

USER MANUAL

diskAshur DT²®



Please make sure you remember your PIN (password), without it there is no way to access the data on the drive.

If you are having difficulty using your diskAshur DT² drive please contact our technical department by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage, Inc 2017. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

iStorage diskAshur DT² Manual – v.2.1



FC CE RoHS

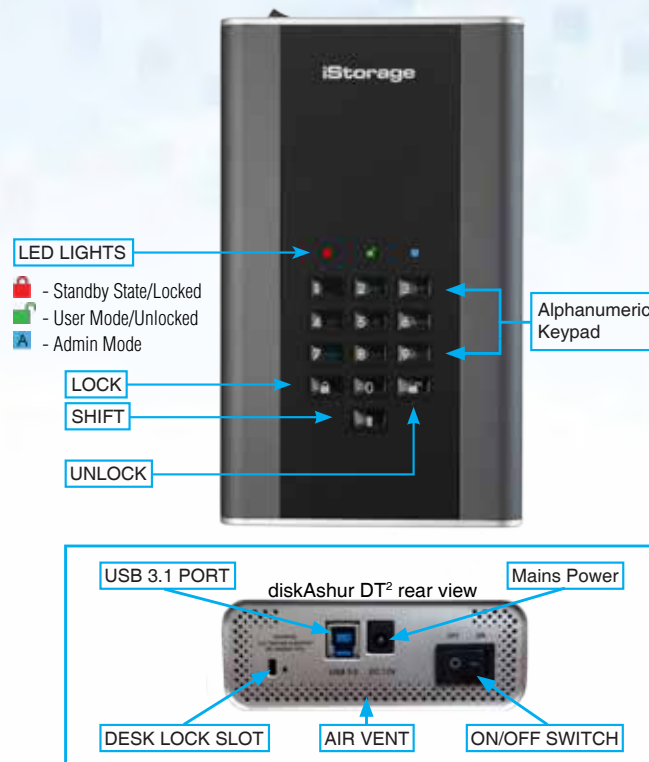
All trademarks and brand names are the property of their respective owners

Trade Agreements Act (TAA) Compliant



Table of Contents

Introduction	4
Box Contents	4
1. diskAshur DT ² Layout	5
2. Connecting your diskAshur DT ²	6
3. diskAshur DT ² LED States	7
4. How to use the diskAshur DT ² for the first time	7
5. Unlocking the diskAshur DT ²	8
6. Locking the diskAshur DT ²	8
7. Entering Admin Mode	8
8. Changing the Admin PIN	9
9. Setting a User PIN Policy	10
10. How to check the User PIN Policy	11
11. Adding a new User PIN in Admin Mode	12
12. Changing the User PIN in Admin Mode	12
13. Deleting the User PIN in Admin Mode	12
14. Set Read-Only in Admin Mode	13
15. Enable Read/Write in Admin Mode	13
16. How to create a Self-Destruct PIN	13
17. How to delete the Self-Destruct PIN	14
18. How to Unlock with the Self-Destruct PIN	14
19. How to Create an Admin PIN after a Brute Force attack or Reset	15
20. Setting the Unattended Auto-Lock Clock	15
21. Turn off the Unattended Auto-Lock Clock	16
22. How to check the Unattended Auto-Lock Clock.....	16
23. How to Unlock diskAshur DT ² with User PIN	17
24. Changing the User PIN in User Mode	17
25. Set Read-Only in User Mode	18
26. Enable Read/Write in User Mode	18
27. Brute Force Protection	19
28. How to perform a complete reset	19
29. Initialising and formatting the diskAshur DT ²	20
30. diskAshur DT ² Setup for Mac OS	22
31. diskAshur DT ² Setup for Linux (Ubuntu 14.04)	24
32. Hibernating, Suspending or Logging off from the Operating System	27
33. How to check Firmware in Admin Mode	27
34. How to check Firmware in User Mode	28
35. Technical Support	29
36. Warranty and RMA information	29
Appendices	
A. iStorage Security Directive #1 – Product Security Features & Secure Handling	30
B. iStorage Security Directive #2 – Sanitisation and Secure Disposal.....	34



Introduction

The diskAshur DT² is an easy to use, ultra-secure, hardware encrypted desktop hard drive with capacities of up to 8TB. Simply switch the power on and connect the USB 3.1 cable to any computer and enter a 7-15 digit PIN, if the correct PIN is entered, all data stored on the drive will be decrypted and accessible. To lock the drive and encrypt all data, simply eject the diskAshur DT² from the host computer and the entire contents of the drive will be encrypted (full disk encryption) using military grade AES 256-bit hardware encryption (XTS mode). If the drive is lost or stolen and an incorrect PIN is entered 15 consecutive times, the drive will reset, the encryption key will be deleted and all data previously stored on the drive will be lost forever.

One of the unique and underlying security features of the GDPR compliant diskAshur DT² is the dedicated hardware based secure microprocessor (Common Criteria EAL4+ ready), which employs built-in physical protection mechanisms designed to defend against external tamper, bypass attacks and fault injections. Unlike other solutions, the diskAshur DT² reacts to an automated attack by entering the deadlock frozen state, which renders all such attacks as useless. In plain and simple terms, without the PIN there's no way in!

