1 Introduction

Congratulations on your purchase of the Armadillo USB 3.0 Encrypted Hard Drive. Your Armadillo is protected by AES-256 XTS encryption. Since 2002, AES has been the encryption standard used by the United States Government. With the proper selection and protection of your password, data stored on the Armadillo is secure from even the most determined hackers. There is no known technique to break AES encryption. A brute force attack is expected to take longer than the lifetime of the universe.¹

As a further precaution, the Armadillo uses the XTS mode of AES. In 2010, the United States National Institutes of Standards recommended the use of XTS to provide “more protection than the other approved confidentiality-only modes against unauthorized manipulation of the encrypted data.” That is, even though the data remains encrypted, sophisticated tools may guess at the underlying information by analyzing patterns of usage and repetition in the encrypted result. XTS overcomes this analysis by introducing an additional encryption key that hides these patterns.

Your Armadillo features a SuperSpeed USB 3.0 connection for enhanced transfer speeds. Legacy USB connections are also supported at lower data rates. The Armadillo only works with Windows XP, Vista, and Win7 based PCs.

2 Setting your password

When you first receive your Armadillo, it will not be password protected. When you plug the Armadillo into your PC, you will see two hard drives appear in your computer. One will be named Armadillo and the other Encrypted Drive.

The Armadillo drive is always available. It is a small read only partition that includes a password application. The Encrypted Drive is where you place your secure data. You must set a password to secure your data. Once a

¹ In order to simply flip through the possible values for a 128-bit symmetric key (ignoring doing the actual computing to check it) would require \(2^{128} - 1\) bit flips. http://en.wikipedia.org/wiki/Brute_force_attack
password has been set and the Armadillo is locked, only the Armadillo drive will be visible.

Open the Armadillo drive and double click the password application. This takes you to the password screen. Enter the password you want. It is good to select a password that is not easily guessed at. A good password has a combination of random letters and numbers. However, make sure you can remember this password. There is no way to recover your data if your password is lost. The password is case sensitive.

To help you remember your password, you can place a reminder in the hint field. The hint will only be displayed if you have entered a wrong password three times. Do not place your password in the hint field. You are not required to enter a hint.

Once you press the “Set Password” button, your drive is protected, but unlocked.

---

2 On some Windows7 computers, you may get a User Account Control warning that a program is trying to make changes to the computer. Select “Yes” if this occurs.

3 When using multiple Armadillos in the same PC at the same time, the password application is linked to the Armadillo that it comes from – locking or unlocking the Encrypted Drive on that physical Armadillo.
3 Locking the Armadillo

**Encrypted Drive** is only visible when the Armadillo is unlocked. Lock the Armadillo by pressing the lock button. The Armadillo will also automatically lock if the USB cable is unplugged, or if it is turned off.

If the computer sleeps, suspends, or hibernates, the Armadillo automatically locks itself, but data cached in the computer’s memory is still available. Small files from the **Encrypted Drive** may still be viewable after the computer wakes up – even though the **Encrypted Drive** is no longer accessible. Similarly, documents that are open in applications are generally stored in memory and still viewable after the Armadillo is locked.

The Armadillo enters a power saving mode after 15 minutes of inactivity. This does not lock the Armadillo.

4 Unlocking the Armadillo

When the Armadillo is locked, only the **Armadillo** drive is visible. The **Encrypted Drive** is not visible in “My Computer”. Because it is made up of seemingly random bits of data, the **Encrypted Drive** looks like an uninitialized, unformatted drive to Windows. This “uninitialized” drive can be found using specialized tools – it is write protected so you cannot accidently format the **Encrypted Drive**.

To unlock the Armadillo, double click on the Password application (found in the **Armadillo** drive) and type in your password. If correct, the **Encrypted Drive** will appear.

The password hint (when used) will be displayed if the password is entered incorrectly 3 times. If the password is entered incorrectly 5 times, you must power the Armadillo off and back on before it will allow another password attempt.
5 Changing your password

Use the Password application to change your password. You must enter the current password in order to change to a new password.

