User Manual

Rocstor DataSecure EX20 Portable Encrypted Drive
FIPS 140-2 Level 3* Validated

TABLE OF CONTENTS

SECTION 1: DATASECURE EX20 OVERVIEW

Thank you for purchasing the DataSecure -Keypad Model ('Drive' hereafter), an easy to use hardware encrypted USB 3.0 portable external data storage drive with on-board alphanumeric 11 button keypad for OS-independent user-authentication.

The Drive uses XTS-AES 256-bit hardware encryption, which encrypts all data on it in real time. It requires no software drivers nor updates and works on all computer and embedded systems that support standard USB protocol. Should your Drive get lost or stolen, rest assured that all data on it is protected by military grade encryption and cannot be accessed without entering the PIN (Person-Identification-Number).

The Drive can be configured with both a User and Admin PINs, making it perfect for personal use and business use such as healthcare, legal, corporate, and government. Your drive may have Cloud Backup and built-in Antivirus features installed. For more information, please contact Technical Support at support@rocstor.com .

Requirements

The Drive must be connected to a computer for access. It works on Windows, Mac, Android, Linux, or Chrome operating systems, or any embedded systems supporting USB 2.0 port, minimum.

What's Included?

• 1 DataSecure EX20 • 1 Quick Start Guide • 1 USB 3.0 Cable

Safety Information

This icon ⚠ indicates important information regarding the safety of the product and your data (Caution messages). Please be mindful of these messages. Contact support if you have questions.

Precautions

⚠ Do not expose the Drive to water or moisture.

⚠ Resetting the Drive will delete all stored data as well as all passwords and settings. The drive will become blank and require formatting.

⚠ Forgetting your password will render the Drive inaccessible. There is no 'backdoor.'

⚠ Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.

EMI Notice

The normal function of the product may be disturbed by strong Electro Magnetic Interference. If so, simply remove and reinsert the product to resume normal operation by following the instruction manual. In case the function could not resume, please use the product in another location.

DataSecure EX20 Features

LED Interpretations

LEDs on the SecureDrive are represented here by colored icons.

LED	Meaning
(blink all together once)	Plugged into computer; LED test
= Red solid	Locked; Momentarily preparing for next input; or failed procedure.
= Red blinking[1]	Locked, ready for input (other than a Setting code). Also, specific feedback[1]
= Red blinking with Green solid	(Settings Mode) Locked & ready for keypad input within 10 seconds, or idle for 30 seconds if procedure is done.
= Green blinking	Unlocked and ready for keypad input
= Green blinking slowly	Unlocked for use in Read-Only Mode
Blue solid **Blue blinking**	Drive is powered and when blinking is transferring data. **Note:** The blue LED may be on or blinking during any procedure after the Drive is unlocked.
= Green solid	Unlocked; operation was successful.

[1] For other LED combinations see specific status requests: *Verifying Existing PIN* and *Determining the Version Number* described in this manual.

PIN Requirements

Your User PIN or Admin PIN must:

- be between 7-15 digits in length
- not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Note: Creating words (using the corresponding number key for each letter) can be more memorable than a string of numbers.

Procedural Conventions

All procedures below require the Drive to be connected to a computer with the USB cable. LED status shown is what you should see after performing each step. Unless otherwise noted, all procedures start with the Drive locked. [🔒]

Note: Each step in all procedures listed below have a 10 second window to perform the next step. In general, a blinking LED times out after 10 seconds.

Cancelling a Procedure

To cancel most procedures prior to finishing, press and hold 🔑 for six seconds. The exception are procedures for setting options (🔑 🔑 🔑) which you can just let time out between steps.

SECTION 2: User Mode

This section describes how to unlock and lock the Drive, change the PIN, and disconnecting the Drive from your computer in User Mode. New drives are shipped with a default User PIN which is 11223344 (otherwise, your vendor will supply it). We strongly recommend changing the password once it is unlocked.

CAUTION: Risk of loss of data. If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible and reformatting will be required.

CAUTION: Loss of data will occur. After ten failed attempts to unlock the Drive, the User PIN and all data on the Drive will be deleted. Refer to *Brute Force Hacking Detection* on page 14.

Unlocking the Drive in User Mode

Note: If the Drive is inserted into a computer when locked, its contents does not appear in your computer's File Manager (Explorer or Finder).

STEPS	LED	ERROR STATE
Connect the Drive to your computer with the USB cable.	-	-
Press 🔑.	🔒	-
Enter the **User PIN**.	🔒	-
Press 🔑.	🔓	🔒 - if error, the red LED fades out then turns solid.

*The factory PIN for new Drives is 11223344. We strongly recommend changing the password once it is unlocked. See *Changing the User PIN* below. If your computer goes into sleep mode while the Drive is unlocked, the Drive may lock after some time depending on your power management settings regarding the USB port.

Changing the User PIN

STEPS	LED	ERROR STATE
Press 🔑.	🔒	-
Enter the **User PIN**.	🔒	-
Press 🔑 🔑.	🔓 + 🔒	-
After you see [🔓], then press 🔑 🔑.	▬	-
Enter the new **User PIN**.	▬	-
Press 🔑 🔑.	🔓	-
Re-enter the new PIN.	🔓	-
Press 🔑 🔑.	🔒 - brielfy Then → 🔓 + 🔒	If unsuccessfull, LEDS will immediately be: 🔓 + 🔒

Note: If a mistake was made or the procedure was not completed, the Drive will retain the old PIN.

Disconnecting from Your Computer

Generally, you can just unplug the USB cable. However, some computer systems may require you to click the **Safely Remove Hardware/Eject** icon within your operating system prior to unplugging the drive cable from your computer. Wait for the red LED to light to turn solid or turn off completely indicating it is locked and ready to disconnect from the computer.

