Ministry of Training, Colleges & Universities

Business and Systems
Management Branch
Suite 200, South Tower
175 Bloor St. E
Toronto ON M4W 3R8

**Ministère de la Formation
et des Collèges et Universités**

Direction de la gestion des
opérations et des systèmes
Bureau 200, tour sud
175, rue Bloor Est
Toronto ON M4W 3R8

Ontario

MEMORANDUM TO: Literacy and Basic Skills Service Delivery Organizations

DATE: September 28, 2012

SUBJECT: Instructions for the decommissioning of the LBS-IMS Client
Application and the LBS-IMS Interim Reporting Process

With the launch of the Employment Ontario Information – Case Management System (EOIS-CaMS) to LBS service providers on April 1, 2012, the LBS-IMS Client Application (aka LBS-IMS) and the LBS-IMS Interim Reporting Process must now be decommissioned.

Effective close of business on Monday, October 15th, 2012, uploads of LBS learner follow-up data, generated by the LBS-IMS, will no longer be accepted by the Ministry. Further, the Ministry requests that LBS service providers refrain from the use the LBS-IMS from this point forward.

As part of your contractual obligations and our mutual commitment to safeguarding client information, LBS service providers will be required to follow the instructions outlined in the attached package as part of the decommissioning of the LBS-IMS.

These decommissioning instructions explicitly outline the minimum steps that must be taken by all LBS service providers in order to protect the personal privacy of LBS learners' personal information. Please note - the Ministry will ask LBS service providers to demonstrate their compliance with these steps.

Launched in 2000, the LBS-IMS includes a database of LBS learners' personal information dating back over this period. LBS service providers are required to take specific steps outlined in the attached instructions to appropriately archive and securely store this personal information.

As part of the LBS-IMS decommissioning, it is imperative to protect LBS learners' personal information by taking steps to:
1. Archive historical LBS learners' personal information which exists in the database;
2. Attest that your organization has appropriately archived and securely stored the historical LBS learners' personal information; and
3. Make this archived information available to the Ministry, upon request, in accordance with your contractual obligations.

Given the importance of this exercise, the Ministry expects senior management of LBS and/or your organization's privacy official, as set-out in Article 9 of the LBS Agreement, to oversee and attest to the proper archiving and secure storage of the LBS-IMS data.

To support the archiving of the LBS-IMS Client Application and the LBS-IMS database, the Ministry requires LBS service providers to use **encrypted** USB drives, as well as uninstalling the Client Application and database from desktops and/or network drives (additional specifics are outlined in the attached document).

The Ministry first alerted LBS service delivery organizations to the upcoming decommissioning exercise when we published in January 2012 the *Literacy and Basic Skills Leaner Carryover and Transition Guide for April 2012.* Please make note of the following key dates:

October 15, 2012 (close of business):
- o Cut-off for the final uploads of LBS learner follow-up data

November 30, 2012:
- o Completion of all decommissioning activities by LBS service providers, and
- o Termination of the LBS-IMS Help Desk Support by the Ministry for the LBS-IMS Client Application and the LBS-IMS Interim Reporting Process.

January 25th, 2013*
- o As part of the reporting of the LBS Q3 QSAR, service providers will be required to attest that their organization has completed the decommissioning.

*Ministry staff may request an attestation prior to this date.

Please contact your Employment and Training Consultant if you have questions.

Thank you.
Business and Systems Management Branch
September 2012

Attachment
Decommissioning Instructions: The LBS-IMS Client Application and LBS-IMS Interim Reporting

DECOMMISSIONING INSTRUCTIONS:
THE LBS-IMS CLIENT APPLICATION AND LBS-IMS INTERIM REPORTING PROCESS

IMPORTANT: The following instructions apply to situations where the LBS-IMS is running on either **Windows XP** or **Windows 7 – 32 bit** Operating Systems. If the LBS-IMS is running on a **Windows 7 – 64 bit** Operating System; please contact the LBS-IMS Help Desk for decommissioning instructions. Steps for determining the Operating System are outlined below.