Box Contents

1. diskAshur DT² Drive
2. USB Cable
3. Universal Mains Adapter
4. Quick Start Guide

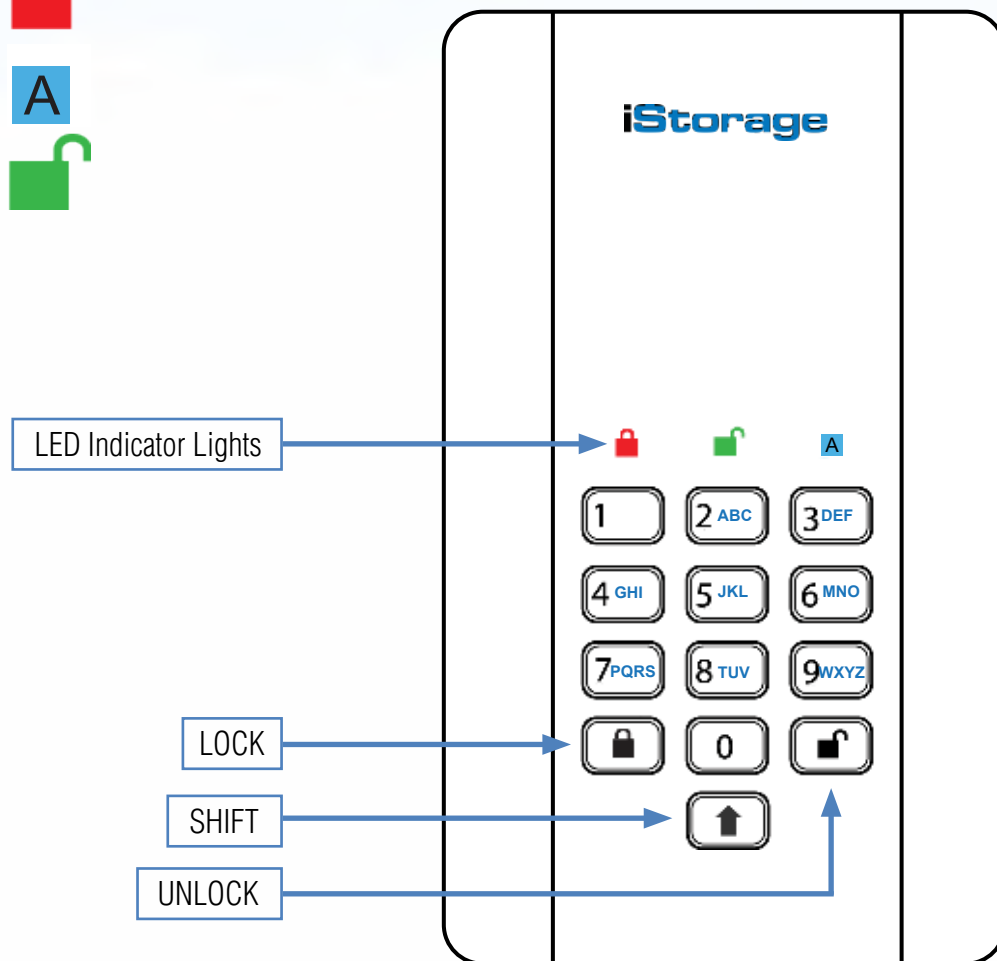
1. diskAshur DT² Layout

The indicator light displays the following colours to indicate the various modes of operation:

RED: Standby Mode 

BLUE: Admin Mode 

GREEN: User Mode 



The “**UNLOCK**” button is used to access the diskAshur DT² and it can also be used as an OK acknowledgement in the following operations:

- Entering a PIN
- Confirming a new PIN
- Accessing various command settings

The “**SHIFT**” button can be used for additional combinations. **SHIFT + 1** is a separate value than just **1**. To create a PIN using additional combinations, press and hold down the SHIFT button whilst entering your 7-15 digit PIN. e.g. SHIFT + 26756498.

To lock diskAshur DT² and return it to Standby State () press the “**Lock**” button.

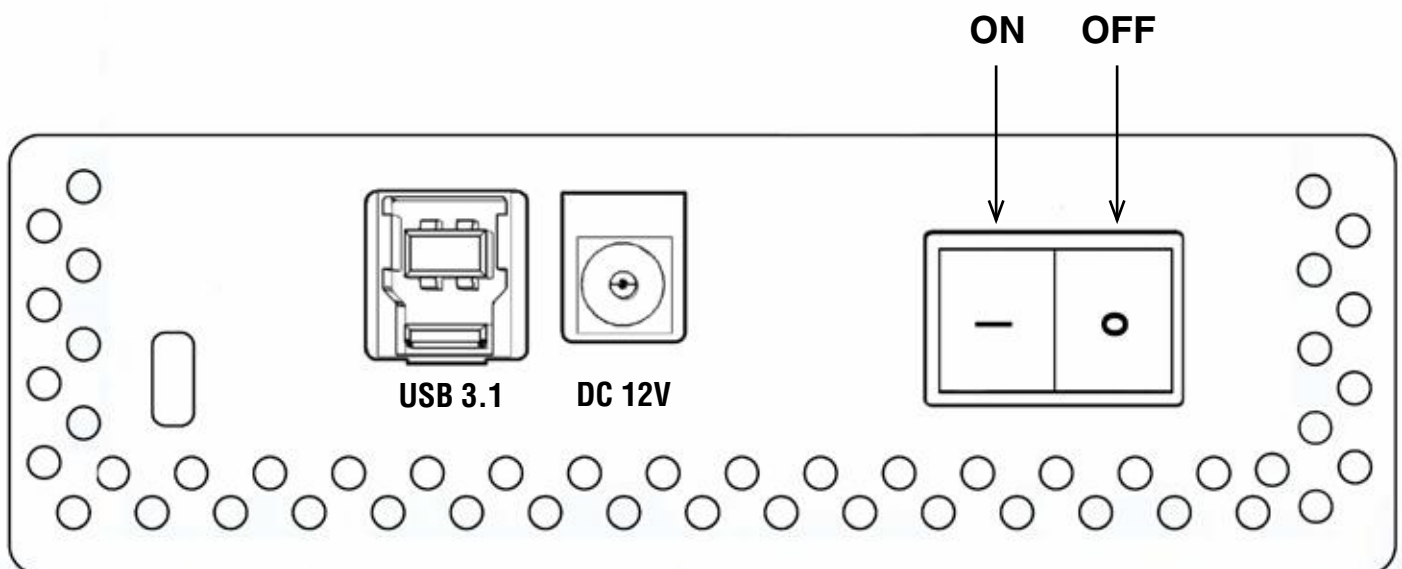
2. Connecting your diskAshur DT²

Be sure to read the following information before you begin to use the diskAshur DT².