User Mode Options

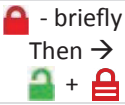
The following section describe options and features requiring only a User PIN. For Administration options see Admin Mode on page 11. This section includes instructions on enabling read-only and read/write options in user mode as well as enabling and disabling a timeout lock.

Procedures that end with these LEDs [].

Note: All procedures require the Drive to be connected to a computer with the USB cable. Each step in all procedures have a ten second window to start the step after it. In general, a blinking LED times out after ten seconds.

Enabling Read-Only in User Mode

The User is able to write content to the Drive and then restrict access to read-only (R-O). Once R-O Mode is activated, access is limited to reading only, until Read/Write is enabled (which can be accomplished by a User or an Administrator). **Setting to Read-Only does not unlock the drive.**

STEPS	LED	ERROR STATE
With the Drive locked, press 🔑.		-
Enter your **User PIN**.		-
Press 🔑🔑.		-
Wait for  , then press 🔑🔑🔑.		-
Press **7**, **6**. (R, O for Read-Only).		-
Press 🔑.	 - briefly Then → +	If unsuccessfull, LEDS will immediately be: +

If successful, the next time the Drive is unlocked it will be in R-O Mode as indicated by the **slow blinking** green LED (as well as messages provided by your computer when you try to save or delete a file).

Enabling Read/Write in User Mode

Read-Only (Write Restriction) can be turned off restoring Read and Write access. Note that setting the drive to R-W does not unlock the drive.

STEPS	LED	ERROR STATE
With the Drive locked, press .		-
Enter your **User PIN**.		-
Press .		-
Wait for , then press .		-
Press **7**, **9**. (R, W for Read/Write).		-
Press .	- briefly Then → +	If unsuccessfull, LEDS will immediately be: +

If successful, the next time the Drive is unlocked it will be in Read/Write Mode with a **solid** green LED.

Setting the Timeout Lock in User Mode

To protect against unauthorized access when the Drive is connected to a host computer and unattended, the Drive can be set to automatically lock after a pre-set amount of idle time (no read or write activity).

Note: When set in User Mode, the Timeout Lock is only active in User Mode and not Admin Mode.

The default state of the Timeout Lock feature is OFF. The Timeout Lock feature can be set to activate (lock) any time between 1 and 99 minutes.

STEPS	LED	ERROR STATE
With the Drive locked, press .		-
Enter your **User PIN**.		-
Press .		-
Wait for , then press .		-
Press **8, 5**. (T, L for Timeout Lock).		-
Press .		-
Enter the length of unattended time for Timeout. Two digits required. **Examples:** 01 = 1 minute 99 = 99 minutes		-
Press .	- briefly Then → +	If unsuccessfull, LEDS will immediately be: +

The Timeout Lock is now set for subsequent Drive use, until changed.

Disabling the Timeout Lock in User Mode

Follow the same steps for setting the Timeout Lock (above) and enter **00** for the time delay.

The Timeout Lock is now disabled.

SECTION 3: Admin Mode

Admin Mode is especially useful for corporate deployment and it can be used to ensure policy. For example:

- Recovering data from a Drive and creating a new User PIN in the event that you or an employee has forgotten the User PIN.
- Retrieving data from a Drive if an employee leaves the company.
- Setting policies such as 'Read-Only' or 'Time Out Lock.'
- The Admin PIN can be used to override all User Mode settings.

Button Pressing Conventions

Many Admin procedures start with pressing and holding a number button down (**1** or **7**, for example) and while holding it, pressing button: abbreviated in the steps below as: *Press and hold down **7-and then press-***. In some cases, you must hold down the number while pressing and releasing button twice: abbreviated as: *Press and hold down **1-and then press-***.

Note: All procedures under this heading start with the Drive plugged into a computer. Each step in all procedures listed below has a 10 second window to start the step after it. In general, a blinking LED times out after 10 seconds.

The PIN requirements are the same as User Mode. Refer to PIN Requirements on page 4.

Admin PINs

CAUTION: Risk of loss of data. If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible and reformatting will be required.

This section describes how to create or change an Admin PIN, create or change a User's PIN in Admin mode, and how to unlock and lock the Drive in Admin mode.

Creating an Admin PIN (No User PIN)

STEPS	LED	ERROR STATE
Press .		-
Press and hold down **1-and then press-** .	rapidly	-
Enter a new **Admin PIN**.	rapidly	-
Press .		- fades out, then solid if PIN doesn't meet the requirements.
Re-enter your new **Admin PIN**.		-
Press .	→ +	- if error, the red LED fades out then turns solid.

Note: If a mistake was made or the procedure not completed, no Admin PIN will be created.

Creating an Admin PIN (User PIN Exists)

STEPS	LED	ERROR STATE
Press .		-
Enter the **User PIN**.		-
Press .		-
Wait for , then press and hold down **1-and then press-**.		-
Enter a new **Admin PIN**.		If an error occurs: +
Press .		-
Re-enter your new **Admin PIN**.		-
Press .	- briefly Then → +	If unsuccessfull, LEDS will immediately be: +

Note: If a mistake was made or the procedure not completed, no Admin PIN will be created.

Unlocking the Drive in Admin Mode

CAUTION: Possible deletion of all data, settings, and both PINs. After ten failed attempts to unlock the Drive, it will reset to a blank factory setting. Refer to *Brute Force Hacking Detection* on page 14.

STEPS	LED	ERROR STATE
Press and hold down **1**-and then press .		-
Enter the **Admin PIN**.		-
Press .	- briefly Then → +	- if error, the red LED fades out then turns solid.