Determining the Operating System

A. Click on the **Start Menu** to find the "My Computer" or "Computer" application.
   - If the Start Menu has "My Computer," the operating system is *Windows XP* and you can continue to follow these instructions for decommissioning.
   - If the Start Menu has "Computer," the operating system is *Windows 7.*
B. If the operating system is *Windows 7*, click on **System Properties** to verify the system type. Within the *System Properties* page, the section labelled "System" will list the "System Type."
   - If the System Type is "32-bit Operating System", continue following these instructions.
   - If the System Type is "64-bit Operating System", please contact the LBS-IMS Help desk for decommissioning instructions.

All steps outlined in this decommissioning exercise must be completed.

Step 1: Locate and verify the LBS Database

        A.   Launch the LBS-IMS Client Application and logon to verify the database.

        B.   Close the application and then re-launch it to run the "Compact and Repair" utility. This process will compact the database and insure its integrity.
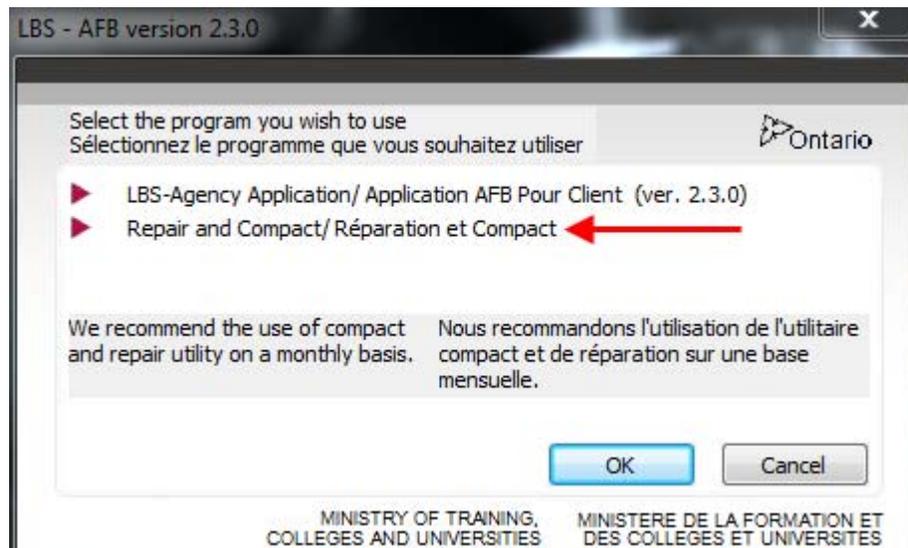
        C.   As shown in the example below, make note of the location of the current database from the *Logon Information* screen.
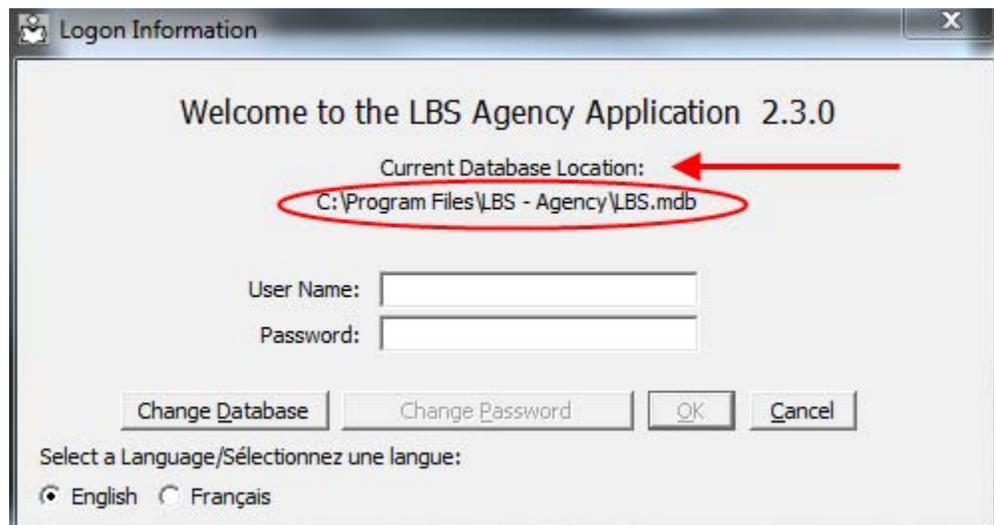
Step 2: Back-up process using an encrypted USB Memory Stick