Attention: Use only the cables provided with your diskAshur DT².
You may damage the drive if you use a cable not included with the diskAshur DT².

1. Ensure that the power switch on the back of the diskAshur DT² is in the **OFF** position.
2. Connect the diskAshur DT² to a power outlet using the included AC Adapter.
3. Attach the USB cable to the diskAshur DT² drive and to an available USB port on your computer.
4. Turn the power switch on the back of the diskAshur DT² to the **ON** position.
5. The LED indicator light should turn **RED**, indicating that the drive is now ready to use.



3. diskAshur DT² LED States

When the diskAshur DT² is plugged in, there are three possible behaviours for the LED indicators as shown in the table below.



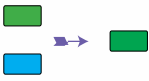
RED	GREEN	BLUE	diskAshur DT ² State
Solid	Off	Off	Factory Reset ¹
Solid	Solid	Solid	Brute Force ²
Solid	Off	Off	Standby ³

1. In Factory Reset State, the drive is waiting for the operation to set up an Admin PIN.
2. In Brute Force state, the drive is waiting for an operation to get more PIN entry attempts.
3. In Standby state, the drive is waiting for an operation to unlock the drive, or enter Admin mode, or reset the drive.

4. How to use the diskAshur DT² for the first time

The diskAshur DT² is shipped with a default Admin PIN of **11223344** and although it can be used straight out of the box with the default Admin PIN, for security reasons we **highly recommend a new Admin PIN be created immediately** by following the instructions under section 8 'Changing the Admin PIN'.

Please follow the 3 simple steps in the table below to unlock the diskAshur DT² for the first time with the default Admin PIN.

Instructions - first time use	LED	LED State
1. Connect the diskAshur DT ² to a USB port		RED LED will be solid awaiting PIN entry
2. Enter Admin PIN (default - 11223344)		RED LED remains solid
3. Within 10 seconds press the "UNLOCK" button once to unlock diskAshur DT ²		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN and finally solid GREEN LED



Note: Once the diskAshur DT² has been successfully unlocked, the GREEN LED will remain on and in a solid state. It can be locked down immediately by pressing the "LOCK" button once or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system. To ensure no data is corrupted, we recommend using 'Safely Remove Hardware/Eject'.

5. Unlocking the diskAshur DT²

The diskAshur DT² can be unlocked with either an Admin or User PIN whilst in standby state (solid RED LED).

1. To unlock as the Administrator, enter the **Admin** PIN and press the “**UNLOCK**” button.
2. To unlock as a **User**, first press the “**UNLOCK**” button (all LEDs, ■ ■ ■ blink on and off) and then enter the **User** PIN and press the “**UNLOCK**” button again.
3. If correct User PIN is entered, both **GREEN** and **BLUE** LEDs will blink alternately and then return to a solid **GREEN** LED.
4. If correct Admin PIN is entered, both **GREEN** and **BLUE** LEDs will blink alternately, then to a solid **BLUE** for 1 second and then to the unlocked state, a solid **GREEN** LED.
5. If correct PIN is entered, the drive displays as “iStorage diskAshur DT² USB Device” under “Computer Management/Device Manager”.

In an unlocked state (**GREEN** LED), there are two possible behaviours for the LED indicators, shown in the table below.

RED	GREEN	BLUE	diskAshur DT²
Off	Solid	Off	No data transfer
Off	Blink	Off	Data transfer in progress

6. Locking the diskAshur DT²


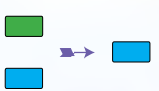
To lock the drive, press the “**LOCK**” button once or by clicking the ‘Safely Remove Hardware/Eject’ icon within your operating system. If data is still being written to the drive, please wait until all data has been written to the drive before pressing the ‘**LOCK**’ button or safely ejecting from the Operating System. When the unattended Auto-Lock timeout is activated, the drive will automatically lock after a predetermined amount of time.



Note: The diskAshur DT² cannot be recognized by the operating system in standby state.

7. Entering Admin Mode

To enter the Admin Mode, do the following:

1. In standby state (solid RED LED), press and hold down “ UNLOCK + 1 ” buttons		Solid RED LED will change to blinking GREEN and BLUE LEDs
2. Enter the Admin PIN (default - 11223344) and press “ UNLOCK ” button		GREEN and BLUE LEDs blink rapidly together for a few seconds then to a solid GREEN and finally a solid BLUE LED indicating the diskAshur DT ² is in “Admin Mode”

To exist Admin mode, press the “**LOCK**” button.

8. Changing the Admin PIN

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- Must 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)

Password Tip: You can create a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

- For “password” you would press the following keys:
7 (pqrs) 2 (abc) 7 (pqrs) 7 (pqrs) 9 (wxyz) 6 (mno) 7 (pqrs) 3 (def)
- For “istorage” you would press:
4 (ghi) 7 (pqrs) 8 (tuv) 6 (mno) 7 (pqrs) 2 (abc) 4 (ghi) 3 (def)

Using this method, long and easy to remember PINs can be created.



Note: The **SHIFT** key can be used for additional combinations. **SHIFT** + 1 is a separate value than just 1. To create a PIN using additional combinations, press and hold down the **SHIFT** button whilst entering your 7-15 digit PIN. e.g. **SHIFT** + 26756498.