Note: If your computer goes into sleep mode while the Drive is unlocked, the Drive may lock after some time depending on your power management settings regarding the USB port.

Creating or Changing a User PIN in Admin Mode

For PIN requirements refer to page 4.

STEPS	LED	ERROR STATE
With the Drive locked, press and hold down **1-and then press-**🔑 .		-
Enter your **Admin PIN**.		- if error, the red LED fades out then turns solid.
Press 🔑🔑.		-
Wait for , then press 🔑🔑.		-
Enter a new **User PIN**.		-
Press 🔑🔑.		If an error occurs: fast + slow
Re-enter the **User PIN**.		-
Press 🔑🔑.		- if error, the red LED fades out then turns solid.

If successful, the User PIN is now added or changed.

Changing the Admin PIN

The Admin PIN cannot be changed from the User Mode. Remember that **Press and hold down 1-and then press** 🔑🔑 means “hold down #1 button and press the Key button twice.” PIN requirements on page 4.

STEPS	LED	ERROR STATE
With the Drive locked, press and hold down **1-and then press-**🔑.		-
Enter the **Admin PIN**.		-
Press 🔑🔑.		- if error, the red LED fades out then turns solid.
Wait for , then press and hold down **1-and then press-**🔑🔑.		-
Enter a new **Admin PIN**.		-
Press 🔑🔑.		If an error occurs: fast + slow
Re-enter the **Admin PIN**.		-
Press 🔑🔑.	- briefly Then → fast + slow Then →	- if error, the red LED fades out then turns solid.

Note: If a mistake is made while defining a new Admin PIN or the procedure is not completed, the Drive retains the old Admin PIN (as well as the old User PIN if one exists).

Admin Mode Options

The following headings describe enabling options and features requiring an Admin PIN such as enabling read-only and read/write mode, and setting Timeout Lock in Admin or User Mode.

Enabling Read-Only in Admin Mode

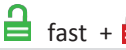
Note: When Admin restricts access to Read-Only, the User cannot change this setting. Setting to Read-Only does not unlock the Drive.

STEPS	LED	ERROR STATE
Press and hold down **1-and then press-**🔑.		-
Enter the **Admin PIN**.		-
Press 🔑 🔑.		 - if error, the red LED fades out then turns solid.
Wait for  , then press 🔑 🔑 🔑.		-
Press **7, 6.** (**R, O** for Read-Only).		-
Press 🔑.	 - briefly, then →  fast +  slow	If an error occurs:  fast +  slow

If successful, the next time the Drive is unlocked it will be in R-O Mode as indicated by the **slow** blinking green LED (as well as messages provided by your computer when you try to save or delete a file).

Enabling Read/Write in Admin Mode

Admin can override a User-set Read-Only state by enabling Read/Write using the Admin PIN. Setting to Read-Write does not unlock the Drive.

STEPS	LED	ERROR STATE
Press and hold down **1-and then press-**🔑.		-
Enter the **Admin PIN**.		-
Press 🔑 🔑.		 - if error, the red LED fades out then turns solid.
Wait for  , then press 🔑 🔑 🔑.		-
Press **7, 9.** (**R,W** for Read/Write).		-
Press 🔑.	 - briefly, then →  fast +  slow	If an error occurs:  fast +  slow

If successful, the next time the Drive is unlocked it will be in R/W Mode as indicated by the **solid** green LED.

Setting the Timeout Lock in Admin Mode

To protect against unauthorized access when the Drive is connected to a computer and idle, it can be set to automatically lock after a preset amount of time.

In its default state, the **Timeout Lock** feature is turned off. It can be set to activate (lock the Drive) any time between 1 and 99 minutes. Admin **Timeout Lock** settings will override User settings.

STEPS	LED	ERROR STATE
Press and hold down **1-and then press-🔑.**		-
Enter the **Admin PIN**.		-
Press 🔑 🔑.		- if error, the red LED fades out then turns solid.
Wait for  , then press 🔑 🔑 🔑.		-
Press **8, 5**. (T, L for Timeout Lock).		-
Press 🔑.		If an error occurs:  fast +  slow
Enter the length of unattended time for Timeout. Two digits required. **Examples:** 01 = 1 minute 99 = 99 minutes		-
Press 🔑.	 - briefly, then →  fast +  slow	If an error occurs:  fast +  slow

If successful, the Timeout Lock is now set.

Disabling the Timeout Lock in Admin Mode

Follow the same steps for setting the Timeout Lock (above) and enter **00** for the time delay. The **Timeout Lock** will be disabled.

SECTION 4: Managing the Drive

The following headings discuss important, though less common, actions for managing your Drive. Except where noted, all procedures assume your Drive is connected to a computer and locked (red LED).

Verifying which PINs have Been Set

To determine which PINs have been set:

Press 🔑 ; These LEDs display for 10 seconds:

- No PIN exists. [🔒]
- Only User PIN exists. [🔒]
- Only Admin PIN exits. [▬]
- Both PINs exist. [🔒 ▬]

Deleting all Files in Admin Mode

An Administrator can delete all data stored on the Drive including User settings and PIN. All Admin settings (and only the Admin settings) will remain on the Drive. For further use, the Drive will need to be reformatted. For reformatting, refer to *Reformatting the Drive* on page 16.

CAUTION: The 'Delete All' procedure deletes all data, User settings, and formatting. The Drive must be reformatted for further use.

Note: All procedures under this heading start with the Drive plugged into a computer. Each step in all procedures below has a 10 second window to start the step after it. In general, a resulting status (indicated by the LEDs) times out after 10 seconds.