Note: Make sure the **encrypted** USB Memory Stick is large enough to store both the database and LBS_AFB Virtual system.

    A. Plug in the **encrypted** USB Memory Stick and follow the encryption software logon process.

    B. Launch Windows Explorer from the Start-up Menu.

    C. Locate the database, by following the file path from the *Logon Information* screen. The database will have the extension "**.mdb**"

    D. Right click on the database file, and select **Copy**.
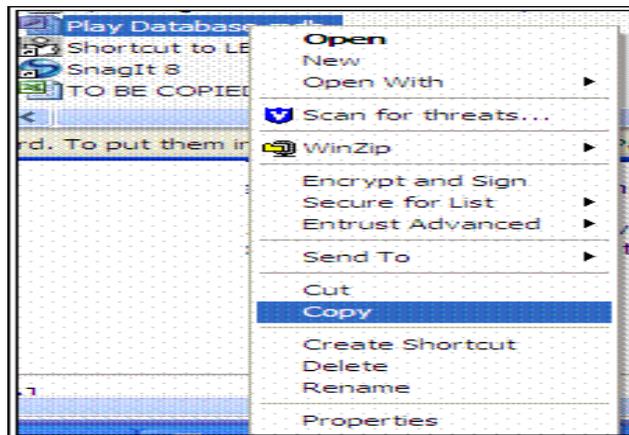
    E. Locate the USB Drive (Removable Disk), by double-clicking on the "Computer" (My Computer) icon on the desktop.
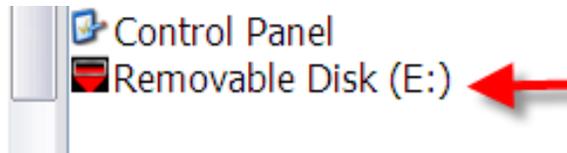
    F. Open the USB Drive by double-clicking on the "Removable Disk". In the above example the USB Drive is "Removable Disk (E:)."

    G. Within the open USB Drive panel, right-click inside select **Paste** from the menu.

    H. Once the database file has saved on the USB Drive, right-click on file and select **Rename** from the menu.

    I. <u>Keep</u> the original file name and add the backup date at the end of the file name. This will help in identifying the date of the backup
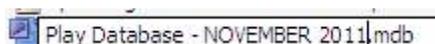
J. Verify that the database file has been saved on the USB Drive. Double-click on the **.mdb** file. If the file opens in Microsoft Access and a password prompt appears, the file has successfully saved.

Step 3: Save a copy of the Virtual LBS-IMS Client Application on the encrypted USB Memory Stick

---

A copy of the LBS_AFB Virtual system should also be on the **encrypted** USB Memory Stick to use in the case your organization or the Ministry needs to access the database. The application does not require installation and can run from any directory or location.

A. The application can be downloaded from the LBS-IMS Secure Portal - LBS-AFB Interim Solution Site URL: http://208.124.226.122
This is a full package; there are no additional installs or patches required.

B. Choose [save icon] to from the *LBS Interim Solution* page to navigate to the *Download* page.

C. Enter the current user name and password, and click **Login**.

D. From the menu, click the link beside **Download:** "LBS-AFB Agency v2.3.0." Both the downloadable file and the instructions can be obtained on this page.