To change the Admin PIN, first enter the “Admin Mode” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode, press and hold down “ UNLOCK + 2 ” buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter NEW Admin PIN and press “ UNLOCK ” button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the NEW Admin PIN and press “ UNLOCK ” button		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking BLUE LED and finally to a solid BLUE LED indicating the Admin PIN has been successfully changed

9. Setting a User PIN Policy

The Administrator can set a restriction policy for the User PIN. This policy includes setting the minimum length of the PIN (from 7 to 15 digits), as well as requiring or not the input of a '**Special Character**'. The "Special Character" functions as '**Shift + digit**'.

To set a User PIN Policy (restrictions) you will need to enter 3 digits, for instance '**091**', the first two digits (**09**) indicate the minimum PIN length (in this case, **9**) and the last digit (**1**) denotes that a 'Special Character' must be used, in other words '**Shift + digit**'. In the same way, a User PIN Policy can be set without the need of a 'Special Character', for instance '**120**', the first two digits (**12**) indicate the minimum PIN length (in this case, **12**) and the last digit (**0**) meaning no Special Character is required.

Once the Administrator has set the User PIN Policy, for instance '091', a new User PIN will need to be created. If the Administrator creates the User PIN as '**247688314**' with the use of a '**Special Character**' (Shift+digit), this can be placed anywhere along your 7-15 digit PIN during the process of creating the User PIN as shown in the examples below.





- A. '**Shift + 2**', '4', '7', '6', '8', '8', '3', '1', '4',
- B. '2', '4', '**Shift + 7**', '6', '8', '8', '3', '1', '4',
- C. '2', '4', '7', '6', '8', '8', '3', '1', '**Shift + 4**',



Note:

- If a 'Special Character' was used during the creation of the User PIN, for instance, example '**A**' above, then the drive can only be unlocked by entering the PIN with the 'Special Character' entered precisely in the order created, as per example '**A**' above - ('**Shift + 2**', '4', '7', '6', '8', '8', '3', '1', '4').
- Users are able to change their PIN but are forced to comply with the set 'User PIN Policy' (restrictions), if and when applicable.
- Setting a new User PIN Policy will automatically delete the User PIN if one exists.
- This policy does not apply to the 'Self-Destruct PIN'. The complexity setting for the Self-Destruct PIN and Admin PIN is always 7-15 digits, with no special character required.



To set a **User PIN Policy**, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode, press and hold down “ UNLOCK + 7 ” buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter your 3 digits , remember the first two digits denote minimum PIN length and last digit (0 or 1) whether or not a special character has been used.		Blinking GREEN and solid BLUE LEDs will continue to blink
3. Press the “ SHIFT ” button  once		Blinking GREEN and Solid BLUE will change to a solid GREEN LED and finally to a solid BLUE LED indicating the User PIN Policy has been successfully set.

10. How to check the User PIN Policy

The Administrator is able to check the User PIN Policy and can identify the minimum PIN length restriction and whether or not the use of a Special Character has been set by noting the LED sequence as described below.

To check the User PIN Policy, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode press and hold down SHIFT () + 7		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the “ UNLOCK ” button and the following happens; <ol style="list-style-type: none"> All LED's (RED, GREEN & BLUE) become solid for 1 second. A RED LED blink equates to ten (10) units of a PIN. Every GREEN LED blink equates to a single (1) unit of a PIN A BLUE blink indicates that a 'Special Character' was used. All LED's (RED, GREEN & BLUE) become solid for 1 second. LEDs return to solid BLUE 		

The table below describes the LED behaviour whilst checking the User PIN Policy, for instance if you have set a 12 digit User PIN with the use of a Special Character, the **RED** LED will blink once (**1**) and the **GREEN** will blink twice (**2**) followed by a single **BLUE** LED blink indicating that a **Special Character** must be used.

PIN Description	3 digit Setup	RED	GREEN	BLUE
12 digit PIN with use of a Special Character	121	1 Blink	2 Blinks	1 Blink
12 digit PIN with NO Special Character used	120	1 Blink	2 Blinks	0
9 digit PIN with use of a Special Character	091	0	9 Blinks	1 Blink
9 digit PIN with NO Special Character used	090	0	9 Blinks	0

11. Adding a new User PIN in Admin Mode

To add a **New User**, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode, press and hold down “ UNLOCK + 3 ” buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter New User PIN and press “ UNLOCK ” button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the New User PIN and press “ UNLOCK ” button		GREEN LED rapidly blinks for a few seconds then changes to a solid BLUE LED indicating the User PIN has been successfully created

12. Changing the User PIN in Admin Mode

To change an existing **User PIN**, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode, press and hold down “ UNLOCK + 3 ” buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter New User PIN and press “ UNLOCK ” button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the New User PIN and press “ UNLOCK ” button		GREEN LED rapidly blinks for a few seconds then changes to a solid BLUE LED indicating the User PIN has been successfully changed

13. Deleting the User PIN in Admin Mode

To delete a **User PIN**, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

1. In Admin mode, press and hold down “ SHIFT + 3 ” buttons and release		Solid BLUE LED will change to blinking RED LED
2. Press and hold down “ SHIFT + 3 ” buttons again.		Blinking RED LED will change to solid RED LED and then to a solid BLUE LED indicating the User PIN was successfully deleted

14. Set Read-Only in Admin Mode



Important: If data has just been copied to the diskAshur DT², make sure to properly disconnect the drive first by clicking 'Safely Remove Hardware/Eject' the diskAshur DT² from the Operating System before reconnecting and setting the diskAshur DT² as 'Read-Only/Write-Protect'.

