Privacy Impact Assessment

Victoria Fire Department Mobile Data Terminals

PIA# 2015-008

Part 1 – General

Name of Department/Branch:	Victoria Fire Department		
PIA Drafters:	Rob Gordon, Douglas Carey, Katherine Wilson		
Email:	rgordon@victoria.ca	Phone:	250 361-0347
Program Manager:	Dan Atkinson, Victoria Fire Department		
Email:	datkinson@victoria.ca	Phone:	250 920-3369
PIA Drafter:	Katherine Wilson		
Email:	kwilson@victoria.ca	Phone:	250.361.0392

1. **Description of the Initiative**

The Victoria Fire Department (VFD) uses Mobile Data Terminals (MDT) to relay important property and contact information to Fire Suppression (Suppression) staff on route to an incident via a wireless tablet in each of the front line apparatus (Engines 1, 2, 3, Battalion 1, Rescue 1, and Ladder 1).

The MDTs use third party software FDM Mobile CAD (Computer Aided Dispatch) to push and display relevant property and contact information or transient data to the MDTs assigned to that incident; this information is only displayed on the tablets while the apparatus and its staff are actively assigned to an incident. Once the call is complete and the apparatus has returned to quarters, the information is no longer displayed on the device. No incident or contact information is stored to the device. No data is entered into FDM Mobile CAD using these devices.

The MDTs, like the mobile phones, are not assigned to any user and have no user account associated with them. As such, there is no email configured nor a PIN to access the device. In previous deployments and similar to most fire departments, a password or PIN on the device is disabled for operational efficiency and practicality purposes. The MDTs have the following asset tags registered with the City of Victoria: C02833, C02944, C02949, C02952, C02953, C02954, C02955.

From time to time, Suppression staff may remove the MDT from its lockable dock in the apparatus but not to take video or photographs for incident reporting or training purposes. Staff are instructed to use their City-issued mobile phones to take photographs or videos as the camera on the phone is better quality (8 megapixels vs. 3 megapixels).

2. **Scope of this PIA**

This PIA reviews VFD's MDTs for compliance with FIPPA's privacy provisions.

3. **Related Privacy Impact Assessments**

VFD Mobile Phone PIA

https://worksites.victoria.ca/sites/Teams/TeamTemplate/FireSupport/Team%20Documents/Mobile%20Phones/PIA%202015-008%20VFD%20Mobile%20Phones%20FINAL.docx

VFD Prevention Tablets PIA

https://worksites.victoria.ca/sites/Teams/TeamTemplate/FireSupport/Team%20Documents/Fire%20Prevention%20Units/PIA%202016%20VFD%20Prevention%20Tablets.docx

4. Elements of Information or Data

Property Contact information: the contact names and numbers for properties are displayed on the MDT while the apparatus is active on that incident. Once the apparatus status is set to Return to Quarters in Mobile CAD, the property and contact information disappears from the MDT.

Information related to single family dwellings is not maintained by the Victoria Fire Department. Mobile CAD also displays comments from Dispatch.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

FDM servers are hosted locally within the City of Victoria servers hosted in Victoria, BC. There is no access from outside Canada nor is information passed to any agency outside of Canada.

Back-up locations of personal information: Backup servers are hosted within the City of Victoria infrastructure. These storage locations are in Victoria, Canada. City of Victoria IT takes backups of its databases daily.

6. Data-linking Initiative*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The linkage purpose is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	When an apparatus is dispatched to an incident, property and building reference information for multiple occupancy, public assembly, commercial and industrial properties is displayed on the MDT.	Collection	26(c)
2.	The information is shared with other firefighters attending an incident	Use	*32(b)*
3.	The information is shared with other firefighters attending an incident	Disclosure	*33.2(a), 33.2(c)*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Apparatus doors are not locked and the MDT is stolen.	Lock the MDTs in the dock inside the apparatus. Key to mount lock	Low	Low

		will only be shared with VFD Suppression staff. Remotely wipe the device when determined to be lost/stolen. Data is gone from MDT once removed from an incident in the Mobile CAD application.		

10. Collection Notice

A collection notice is not required. Personal information is collected indirectly under section 27(1)(b) and 27(3)(c).

Part 3 – Security of Personal Information

***11.* Please describe the physical security measures related to the initiative (if applicable).**

The MDT is to stay locked in its lockable mount in the apparatus unless it is required outside of the apparatus. The key to unlock the device mount is stored in the concealed lock box on each apparatus to allow Suppression staff assigned to that apparatus to remove the MDT if required. A copy of the key is kept with the VFD Master Mechanic at the Firehall headquarters.

12. Please describe the technical security measures related to the initiative (if applicable).

Once the apparatus completes the call and returns to quarters, the incident information disappears from the MDT.

Security features for system maintenance, patch updates, synchronization:

- Only transitory data from FDM is only displayed to the MDT. No information is entered or stored to the device.
- If a device is stolen, then it can be remotely erased using InTune.
- Patch updates are done using InTune.

Transmission security:

- All communication is encrypted with SSL.
- All data stored on the device is also encrypted.
- All connectivity to City of Victoria servers must begin with a login, which creates a session.
- All API access is limited to sessions.
- Using static IP addresses for access to Mobile CAD application.
- Firewalls, DDoS protection, SSAE 16

13. Does your branch/department rely on any security policies?

Governance: VFD MDT users have been instructed not to use the mobile phone to take photographs or videos. Both the front and rear cameras have been disabled on the tablets.

Only approved staff are permitted to access data within FDM. These permissions are maintained by VFD and changes are made by IT as required. VFD has process and permissions in place to control access to personal information stored in FDM.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Personal information cannot be added or deleted in FDM using the MDT; data stored in FDM cannot be changed using the MDT and/or Mobile CAD. Personal information is only displayed on the device; no information is entered or stored.

15. Please describe how you track who has access to the personal information.

Only personal information required to assist with the incident is displayed on the MDT – property address and contact names and numbers. VFD keeps record of crew on duty and to which apparatus they are assigned. Only approved staff are permitted to access data within FDM. These permissions are maintained by VFD and changes are made by IT as required. VFD has process and permissions in place to control access to personal information stored in FDM.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

An individual's contact information is updated or corrected when VFD is requested to do so. Contact information is often updated following incident response, or provided during company inspections or pre-plan exercises. Personnel manually enter the information into the FDM database when they complete Incident Reports or enter inspection and preplan information, but this is done on their desktop device within the City of Victoria network, not using the MDT. Individual's information cannot be updated using the MDT. Sometimes during an active incident, Dispatch will update contact information from the caller directly into FDM.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.
No

Part 5 – Further Information

18. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

The information forms part of incident reports that are forwarded to the Office of the Fire Commissioner.

19. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

20. Will a personal information bank (PIB) result from this initiative?

No.

Part 6 – Privacy Officer Comments

1. Please advise the Privacy Officer whenever there are changes to the MDTs that may affect the collection, use or disclosure of personal information.

Part 7 – Program Area Signatures

Rob Gordon		April 20/16
Privacy Officer/Privacy Office Representative	Signature	Date
Dan Atkinson		April 18/2016
Program/Department Manager	Signature	Date
MIKE PALMER		April 15/2016
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Rob Gordon		April 20/16
Head of Public Body, or designate	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.