E. When prompted, choose **Save**.

F. Locate the **encrypted** USB Memory Stick, and save the file. Do <u>NOT</u> change the "File name."
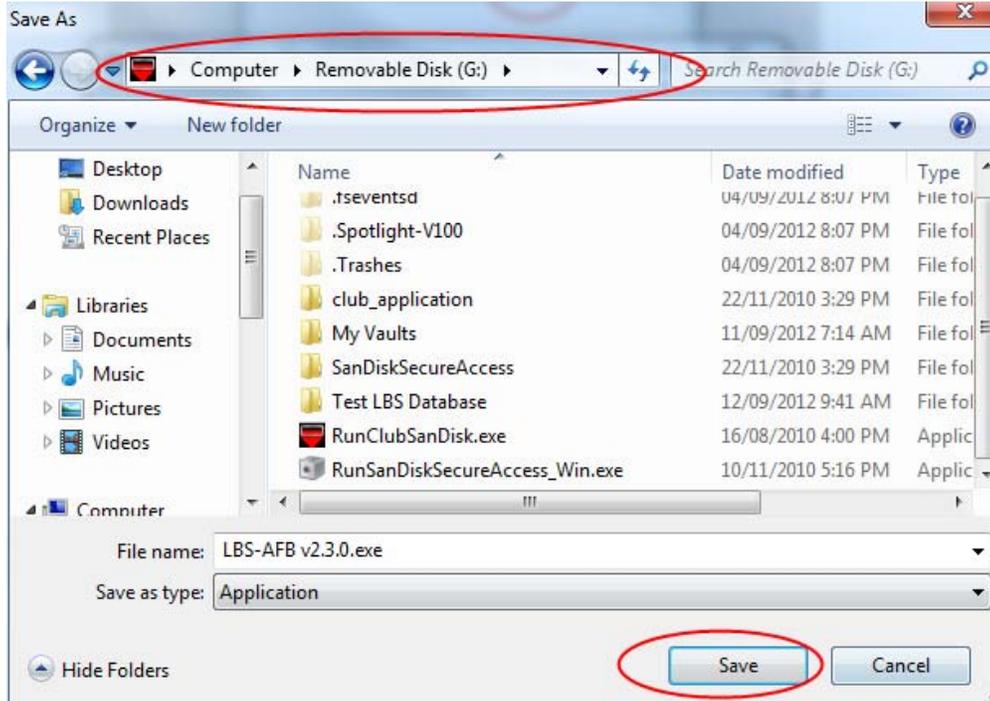
Step 4: Keep a repository of key LBS-IMS information

LBS organization must keep, **in a locked/secured manner**, a repository of key LBS-IMS Client Application information such as the user name, password, and a user manual. In addition, providers must keep all passwords related to the encrypted USB Drive in a separate but equally secured location. Organizations should:

1) Save a text file with the User Name and Password which you currently used to access the database
2) Review the documents that are currently available in the secure portal and save any documents you find relevant such as the user manual. Remember, the portal will also be decommissioned and these documents will not be available after November 30, 2012.

Step 5: Removal of the LBS database and uninstall of the LBS-IMS Agency Client v2.3.0

LBS agencies are expected to remove copies of the LBS database and uninstall the LBS-IMS Agency Client application from <u>ALL</u> desktops.

Follow these steps to uninstall the LBS-AFB Agency Client v2.3.0 (Virtual Client)
    A. Search for the application by clicking on **Search** from the Start menu.
    B. Search all files and folders for file name "VOS".

    C. Follow the path displayed in your Search window and permanently delete the file(s).

Follow these steps to uninstall the LBS-IMS Agency Client v2.3.0
    A. Open the **Control Panel** from the Start Menu.
    B. In the **Control Panel**, choose "Add and Remove Program."
    C. Uninstall LBS-IMS Agency Client.

Removing all copies of the LBS-IMS database
    A. Identify all desktops where the LBS-IMS database is stored by searching a desktop for the database by clicking on Start button, then **Search** from the Start Menu.
    B. Search all file and folders for file name " ***.mdb** "
    C. Delete any databases found through the search window by following the path indicated in the search window.
    D. Repeat this search on all local and network drives that are connected to the desktops, and delete any remaining databases.