When Admin writes content to the diskAshur DT² and restricts access to read-only, the User cannot change this setting in User mode. To set the diskAshur DT² to Read-Only, first enter the "Admin Mode" as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down "7 + 6" buttons. (7=Read + 6=Only)		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Release 7+6 buttons and press "UNLOCK"		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the drive is configured as Read-Only

15. Enable Read/Write in Admin Mode

To set the diskAshur DT² to Read/Write, first enter the "Admin Mode" as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down "7 + 9" buttons. (7=Read + 9=Write)		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Release 7+9 buttons and press "UNLOCK"		GREEN and BLUE LEDs change to a solid GREEN LED then to a solid BLUE LED indicating the drive is configured as Read/Write

16. How to create a Self-Destruct PIN



The self-destruct feature allows you to set a PIN which can be used to perform a crypto-erase on the entire drive. When used, the self-destruct PIN will **delete ALL data, Admin/User PINs** and then unlock the drive. Activating this feature will cause the Self-Destruct PIN to become the new User PIN and the diskAshur DT² will need to be partitioned and formatted before any new data can be added to the drive.

To set the Self-Destruct PIN, first enter the "Admin Mode" as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down "UNLOCK + 6" buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Create a 7-15 digit Self-Destruct PIN and press the "UNLOCK" button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the PIN and press the "UNLOCK" button		GREEN LED will rapidly blink for several seconds and then changes to a solid BLUE LED to indicate the Self-Destruct PIN has been successfully configured

17. How to Delete the Self-Destruct PIN

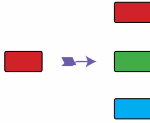
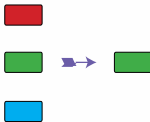
To delete the Self-Destruct PIN, first enter the “Admin Mode” as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down “SHIFT + 6” buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down “SHIFT + 6” buttons again		Blinking RED LED will become solid and then change to a solid BLUE LED indicating the Self-Destruct PIN was successfully deleted

18. How to Unlock with the Self-Destruct PIN

When used, the self-destruct PIN will **delete the encryption key, ALL data, Admin/User PINs** and then unlock the drive. Activating this feature will cause the **Self-Destruct PIN to become the new USER PIN** and the diskAshur DT² will need to be partitioned and formatted before any new data can be added to the drive.

To activate the Self-Destruct mechanism, the drive needs to be in the standby state (solid RED LED) and then proceed with the following steps.

1. In standby state, press the “UNLOCK” button		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter your Self-Destruct PIN and press the “UNLOCK” button		RED, GREEN and BLUE blinking LEDs will change to GREEN and BLUE LEDs alternating on and off for approximately 15 seconds and finally shifts to a solid GREEN LED



Important: When the Self-Destruct mechanism is activated, all data, the encryption key and the Admin/User PINs are deleted. **The Self-Destruct PIN becomes the User PIN.** No Admin PIN exists after the Self-Destruct mechanism is activated. The diskAshur DT² will need to be reset (see ‘How to perform a complete reset’ Section 28, on page 19) first in order to create an Admin PIN with full Admin privileges including the ability to create a User PIN.

19. How to Create an Admin PIN after a Brute Force attack or Reset




It will be necessary after a Brute Force attack or when the diskAshur DT² has been reset to create an Admin PIN before the drive can be used. If the drive has been brute forced or reset, the drive will be in a standby state (solid RED LED). to create an Admin PIN proceed with the following steps.

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- Must 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: The **SHIFT** key can be used for additional combinations. **SHIFT + 1** is a separate value than just 1. To create a PIN using additional combinations, press and hold down the **SHIFT** button whilst entering your 7-15 digit PIN. e.g. **SHIFT + 26756498**.

1. In Standby state, press and hold down “ SHIFT + 1 ” buttons		Solid RED LED will change to blinking GREEN and solid BLUE LEDs
2. Enter NEW Admin PIN and press “ UNLOCK ” button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the NEW Admin PIN and press “ UNLOCK ” button		Blinking GREEN LED and solid BLUE LED change to BLUE LED rapidly blinking for a few seconds and then to a solid BLUE LED indicating the Admin PIN was successfully configured.

20. Setting the Unattended Auto-Lock Clock


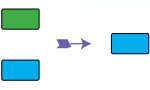
To protect against unauthorised access if the drive is unlocked and unattended, diskAshur DT² can be set to automatically lock after a pre-set amount of time. In its default state, the diskAshur DT² Unattended Auto Lock feature is turned off. The Unattended Auto Lock can be set to activate between 5 - 99 minutes.

To set the Unattended Auto Lock, first enter the “**Admin Mode**” as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down “ UNLOCK + 5 ” buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter the amount of time that you would like to set the Auto-Lock timeout feature for, the minimum time that can be set is 5 minutes and the maximum being 99 minutes (5-99 minutes). For example enter: 05 for 5 minutes 20 for 20 minutes 99 for 99 minutes		
3. Press the “ SHIFT ” button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out is successfully configured

21. Turn off the Unattended Auto-Lock Clock


To turn off the Unattended Auto Lock, first enter the “Admin Mode” as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down “UNLOCK + 5” buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter “00” and press the “SHIFT” button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out has been successfully switched off

22. How to check the Unattended Auto-Lock Clock

The Administrator is able to check and determine the length of time set for the unattended auto-lock clock by simply noting the LED sequence as described on the table at the bottom of this page.

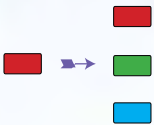
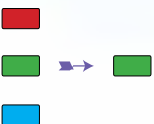
To check the unattended auto-lock, first enter the “Admin Mode” as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down SHIFT (↑) + 5		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the “UNLOCK” button and the following happens;		
<ol style="list-style-type: none"> All LED's (RED, GREEN & BLUE) become solid for 1 second. Each RED LED blink equates to ten (10) minutes. Every GREEN LED blink equates to one (1) minute. All LED's (RED, GREEN & BLUE) become solid for 1 second. LEDs return to solid BLUE 		

The table below describes the LED behaviour whilst checking the unattended auto-lock, for instance if you have set the drive to automatically lock after **26** minutes, the RED LED will blink twice (**2**) and the GREEN LED will blink six (**6**) times.

