1. INTRODUCTION

Thank you for purchasing the Kanguru Defender. The Kanguru Defender is a compact USB flash drives that utilizes AES hardware encryption. These drives keep your data secure and available wherever you are.

The Kanguru Defender can:

- Encrypt & decrypt your sensitive data using simple drag and drop
- Secure all your data using strong password protection

System Requirements

- Operating Systems:
  - Windows XP Service Pack 2 or Service Pack 3
  - Windows 2003
  - Windows Vista
  - Windows 7
- 32bit and 64bit supported
- 1 Available USB port (USB 2.0 Recommended)
- 256MB of internal DDR RAM or more
- 500MHz internal CPU or faster

Package Contents

If any of the items listed are missing, please call Kanguru Solutions' Tech Support department at: (508) 376-4245 and replacement parts will be shipped to you ASAP.

- Kanguru Defender Flash Drive
- Quick Start Guide
- Registration Form
- Lanyard
- USB Extension Cable (32GB and larger capacities only)

Note: This is a Quick Start Guide only. The comprehensive user manual can be downloaded from the Kanguru Support Site under the Downloads section at: http://support.kanguru.com/

2. KANGURU DEFENDER MANAGER

Kanguru Defender Manager (KDM) manages your password and allows you to access the Defender's secure partition. It is pre-loaded on your Kanguru Defender so no installation on your PC is necessary.

To start KDM, plug in your Kanguru Defender. KDM should autorun itself.

If KDM does not run automatically, open My Computer or Windows Explorer. The Kanguru Defender will be displayed as **two drive letters**. One drive is the CD-ROM partition where KDM is pre-loaded, the other drive is the secured partition which will appear as a removable disk (the secure partition will appear as SECURITY after you login). The drive letters (e.g. D:, E:, F:, etc.) will depend on your computer.

CD-ROM Partition — Secure Partition

Open the CD-ROM partition and then double-click on the **KDM.exe** file to start the application.

Note: Your Kanguru Defender has a manual write protect switch that needs to be set to the unlocked position (switched towards the USB connector) in order to setup KDM.

The KDM.exe file will remain on your Kanguru Defender's CD-ROM partition so that you can run the application on different computers from your Defender. Please always run the application from the CD-ROM partition and never from a hard drive on your laptop/desktop.

Warning: While using KDM, you should never disconnect your drive without first closing KDM properly by clicking the KDM taskbar icon and selecting "Unmount Kanguru Defender" and then using the "Safely Remove Hardware" option.

When you start KDM for the first time, you will be greeted by the Setup Wizard.

To begin, click on the **Next** button and then follow the simple instructions to setup your Defender's login password.

3. ACTIVATING ANTIVIRUS

KDM will automatically check if your drive has a valid antivirus license key. Your Defender needs to be connected to a computer with internet access in order to activate the on-board antivirus protection. **Note:** If your drive is configured for use with Kanguru Remote Management Console Enterprise, this step will not be available.

If your Defender does not already have a valid antivirus license key, then you must fill out the registration form with the required information and then click on the **Apply** button in order to activate your one (1) year of free antivirus protection.

Click on the **Skip** button if you do not wish to activate antivirus protection. If you decide to skip activating your antivirus now, you will not be able to activate it in the future without first resetting your drive to the factory default setting.

Click on the **Next** button to continue with setting up your Defender's login password.

KANGURU Solutions™

Technology on the Move!

KANGURU Defender™

AES Hardware Encryption

Quick Start Guide

4. SETTING A PASSWORD

The password that you choose must contain at least 8 characters (by default). For security reasons, it is recommended that you incorporate letters, numbers and symbols to achieve maximum security. If your passwords do not match or there is any other issue with the password which you have entered in the Set Password section, an explanation will be visible in the Password Info section.

Note: The Password Info section updates in real time. It may tell you that your confirmation password is too short or does not match before you have finished re-typing the entire password. Please disregard the messages in the Password Info section until you have finished entering your password in both the Password and Confirm Password fields.

After you have entered your password in both boxes (Password & Confirm Password), click on the **Apply** button and then click on the **Next** button to set your security password to your drive.

5. ENABLING KRMC CLOUD

Kanguru Defender drives can be remotely managed using the Kanguru Remote Management Console (KRMC). KRMC Cloud is hosted on Kanguru's server. **Note:** If your drive is configured for use with Kanguru Remote Management Console Enterprise then this step will not be available. If your drive is a Defender Basic model then this step will not be available.

To Enable KRMC Cloud functionality:

1. Select the **Enable KRMC Cloud** option and then click on the **Apply** button.
2. A dialog box will appear asking if you want to register your device with KRMC Cloud. Click on the **Yes** button.
3. Your web browser will open and direct you to the KRMC Cloud login page.
4. Purchase a license for your drive in order to use it with KRMC Cloud.

If you choose not to remotely manage your Defender using KRMC Cloud, select the **Disable KRMC Cloud** option and then click on the **Apply** button. You will not be able to enable KRMC Cloud functionality again, unless you first reset your drive to the default factory settings.

6. LOGGING INTO KDM

After completing the Setup Wizard the KDM application will start. For security reasons, you will be asked to enter your password.

To continue, enter your password and then click on the **Login** button. Once KDM has confirmed your login password, it will mount the secure partition. You can now access the secure partition as you would a standard removable drive.

Warning! If you enter your password incorrectly 7 times in a row (by default), then your data will be automatically erased. An on screen warning message will be displayed after the 6th failed attempt, informing you that you only have one password attempt remaining.

Note: Click on the **VK** icon to access the virtual keyboard. The virtual keyboard is a graphical representation of a standard keyboard layout. You can click on the keys on the virtual keyboard to enter your password in order to prevent keylogging software from spying your login password.

7. ENCRYPTING FILES AND FOLDERS

A key feature of the Kanguru Defender is Drag & Drop functionality; allowing you to simply drag files and folders that you want to encrypt onto the drive's secure partition using the standard Windows Explorer interface. The Kanguru Defender automatically encrypts these files.

To open the secure partition, simply click on the KDM taskbar icon and select **Explore Security Drive**.

Alternatively, you can access the private partition through My Computer or Windows Explorer. The secure partition will be labeled SECURITY once it is unlocked. We recommend using either the Drag & Drop feature or the shortcut keys for copying (Ctrl+C) and pasting (Ctrl+V) to transfer files.

Note: Files saved on the secure partition of your Kanguru Defender device are only accessible after you have successfully logged into KDM.

8. REMOVING YOUR DEFENDER

To exit KDM, click on the KDM taskbar icon and select **Unmount Kanguru Defender.**

When you exit the application, KDM will lock the SECURITY partition and your files will become inaccessible until you login with the correct password again.

Warning: Do not disconnect the Kanguru Defender without first properly unmounting your device. Doing so may result in file damage or corruption.

Note: After you have umounted the security partition, use the "Safely Remove Hardware" option from the system tray to disconnect your drive. Otherwise you risk corrupting the data on your Kanguru Defender.