STEPS	LED	ERROR STATE
With the Drive locked, press and hold down **1-and then press-**🔑.	🔒 🔓	-
Enter the **Admin PIN**.	🔒 🔓	-
Press 🔑 🔑.	🔒	🔒 - if error, the red LED fades out then turns solid.
Wait for 🔒 🔓, then press 🔑 🔑 🔑.	▬ 🔓	-
Press **3, 2.** (**D, A** for Delete All)	▬ 🔓	-
Press 🔑.	🔒↔🔓 alternating	If an error occurs: 🔓 fast + 🔒 slow
Enter the **Admin PIN** again.	🔒↔🔓 alternating	-
Press 🔑.	🔒 - momentarily, then → 🔓 fast + 🔒 slow	If an error occurs: 🔒 - briefly, then → 🔓 fast + 🔒 slow

All data and User settings have now been deleted from the Drive.

Brute Force Hacking Detection

Entering a User PIN

Status: Both Admin and User PINs have been created.

If a User enters an incorrect User PIN ten consecutive times, regardless of the time intervals in-between attempts, the Drive's brute force detection will trigger and **the User PIN will be deleted**. All data remains on the Drive and can be accessed by the Admin after entering the correct Admin PIN.

Status: Only User PIN has been created.

If a User enters an incorrect User PIN ten consecutive times regardless of the time intervals in between attempts, the Drive's brute force detection triggers and the **User PIN and encryption key will be deleted and all data will become inaccessible and lost forever**. The Drive will need to be formatted before it can be reused. Refer to *Reformatting the Drive* on page 16.

Entering an Admin PIN

Status: Admin PIN, or Admin and User PINs have been created.

If an Admin enters an incorrect Admin PIN ten consecutive times, regardless of the time intervals in-between attempts, the Drive's brute force detection triggers and **both the User and Admin PINs and the encryption key will be deleted and all data will become inaccessible and lost forever**. The Drive will need to be formatted before it can be reused.

This table illustrates the different PIN states and what happens when Hacking Detection triggers.

PIN attempted to use to unlock	PINs setup on the USB at the time	After 10 consecutive incorrect PIN entries, the brute force mechanism triggers and does this:
User PIN	Admin & User PINs	The User PIN will be deleted. All data will remain on the USB and can only be accessed by the Admin entering the correct Admin PIN.
User PIN	User PIN Only	The encryption key will be deleted, and all data will be inaccessible and lost forever including the PINs.
Admin PIN	Admin & User PINS	
Admin PIN	Admin PIN Only	

Resetting (Deleting) the Drive

CAUTION: Resetting the Drive will delete all data stored on it including both PINs. After Resetting, the Drive must be formatted (initialized).

In the event that both the Admin and User PINs have been forgotten, or you want to delete all data stored on the Drive including the PINs, you can perform the following Reset function. It also removes the encryption, requiring the Drive to be reformatted—to format the Drive refer to the heading *Reformatting the Drive* on page 16.

STEPS	LED	ERROR STATE
With Drive locked, press and hold down **7**-and then press 🔑.	alternating	-
Press **999.**	alternating	-
Press and hold down **7**-and then press 🔑.	& momentarily	- if error, the red LED fades out then turns solid.

The Drive is now blank and locked.

Creating a User PIN after a Reset (Blank Drive)

Follow this procedure when the Drive is blank: such as after it has been reset or Hacking Detection has triggered.

STEPS	LED	ERROR STATE
Connect the Drive to your computer with the USB cable.	-	-
Press 🔑.		-
Wait four (4) seconds, press 🔑🔑.		-
Enter new User PIN.		-
Press 🔑🔑.		-
Re-enter the new User PIN.		-
Press 🔑🔑.	Fades out →	If error: Fades out →

Note that the Drive still requires formatting.

Reformatting the Drive

In the event that hacking detection has been triggered or the Drive has been reset, all data on the Drive will be lost forever. The Drive must then be reformatted.

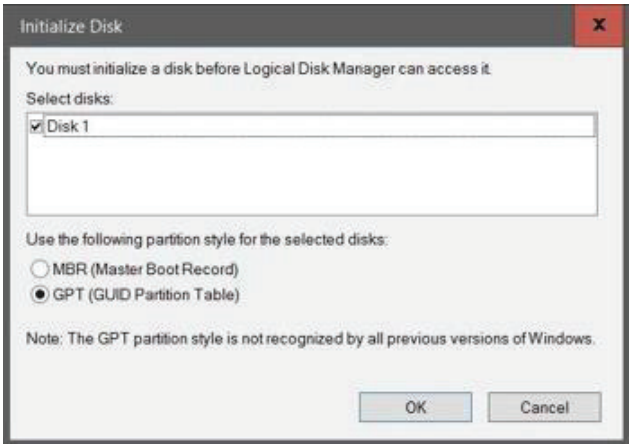
CAUTION: Loss of data. All data and settings will be deleted from the Drive when formatted, whether or not the Brute Force Hacking Detection was triggered or not.

To initialize (reformat) your SecureDrive, do the following:

For a Windows OS

Admin permission on the PC is required for this procedure.

1. Connect the Drive to your computer with the USB cable.
2. Unlock the drive with either User or Admin PIN. (To create a User PIN if you have not already done so, see *Creating a User PIN after a Reset (blank Drive)* on page 15.)
3. Open **Explorer**.
4. Right-click **This PC** > Left-click **Manage**.
5. In the Computer Management dialog's left column, click **Storage** > **Disk Management** and wait for it to populate.
6. If the Initialize Disk dialog doesn't popup, Right-click the 'Unknown' (or 'Not Initialized'), and click **Initialize** disk.
7. Make sure **GPT** is selected and then click **OK**.