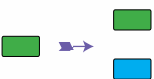
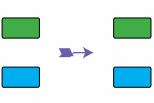
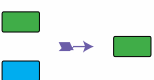
Auto-Lock in minutes	RED	GREEN
8 minutes	0	8 Blinks
15 minutes	1 Blink	5 Blinks
26 minutes	2 Blinks	6 Blinks
40 minutes	4 Blinks	0

23. How to Unlock diskAshur DT² with User PIN

<p>1. In the standby state (solid RED LED) Press the “UNLOCK” button</p>		<p>RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off</p>
<p>2. Enter User PIN and press the “UNLOCK” button</p>		<p>RED, GREEN and BLUE blinking LEDs will change to alternating GREEN and BLUE LEDs then to a rapidly blinking GREEN LED and finally shifts to a solid GREEN LED indicating drive successfully unlocked in User mode</p>

24. Changing the User PIN in User Mode

To change the **User PIN**, first unlock the diskAshur DT² with a User PIN as described above in section 23. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

<p>1. In User mode press and hold down “UNLOCK + 4”</p>		<p>Solid GREEN LED will change to a blinking GREEN LED and a solid BLUE LED</p>
<p>2. Enter New User PIN and press the “UNLOCK” button</p>		<p>Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs</p>
<p>3. Re-enter New User PIN and press the “UNLOCK” button</p>		<p>Blinking GREEN and solid BLUE LEDs will switch to a rapidly blinking GREEN LED and then to a solid GREEN LED indicating successful User PIN change</p>

25. Set Read-Only in User Mode



Important: If data has just been copied to the diskAshur DT², make sure to properly disconnect the drive first by clicking 'Safely Remove Hardware/Eject' the diskAshur DT² from the Operating System before reconnecting and setting the diskAshur DT² as 'Read-Only/Write-Protect'.

To set the diskAshur DT² to Read-Only, first enter the "User Mode" as described in section 23. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode, press and hold down "7 + 6" buttons. (7=Read + 6=Only)		Solid GREEN LED will change to blinking GREEN and BLUE LEDs
2. Release 7+6 buttons and press "UNLOCK"		GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read-Only



Note: 1. This setting is activated the next time the drive is unlocked.
 2. If a User set the drive as Read-Only, Admin can override it by setting the drive as Read/Write in Admin mode.
 3. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write

26. Enable Read/Write in User Mode

To set the diskAshur DT² to Read/Write, first enter the "User Mode" as described in section 23. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode, press and hold down "7 + 9" buttons. (7=Read + 9=Write)		Solid GREEN LED will change to blinking GREEN and BLUE LEDs
2. Release 7+9 buttons and press "UNLOCK"		GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read/Write



Note: 1. This setting is activated the next time the drive is unlocked.
 2. If a User set the drive as Read-Only, Admin can override it by setting the drive as Read/Write in Admin mode.
 3. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write

27. Brute Force Protection

If an incorrect PIN is entered 15 (3 x 5 PIN clusters) consecutive times, then all Admin/User PINs, the encryption key and **all data will be deleted** and lost forever. The diskAshur DT² will then need to be formatted and partitioned before it can be reused.

1. If a PIN is entered incorrectly 5 (five) consecutive times, all LEDs - **RED**, **GREEN**, **BLUE** will light up and become solid.
2. Switch the **ON/OFF** power button **OFF** and then back **ON** again to get five more PIN attempts. If PIN is incorrectly entered 5 more times, (10 in total - 5 from step 1 and 5 from step 2) all LEDs - **RED**, **GREEN**, **BLUE** will light up and become solid again.
3. Switch the **ON/OFF** power button **OFF**, then hold down the “**SHIFT**” button while switching the power back **ON** again, all LEDs - **RED**, **GREEN**, **BLUE** will light up and blink together.
4. With all LEDs blinking, enter “**47867243**” and press the “**UNLOCK**” button to get 5 final attempts.



Caution: After 15 consecutive incorrect PIN entries the Brute Force Defence Mechanism activates and deletes all Admin/User PINs, the encryption key and data. A new Admin PIN must be created, refer to Section 19 on page 15 on ‘[How to Create an Admin PIN after a Brute Force attack or Reset](#)’, the diskAshur DT² will also need to be partitioned and formatted before any new data can be added to the drive.

28. How to perform a complete reset

To perform a complete reset, the diskAshur DT² must be in a standby state (solid **RED** LED). Once the drive is reset then all Admin/User PINs, the encryption key and all data will be deleted and lost forever and the drive will need to be formatted and partitioned before it can be reused.

To reset the diskAshur DT² proceed with the following steps.

<p>1. In standby state, press and hold down “0” button until all LEDs blink alternately on and off</p>		<p>Solid RED LED will change to all LEDs, RED, GREEN and BLUE blinking alternately on and off</p>
<p>2. Press and hold down “2 + 7” buttons until all LEDs become solid for a second and then to a solid RED LED</p>		<p>RED, GREEN and BLUE alternating LEDs will change to all solid for a second and then to a solid RED LED indicating the drive has been reset</p>



Important: After a complete reset a new Admin PIN must be created, refer to Section 19 on page 15 on ‘[How to Create an Admin PIN after a Brute Force attack or Reset](#)’, the diskAshur DT² will also need to be partitioned and formatted before any new data can be added to the drive.

