SecureLock™

User Manual

Encryption Application for portable Storage Devices

User Manual Version 1.0.0.3
© 2004-2011 Integral Memory plc
**Table of Contents**

Table of Contents ................................................................................................... 2

1. Introduction..................................................................................................... 3
2. System Requirements .................................................................................... 4
3. Installation ...................................................................................................... 5
4. Registration .................................................................................................... 6
5. Working with SecureLock...............................................................................7
   5.1. Setting up SecureLock........................................................................... 7
   5.2. Setting up a Password ........................................................................... 7
   5.3. Password retries .................................................................................. 10
   5.4. Using Drag & Drop to copy files ........................................................... 10
   5.5. Opening and modifying files within SecureLock................................... 13
   5.6. Security settings................................................................................... 13
6. Safely Remove Hardware ............................................................................ 15
7. Support......................................................................................................... 16
8. Important Notice / Disclaimer ....................................................................... 17
1. Introduction

Protecting data in transit is essential to ensure no third party has access to data in case a device is lost, misplaced or stolen. SecureLock protects data on the device with Government-approved 256bit AES CBC-mode encryption.

With the intuitive Drag & Drop interface, files can be quickly copied to and from the device for fast, secure and efficient workflow.

SecureLock is a portable application that does not require any installation process on the host PC.
2. **System Requirements**

Operating Systems:

- Windows XP (Service Pack 2 is recommended)
- Windows Vista (all Versions)
- Windows 7

Available USB port

Removable USB Storage Device to start the application from (e.g. USB Flash Drive, External Hard Drive, Memory Card).

If the portable storage device has a manual write protection switch (lock), it must be in the unprotected (writable) position to be able to use SecureLock.

SecureLock does not require Administrative rights.
3. Installation

To install SecureLock on a USB flash drive (or other portable USB storage device), simply copy the file "SecureLock.exe" to the root folder of a partition associated with that device.
4. Registration

To register, you need to use the license key you have received bundled with your package. Please enter the license key in the Registration window and click the “Register” button in order to start using the software:

Please save your license key in a safe place for future reference.
5. Working with SecureLock

5.1. Setting up SecureLock

To start SecureLock simply double-click the SecureLock.exe that is saved in the root folder of the portable storage device.

5.2. Setting up a Password

In order to secure (encrypt) your data, you will need to set up a password. The password must be at least 6 (six) characters long.

For security reasons, it is recommended that you incorporate letters, numbers and symbols into your password.

Click “Next” to proceed.
Enter your password, and then confirm it.

It is recommended that you also set up a password reminder that will help you in case you forget your password.

For security reasons, the password reminder cannot be the same as the password itself.
Click “Finish” to continue.
5.3. **Password retries**

Each time the application starts, you will be asked, for security reasons, to introduce your password.

For that case that your drive was lost or stolen the number of password retries is limited to 10 (ten). After the password has been entered wrongly 10 (ten) times in a row, SecureLock will safely erase all encrypted files stored on the portable storage device.

The data on the portable storage device can thereafter not be recovered or recreated. It is permanently erased.

5.4. **Using Drag & Drop to copy files**

A key feature of SecureLock is the Drag & Drop functionality which allows you to simply drag the file(s) and/or folder(s) that you want to copy on the device and drop them onto the window of SecureLock. These files will be automatically encrypted, ensuring that your data stay safe and private.
The file encryption and transfer status can be seen with the help of the progress bar. When the bar reaches the end, your files have been copied and encrypted.
You can navigate through your encrypted files if you are using Windows Explorer. Clicking on an item with the right mouse button will give you access to options such as “Refresh”, “Copy” and “Delete”.

Copying files from your HDD to the portable storage device using Explorer is **not recommended**!

We recommend using either the Drag & Drop feature or the shortcut keys for copying and pasting, Ctrl+C and Ctrl+V to transfer data to your portable storage device though the SecureLock interface.

In the toolbar area of SecureLock you can find additional icons that you can also use to copy and encrypt your files.
Note that the files on your portable storage device are not visible after encryption, unless SecureLock is running.

To exit SecureLock, select the File menu and choose Exit, or simply click the “X” button in the upper-right corner of the application window.

5.5. **Opening and modifying files within SecureLock**

Copied data on device can be viewed and edited directly from within SecureLock. This function is accessible with the “Open” command or double clicking the desired file.

The user has to open documents from the device with the associated application. SecureLock will try to close these documents once it has exited If a document is modified (saved with the same name or even to the same folder) it will be encrypted and stored on the device. If a document is modified and saved but fails to be encrypted, for example when the device is unexpectedly removed, it will be encrypted the next time SecureLock is started.

5.6. **Security settings**

The security settings can be modified from within SecureLock. After logging in, you can modify your password. To do this you need to access the security settings menu. This can be done by either selecting Options->Security Settings from the toolbar area or by pressing the hotkey Ctrl + O.
Change Password

Old Password: 

New Password: 

Confirm New Password: 

New Password Reminder: 

Password Info

Please enter your old password.
6. **Safely Remove Hardware**

Before you unplug your portable storage device from the USB port of your computer, you have to use the “Safely Remove Hardware” option from the system tray, otherwise you risk corrupting the data on your USB Drive.

To Safely Remove Hardware, double-click on the system tray icon, then select the USB Drive you want to remove from the list and click on the “Stop” button.

A message will appear indicating that the portable storage device can now be securely removed. If a message saying “The ‘…’ device cannot be stopped right now” appears, you have to close your Windows Explorer, SecureLock or any other application that is still accessing the data on the USB Drive.
7. Support

In case additional help, such as the FAQs or e-mail support is required, you can visit the support website directly at http://www.integralmemory.com/securelock
8. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. Integral Memory cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and Integral Memory disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2011 Integral Memory plc; All rights reserved. Windows and .NET Framework are registered trademarks of Microsoft Corporation. All other names and trademarks are property of their respective owners.