IMPORTANT: If you and/or the Ministry requires access to the database stored on an encrypted USB Memory Stick

Running the LBS-AFB Agency Client v2.3.0
   A. Plug in the **encrypted** USB Memory Stick, and follow the USB encryption software login process.
   B. Open Windows Explorer and browse the USB Drive to locate the LBS-AFB Agency Client v2.3.0.
   C. To launch the application, double-click on the "LBS-ABF Agency v2.3.0.exe"
   D. Click **Run** to launch the application.
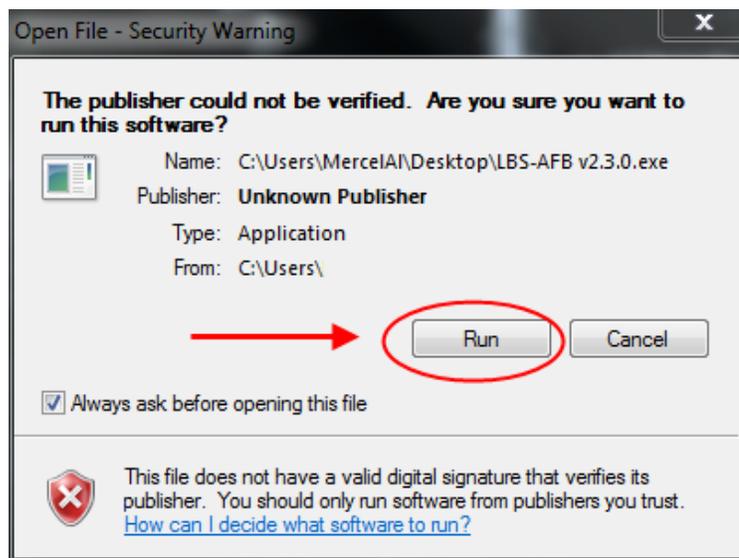
   E. Select the "LBS-Agency Application", and click **OK**.
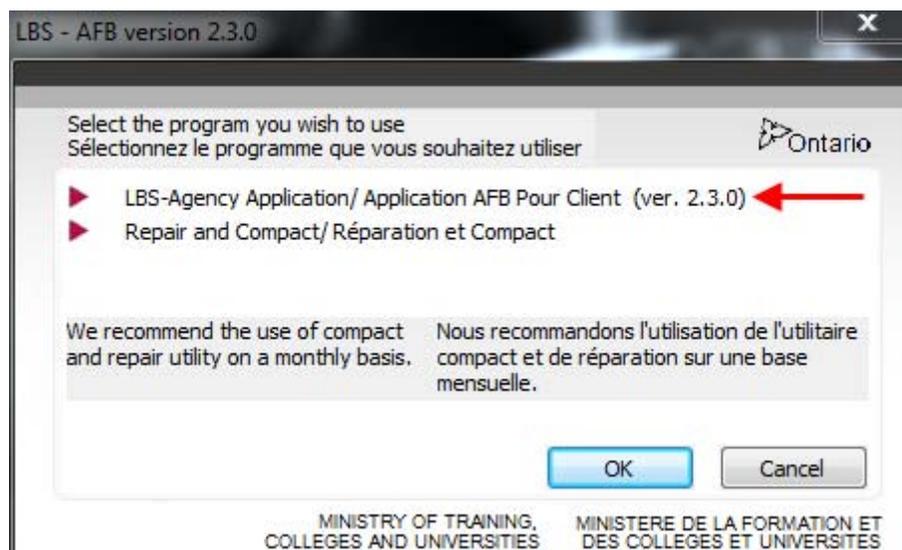
Note: Once the LBS-Agency Application has opened, a folder will be created in the same location as the application called "VOS." This directory stores all the settings and files for the application. If this directory is deleted, the application will recreate it back to its default settings with a default blank database.