29. Initialising and formatting the diskAshur DT²

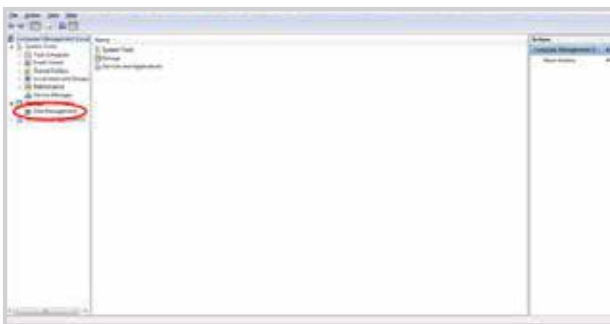
After a 'Brute Force Attack' or a complete reset of the diskAshur DT² will delete all data, encryption key and partition settings. You will need to initialise and format the diskAshur DT² before it can be used.

To initialise your diskAshur DT², do the following:

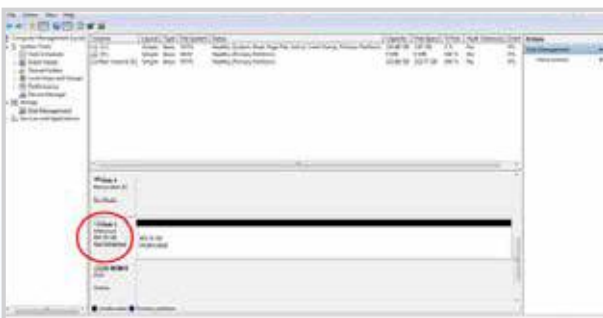
1. Attach the diskAshur DT² to the computer.
2. Create a new Admin PIN - see page 15, section 19, 'How to create an Admin PIN after a Brute Force attack or reset'.
3. With the diskAshur DT² in standby state (RED LED) enter New Admin PIN to unlock (GREEN LED).
4. **Windows 7:** Right click **Computer** and then click **Manage** and then select **Disk Management**
Windows 8: Right-click left corner of desktop and select **Disk Management**
Windows 10: Right click on the start button and select **Disk Management**
5. In the Computer Manage window, click **Disk Management**. In the Disk Management window, the diskAshur DT² is recognised as an unknown device that is uninitialised and unallocated.



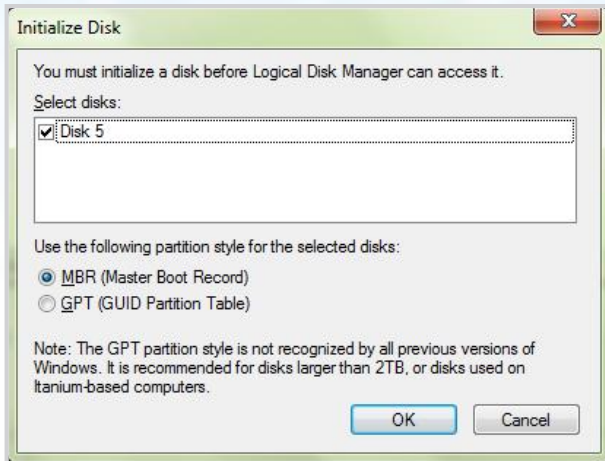
Note: If the Initialise Disk Wizard window opens, click **Cancel**.



6. Right-click Unknown Disk, and then select Initialise Disk.



7. In the Initialise Disk window, click **OK**.



8. Right-click in the blank area under the Unallocated section, and then select New Simple Volume. The Welcome to the New Simple Volume Wizard window opens.



9. Click **Next**.
10. If you need only one partition, accept the default partition size and click **Next**.
11. Assign a drive letter or path and click **Next**.
12. Create a volume label, select Perform a quick format, and then click **Next**.
13. Click **Finish**.
14. Wait until the format process is complete. The diskAshur DT² will be recognised and it is available for use.

30. diskAshur DT² Setup for Mac OS

Your diskAshur DT² is preformatted in NTFS for Windows. To reformat the drive to a Mac compatible format please read below.

Once the drive is unlocked, open Disk Utility from Applications/Utilities/Disk Utilities.

To format the diskAshur DT²:

1. Select diskAshur DT² from the list of drives and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as 'iStorage diskAshur DT² Media' or 232.9 diskAshur DT².



2. Click the 'Erase' button (figure 1).



figure 1

3. Enter a name for the drive (figure 2). The default name is Untitled. The name of the drive will eventually appear on the desktop.

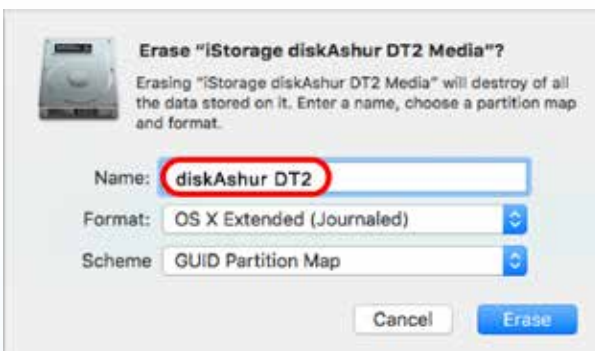


figure 2

4. Select a scheme and volume format to use. The Volume Format dropdown menu (figure 3) lists the available drive formats that the Mac supports. The recommended format type is 'Mac OS Extended (Journaled)'. The scheme format dropdown menu lists the available schemes to use (figure 4). We recommend using 'GUID Partition Map' on drives larger than 2TB.