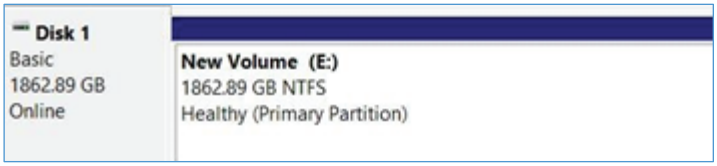


Note: GPT is needed for drives larger than 2 TB. For drives less than 2 TB, use the MBR option.

8. After **Unknown** changes to **Online**, right-click near **Unallocated** > **New Simple Volume**.
9. Follow the Wizard prompts. Select a **Drive letter** (it generally defaults to the next available letter) and then follow the prompts in the Wizard.
10. At the **Format Removable Disk** dialog, select a **Volume** Label, and select the appropriate file system.
11. Continue to follow the prompts.

Note: While the SecureDrive is formatting the blue LED blinks.

12. Click **Finish** to end and close the Wizard.



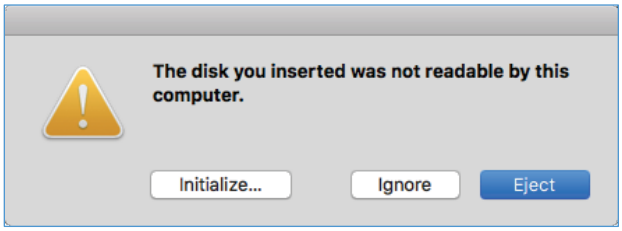
The SecureDrive is displayed here as "Disk 1."
It is Online and allocated (Healthy) and ready for use.

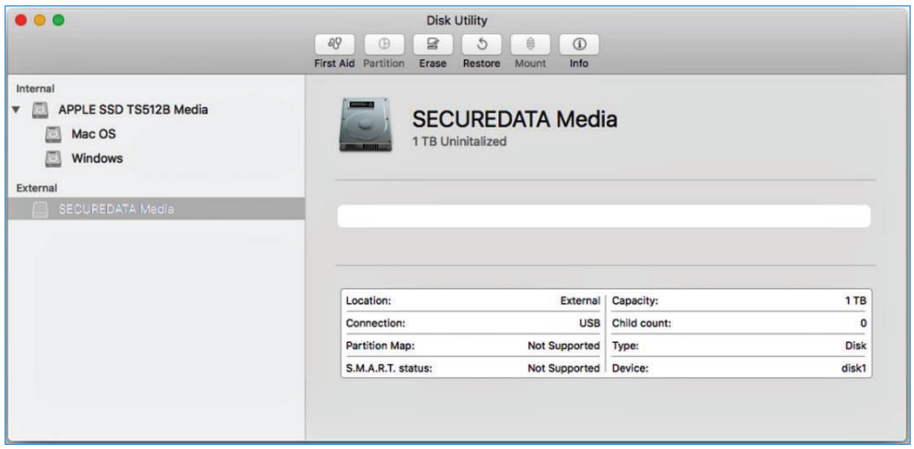
13. Close the Computer Management dialog if it's still open.

When finished the New Volume reads Healthy and Explorer window opens to display the Drive contents. The SATA blue and Green LED lights.

For Mac OS

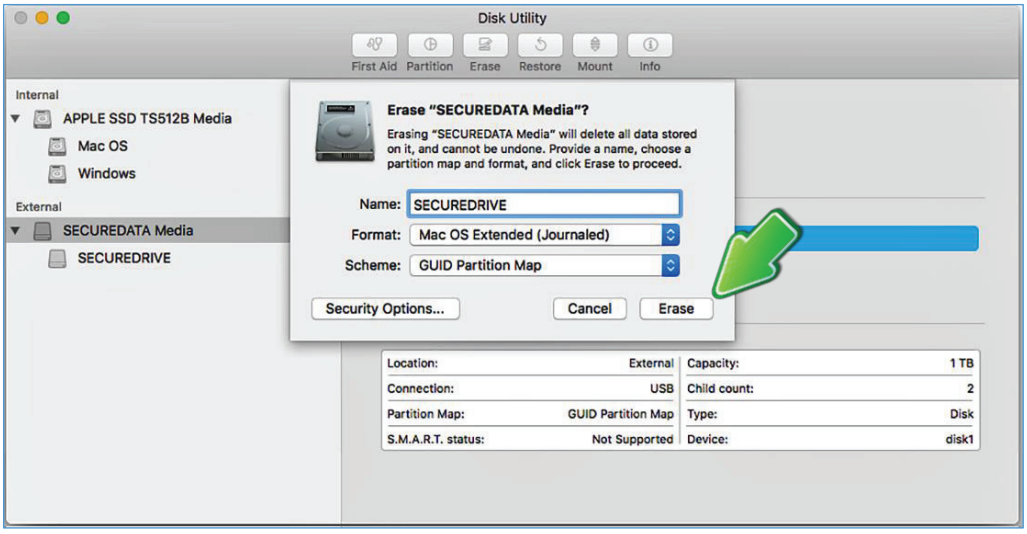
1. Connect to a Mac computer's USB port.
2. Unlock the drive with either **User** or **Admin PIN**. (To create a User PIN if you have not already done so, see *Creating a User PIN after a Reset (blank Drive)* on page 15.)
3. Click **Initialize** in the popup message (shown below). The Disk Utility Dialog displays.

