyed and/or erased with commercial degaussing equipment.

4. Disaster Recovery and Records Backup

4.1. Disaster Planning and Recovery

The Recipient must have disaster planning and recovery plans in place, acceptable to Manitoba, acting reasonably, that have been tested for viability and documented to protect records against loss.

4.2. Data Backup

Unless otherwise provided for in the MOU, the Recipient must backup electronic records on a regular schedule, keeping the backup copies in a separate off-site storage area, which meets security, environmental and fire prevention and suppression standards acceptable to Manitoba.

5. Recipient Policies and Procedures

5.1. Written Policies and Procedures

The Recipient must have written security policies and procedures acceptable to Manitoba.

5.2. Representatives Awareness

The Recipient must make its Representatives aware of its written security policies and procedures and the Recipient's obligations under this Schedule.

5.3. Breaches of Security

In addition to other requirements identified in this Schedule, the Recipient's security policies and procedures must include provisions to:

(a) identify and record security breaches and attempted security breaches;

(b) take corrective action to address security breaches and attempted security breaches; and

(c) notify Manitoba immediately, in writing, of any security breach or attempted security breach involving Manitoba's Confidential Information and identify what steps are being taken to prevent a recurrence.

6. Inspections or Investigations by Manitoba

6.1. Right to Carry out Inspections or Investigations

Upon reasonable advance written notice, Manitoba may, using either internal or external auditors, carry out inspections or investigations of the Recipient's and its Representative's security practices involving Manitoba's Confidential Information, as Manitoba considers necessary to ensure the adequate protection of the information.

6.2. Cooperation by the Recipient

The Recipient and its Representatives must cooperate in any inspection or investigation carried out by Manitoba. In addition, the Recipient and its Representatives must permit access, at all reasonable times, to their premises, records and information in order to carry out such inspections and investigations and to ensure compliance with this Schedule.

6.3. Correction of Deficiencies

If an inspection or investigation identifies deficiencies in the Recipient's or its Representative's security practices which expose Manitoba's Confidential Information to risk of unauthorized disclosure, the Recipient must take reasonable steps, acceptable to Manitoba, to promptly correct the deficiencies.