F.   The LBS-IMS Application will launch the *Logon Information* screen.
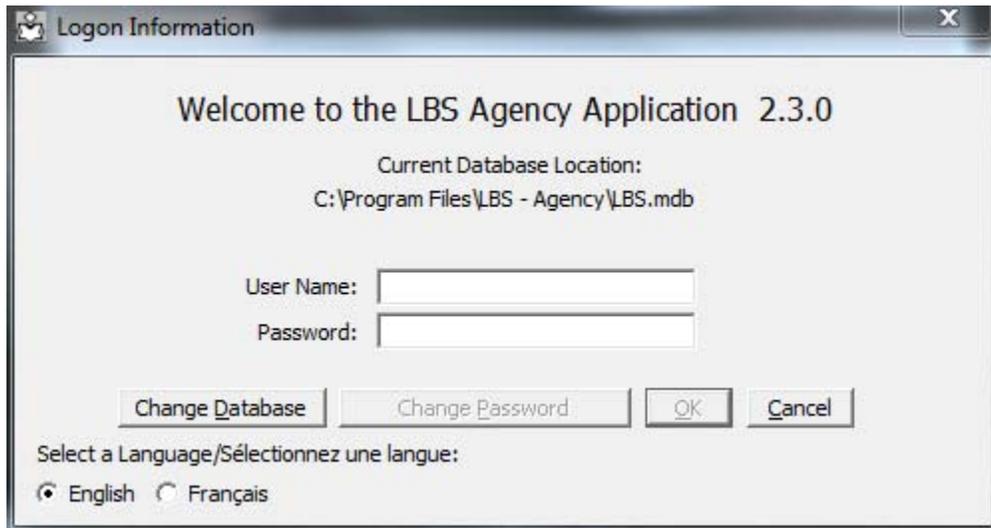
G.   Choose the **Language Preference**, and then click on **Change Database** to locate the database file saved on the **encrypted** USB Memory Stick.
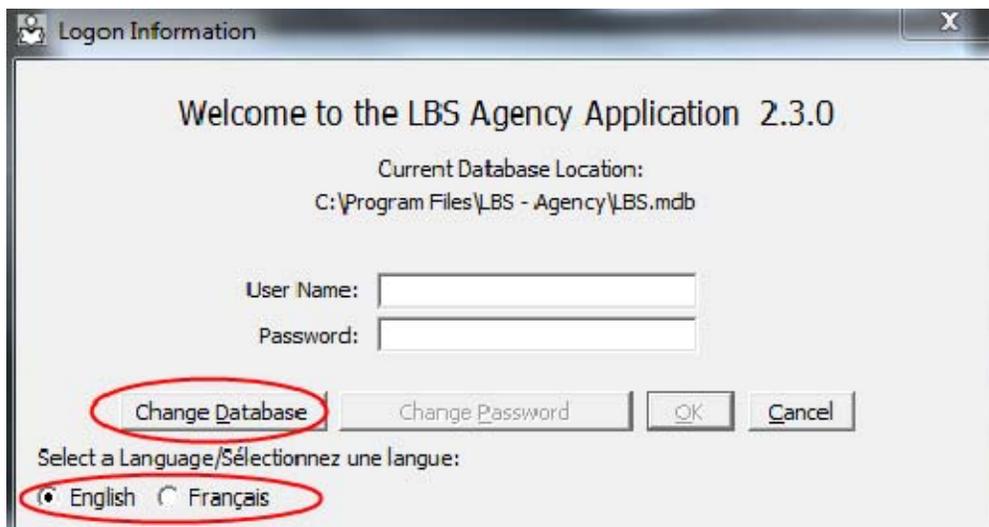
H.   Enter the **User Name** and **Password** information, and click **OK**.

Note: This application runs in a virtual environment. This means it has its own directory structure and does not write to the Window's file system. This application will run from any location including an **encrypted** USB Memory Stick.