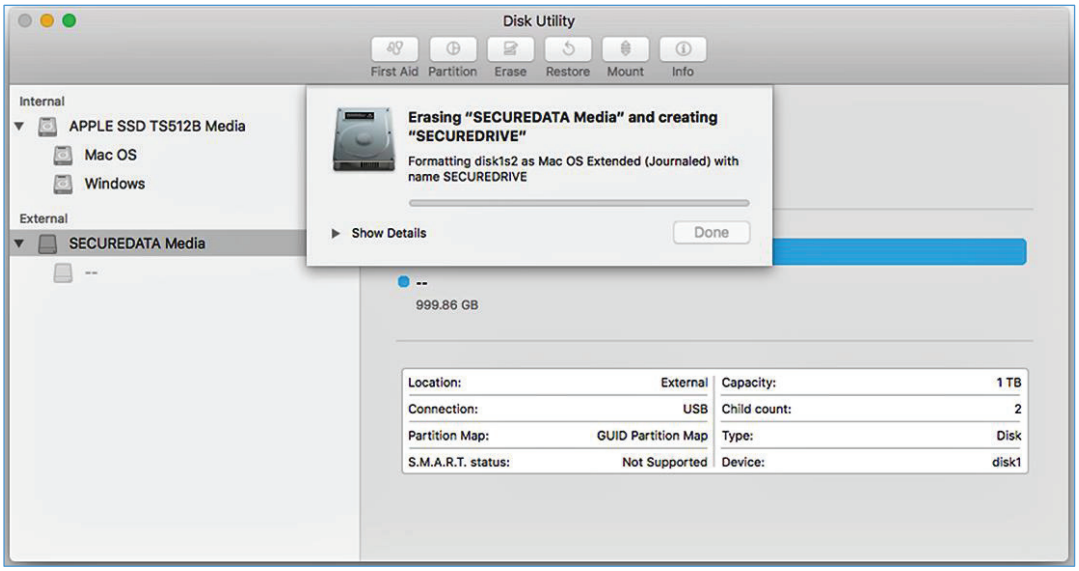


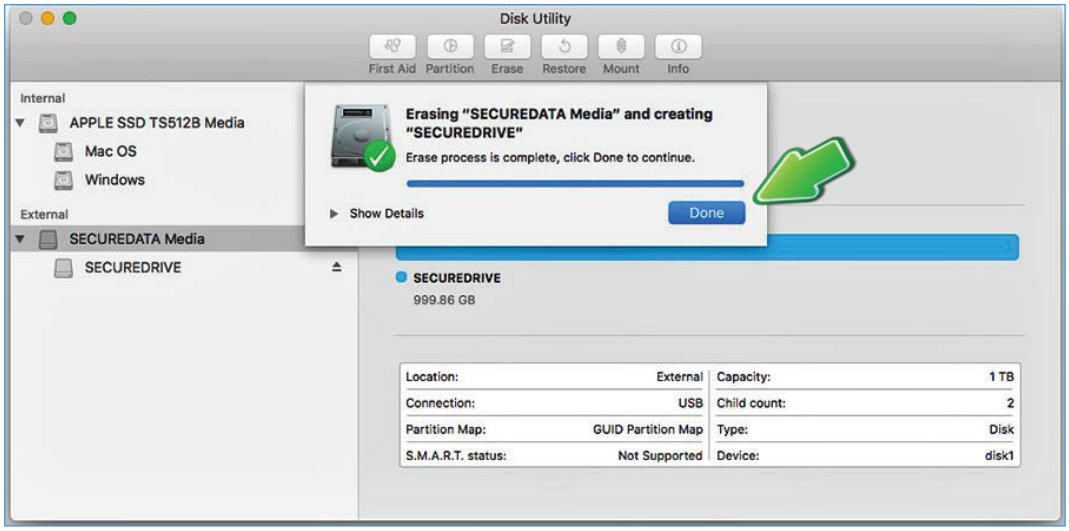


The Disk Utility Dialog. Make sure the correct drive is highlighted. (There is only one External drive listed in this image).

4. Click **Erase**. The system begins erasing the external Drive.







SecureDrive displays under the list of External Drives when done (as well as on the desktop).

5. Click **Done** in the message dialog when available.

Note: SecureDrive is now displayed under **External** in the left column.

6. Close the **Disk Utility**.

Troubleshooting

After unlocking the Drive, your computer shows that the external Drive is connected (icon displays) but you cannot access the Drive data (it doesn't display in Explorer (Windows) or Finder (Mac).

The Drive needs to be formatted—no data exists. It may have been reset. To format the Drive Refer to *Reformatting the Drive* on page 16.

If you think your keypad is faulty, contact Technical Support, page 20.

Determining the Version Number

In User Mode:

STEPS	LED
With the Drive locked, press .	
Enter your **User PIN**.	
Press	
Wait for , then press .	
Press **8, 6.** (**V, N** for Version Number)	
Press .	All LEDs Blink Once Together

Then the Red will blink the number of times that represent the major version number (left of the decimal point), and the Green will blink the number of times that represent the update version (right side of the decimal point). When the sequence has ended All LEDs blink once together, then .

EXAMPLE: if the version number is 1.7, the red LED will blink once and the green LED will blink seven times.

In Admin Mode:

STEPS	LED
Press and hold down **1-and then press-.**	
Enter your **Admin PIN**.	
Press	
Wait for , then press .	
Press **8, 6.** (**V, N** for Version Number)	
Press .	All LEDs Blink Once Together

SECTION 5: CONTACT AND WARRANTY INFORMATION

LIMITED WARRANTY

This Limited Warranty is provided by Rocstorage, Inc. (hereinafter: Rocstor) for all lines of products.

General Terms

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, ROCSTOR MAKES NO OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARCTICULAR PURPOSE. ROCSTOR EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITA TIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU.

This Limited Warranty applies to the Rocstor branded hardware products sold by or leased from Rocstorage, Inc., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this Limited Warranty as "Rocstor") with this Limited Warranty. This Limited Warranty is applicable in all countries and may be enforced in any country where Rocstor or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements in the country of purchase.