6 Disabling password protection

If password protection is disabled, the Armadillo cannot be locked. Data on the Encrypted Drive can be accessed without a password by Windows PCs and also by non-Windows based devices like Macs, Linux PCs, and some TVs and game consoles.

You must confirm the current password in order to disable password protection.
7 Erasing the drive

The “Erase Drive” button securely and permanently erases the encrypted contents of the Armadillo in just a few seconds. You do not need the current password to do this. This may be useful when disposing of the drive or if the password has been lost. The Armadillo read only partition is not affected by the erasure.

The Encrypted Drive is write-protected when it is locked.

To reuse the Armadillo after it has been erased, you must initialize and format the Encrypted Drive. You can accomplish this with the Disk Management tool built into Windows.
8 Keeping your Armadillo healthy

The Armadillo should be protected from physical and electrical shock as well as moisture. Microsoft recommends drives be safely removed through Windows first before disconnecting the USB cable or powering down the drive. This lets the Armadillo park the drive head before shutting off power to the drive.

The password application continually keeps track of the Armadillo’s health. If the health indicator ever changes from “Good” you should backup the drive’s contents to another disk. The health status is only a statistical indicator; drives may fail at any time without the status changing.

9 Limited Warranty and Legal Notices

Armadillo USB 3.0 Encrypted Hard Drive
Copyright (c) 2010, LucidPort Technology, Inc.

Please contact support@marathon6.com for technical questions.
Contact sales@marathon6.com for sales or warranty related inquires.

Marathon6 warrants to you that the Armadillo will be free from defects in materials and workmanship under normal use for the 90 day warranty period starting on your date of purchase. Your dated sales or delivery receipt is your proof of purchase date. You may be required to provide proof of purchase as a condition of receiving warranty service.
If Marathon6 receives, during the warranty period, notice of a defect in the Armadillo, Marathon6 will repair or replace the product, at Marathon6’s option. Marathon6 shall have no obligation to repair, replace, or refund until you return the defective product to Marathon6. If your Armadillo has recurring failures, at Marathon6’s option, Marathon6 may provide you a replacement of Marathon6’s choosing that is the same or equivalent in performance or a refund of your purchase price instead of a replacement.

To the extent permitted by local law, Marathon6, and any replacement products or parts, may contain new and used materials equivalent to new in performance and reliability. Any replacement product or part will also have functionality at least equal to that of the product or part being replaced. Replacement products and parts are warranted to be free from defect in material or workmanship for 90 days.

Marathon6, at its sole discretion, may subcontract to or engage a third party to provide the warranty services.

DATA LOSS IS A FREQUENT CONSEQUENCE OF REPAIR. DATA STORED ON THE ARMADILLO IS NEVER COVERED BY WARRANTY.

This Limited Warranty does not apply to expendable or consumable parts or to any product in which the chassis has been opened or if damaged or defective (a) due to accident, misuse, abuse, contamination, virus infection, improper or inadequate maintenance or calibration or other external causes; (b) by software, interfacing, parts or supplies not supplied by Marathon6; (c) improper site preparation or maintenance; (d) loss or damage in transit; or (f) modification or service by other than Marathon6 or an Marathon6 authorized service provider.

TO THE EXTENT ALLOWED BY LOCAL LAW, IN NO EVENT SHALL LUCIDPORT TECHNOLOGY, INC. BE LIABLE FOR ANY DAMAGES CAUSED BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY AND WHETHER ADVISED OF THE POSSIBILITIES OF SUCH DAMAGES. LUCIDPORT TECHNOLOGY, INC. IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY.

The AES encryption technology in the Armadillo is classified by the United States government as an ECCN 5A002 item and can be exported under License Exception ENC, Sec. 740.17 (b)(3) of the Export Administration Regulations (“EAR”). The Armadillo may not be used or otherwise exported or re-exported into (or to a national or resident of) Cuba, Iran, North Korea, Sudan, or Syria. No further approvals or authorizations from the US government are required.