Rocstor warrants that the Rocstor hardware product and all the internal components of the product that you have purchased or leased from Rocstor are free from defects in materials or workmanship under normal use during the Limited Warranty Period. The Limited Warranty Period starts on the date of purchase or lease from Rocstor. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your Rocstor branded hardware is required within the Limited Warranty Period. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee.

Rocstor products are manufactured using new materials or new and used materials equivalent to new in performance and reliability. Spare parts may be new or equivalent to new. Spare parts are warranted to be free from defects in material or workmanship for thirty (30) days or for the remainder of the Limited Warranty Period of the Rocstor hardware product in which they are installed, whichever is longer.

Rocstor's Obligation under the Limited Warranty

During the Limited Warranty Period, Rocstor will repair or replace the defective component parts or the hardware product. All component parts or hardware products removed under this Limited Warranty become the property of Rocstor. The replacement part or product takes on either the Limited Warranty status of the removed part or product or the thirty (30) day limited warranty of the spare part. In the unlikely event that your Rocstor product has a recurring failure, Rocstor, at its discretion, may elect to provide you with a replacement unit of Rocstor's choosing that is at least equivalent to your Rocstor branded product in hardware performance. Rocstor reserves the right to elect, at its sole discretion, to give you a refund of your purchase price or lease payments (less interest) instead of a replacement. This is your exclusive remedy for defective products.

The original Limited Warranty is not extended when the product, or a part of the product, is repaired or replaced during the Limited Warranty period. Rocstor shall not be responsible or liable for backing up any data that is on a drive being returned for service

YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION, OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY, OR PERSONAL INFORMATION. ROCSTOR IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA, OR REMOVABLE STORAGE MEDIA. ROCSTOR IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTOR WHEN THE PRODUCT WAS MANUFACTURED.

Rocstor does not warrant that the operation of this product will be uninterrupted or error-free. Rocstor is not responsible for damage that occurs as a result of your failure to follow the instructions that came with the Rocstor branded product.

This Limited Warranty does not apply to expendable parts. This Limited Warranty does not extend to any product from which the serial number has been removed or that has been damaged or rendered defective (a) as a result of accident, misuse, abuse, or other external causes; (b) by operation outside the usage parameters stated in the user documentation that shipped with the product and/or posted on the Rocstor website; (c) by the use of parts not manufactured or sold by Rocstor; (d) as a result of normal wear; or (e) by modification or service by anyone other than (i) Rocstor, (ii) a Rocstor authorized service provider, or (iii) your own installation of end-user replaceable Rocstor or Rocstor approved parts if available for your product in the servicing country.

These terms and conditions constitute the complete and exclusive limited warranty agreement between Rocstor and you regarding the Rocstor branded product you have purchased or leased. These terms and conditions supersede any prior agreements or representations including representations made in Rocstor sales literature or advice given to you by Rocstor or an agent or employee of Rocstor-that may have been made in connection with your purchase or lease of the Rocstor branded product. No change to the conditions of this Limited Warranty is valid unless it is made in writing and signed by an authorized representative of Rocstor.

Buyer's Obligation under the Warranty

The person requesting coverage under this warranty shall prove that he or she is the original purchaser and declares that the product has not been sold, leased, bartered or otherwise changed possession. **The purchaser shall frequently backup the Rocpro hard drive and backup the data immediately prior to returning the drive for warranty service.**

The buyer must notify Rocstor and show proof of notification, through any reasonable means of communication. See full street address email address and toll free phone numbers below or updated contact information are available on Rocstor.com website. The notification shall identify any defect, malfunction, or nonconformity promptly upon discovery. Rocstor will acknowledge receipt of the communication and issue a Return Merchandise Authorization (RMA) code. The buyer is obligated to securely and safely package(s) the product, preferably in the original packing materials, WITH THE RMA number, and deliver it together with a copy of the original purchase receipt and a description of the problem to the Rocstor home office. Buyer is responsible for the product until it is received by Rocstor. It is recommended that the product be insured during transportation by the sender. You must prepay any shipping charges, taxes, or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

Limitation of Damages (Liability)

IF YOUR ROCSTOR BRANDED HARDWARE PRODUCT FAILS TO WORK AS WARRANTED ABOVE, THE ORIGINAL PURCHASER'S SOLE AND EXCLUSIVE REMEDY SHALL BE REPAIR OR REPLACEMENT. ROCSTOR'S MAXIMUM LIABILITY UNDER THIS LIMITED WARRANTY IS EXPRESSLY LIMITED TO THE LESSER OF THE PRICE YOU HAVE PAID FOR THE PRODUCT OR THE COST OF REPAIR OR REPLACEMENT OF ANY ROCSTOR HARDWARE COMPONENTS THAT MALFUNCTION IN CONDITIONS OF NORMAL USE. ROCSTOR IS NOT LIABILE FOR ANY DAMAGE TO ANY OTHER PRODUCT CONNECTED TO A ROCSTOR PRODUCT.

Limitation on Consequential Damages

ROCSTOR IS NOT LIABLE FOR ANY DAMAGES CAUSED BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY LOST PROFITS OR SAVINGS OR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES. ROCSTOR IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY. THIS LIMITATION OF LIABILITY ALSO APPLIES WHETHER DAMAGES ARE SOUGHT OR A CLAIM IS MADE UNDER THIS LIMITED WARRANTY OR AS A TORT CLAIM (INCLUDING NEGLIGENCE AND STRICT PRODUCT LIABILITY), A CONTRACT CLAIM OR ANY OTHER CLAIM. THIS LIMITATION OF LIABILITY CANNOT BE WAIVED OR AMENDED BY ANY PERSON. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF YOU HAVE ADVISED ROCSTOR OR AN AUTHORIZED REPRESENTATIVE OF ROCSTOR OF THE POSSIBILITY OF ANY SUCH DAMAGES.

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR A FULL DETERMINATION OF YOUR RIGHTS.

Disclaimer

We accept no liability for any loss of data, damages and the inability of Rocstor products to work with any third party equipment. Nor can Rocstor accept any liability or responsibility for software or third party hardware products.

Limited Warranty Period

The limited warranty period for the **DataSecure** is four (4) Year Parts and Labor. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee

Types of Limited Warranty Service

Your Rocstor Limited Warranty consists of repair or replacement of defective parts, including hard drives identified by Rocstor Support Organization as "pre-failure".

Carry-in Limited Warranty Service Available Monday - Friday

Under the terms of carry-in service, you may be required to deliver your Rocstor product to the Rocstor Service Center or an authorized service location for warranty repair. You must prepay any shipping charges, taxes or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION. ROCSTORAGE IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA OR REMOVABLE STORAGE MEDIA. ROCSTORAGE IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTORAGE WHEN THE PRODUCT WAS MANUFACTURED.

Rocstorage shall not be responsible or liable for backing up any data that is on a drive being returned for service. Expect that all data on the drive will be destroyed and not retrievable when returned for warranty service.

Rocstor Replaceable Parts Program

Where available, the Rocstor Replaceable Parts program ships approved replacement parts directly to you to fulfill your warranty. This will save considerable repair time. After you call the Rocstor Technical Support Center at **888.877.8777** a replaceable part can be sent directly to you. Once the part arrives, call the Rocstor Technical Support Center. A technician will assist you over the phone to ensure that the installation is quick and easy.

Service Upgrades

Rocstor offers extra coverage for your product. For information on service upgrades, visit www.rocstor.com.
Service upgrades purchased in one country are not transferable to another country.

Capacity Disclaimer

Actual accessible hard drive capacity will indicate up to 10% lower than stated under different Operating Systems and formatting.

The storage volume is measured in total bytes before formatting. References to round numbers of gigabytes or terabytes are an approximation only. For example, a disk drive labeled as having 500GB (Gigabytes) has space for approximately 500,000,000 bytes before formatting. After formatting, the drive capacity is reduced by about 5% to 10% depending on the operating system and formatting used or "1GB = 1,000,000,000 bytes.

Options and Software

The Limited Warranty terms and conditions for Rocstor options are as indicated in the Limited Warranty applicable to Rocstor options. ROCSTOR DOES NOT WARRANTY SOFTWARE PRODUCTS, INCLUDING ANY SOFTWARE PRODUCTS OR THE OPERATING SYSTEM PREINSTALLED BY ROCSTOR. Rocstor's only obligations with respect to software distributed by Rocstor under the Rocstor brand name are set forth in the applicable end-user license or program license agreement. Non-Rocstor hardware and software products are provided "AS IS" and without any Warranty. However, non-Rocstor manufacturers, suppliers or publishers may provide their own warranties directly to you.

The data stored in Rocstor and Rocsecure storage product lines are not guaranteed by Rocstor (or the hard disk manufacturer.) We are not responsible for any loss of data. Always back up data regularly

TECHNICAL SUPPORT

Software Technical Support

Software technical support is defined as assistance with questions and issues about the software that was either preinstalled by Rocstor on the Rocstor branded product or that was included with the Rocstor branded product at the time of your purchase or lease of the product. Technical support for software is available for the first ninety (90) days from date of product purchase or lease. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving software technical support. After the first ninety (90) days, technical support for software that was either preinstalled by Rocstor on the Rocstor branded product or included with the Rocstor branded product at the time of your purchase or lease of the product is available for a fee.

WARNING: **The individual user should take care to determine prior to use whether this device is suitable, adequate or safe for the use intended. Since individual applications are subject to great variation, the manufacturer "Rocstor" makes no representation or warranty as to the suitability or fitness of these devices for any specific application**.

Technical Support

The Rocpro T34Bay RAID is backed by free telephone technical support for two (2) years from the date of purchase. Please register your product with Rocstor. To register, fill in the Limited Warranty Registration form in the Support tab at www.rocstor.com.

Free telephone technical support is available weekdays from 9 AM until 6 PM Pacific Standard Time. Customers in the United States and Canada can call toll-free: **(888) 877-8777**; all others must call **(818) 449-2000**.
When calling for support, please have the product's serial number (printed on the label on the bottom of the drive) and system hardware information available.

TRADEMARKS ACKNOWLEDGEMENTS

CONTACT INFORMATION

Technical Support / RMA
Hours: 9:00 am - 5:00 pm PST
Mon - Fri (excluding holidays)

Tell: +1 (818) 727-7000 (Domestic and Internationals)
Fax: +1 (818) 875-0002
Email: support@Rocstor.com

Corporate, Government and Academic Customers
Our Corporate Sales Team's goal is to help our U.S.A. and Canadian customers find a storage solution that best serves their needs. We will help you determine your best purchasing options. For more information please contact the appropriate department below or call us at +1 (818) 727-7000.

General sales information: sales@Rocstor.com
Corporate sales information: corporate_sales@Rocstor.com
Educational sales information: academic_sales@Rocstor.com
Federal, State & Local government sales information: government_sales@Rocstor.com

Resellers/Business Development/OEM Partners
All Channel National and International Resellers, VARs, Consultants …
contact Rocstor Channel Sales: call: +1 (818) 727-7000
Email: reseller_info@Rocstor.com

*FIPS 140-2 Level 3 Validated Certificate (cert. #3297) under Securedata, Inc. SecureDrive KP Model.

Assembled and integrated in U.S.A. using domestic and / or foreign components.

FC CE RoHS