figure 3

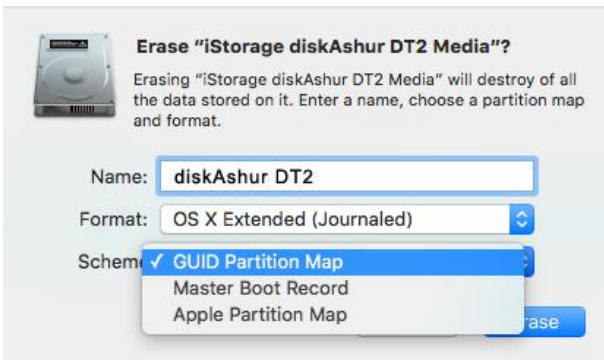


figure 4

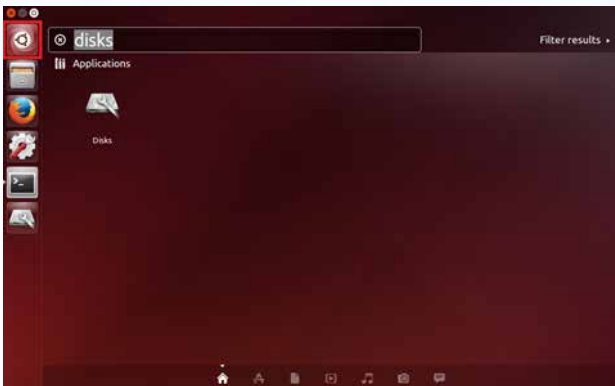
5. Click the 'Erase' button. Disk Utility will unmount the volume from the desktop, erase it, and then remount it on the desktop.

31. diskAshur DT² Setup for Linux (Ubuntu 14.04)

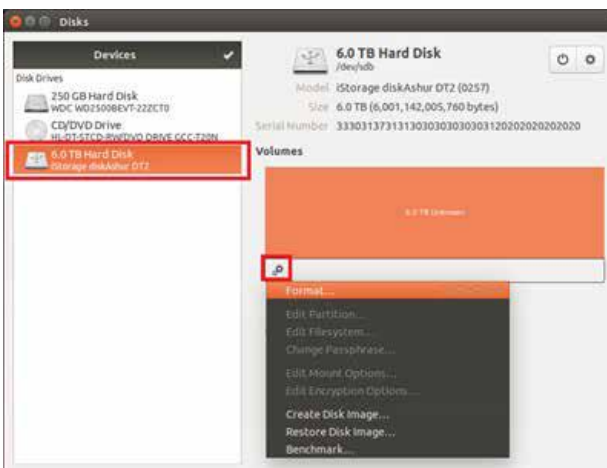
If your diskAshur DT² has been initialised and formatted in NTFS for Windows, you can directly use the drive on Ubuntu. If not, please read below.

To format the diskAshur DT² as FAT filesystem:

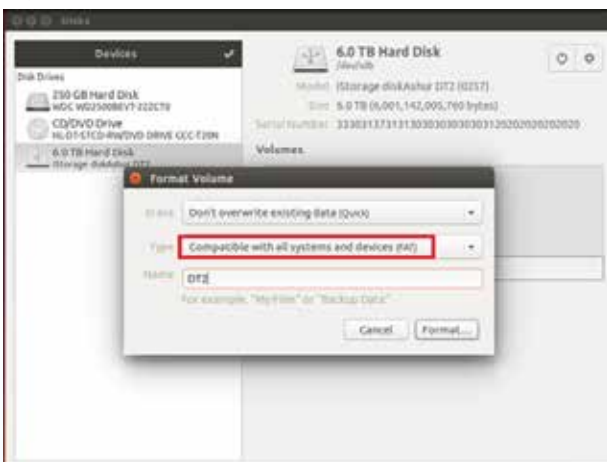
1. Open 'Unity Dash' and type 'Disks' in the search box. Click on the 'Disks' utility when displayed.



2. Click to select the drive (6.0 TB Hard Disk) under 'Devices'. Next click on the gears icon under 'Volumes' and then click on 'Format'.



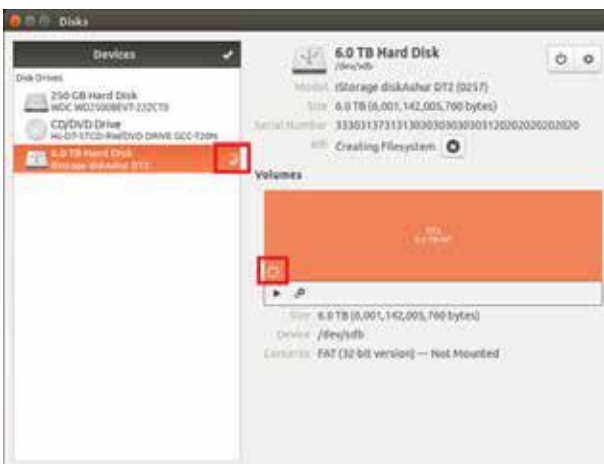
3. Select 'Compatible with all systems and devices (FAT)' for the 'Type' option. And enter a name for the drive, e.g: diskAshur DT². Then, click the 'Format' button.




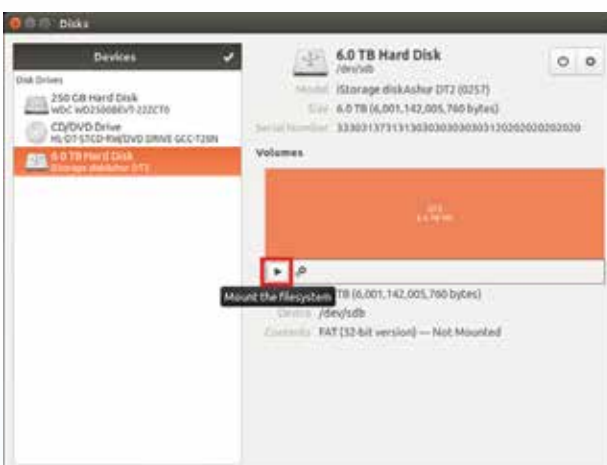
4. Click 'Format' again.



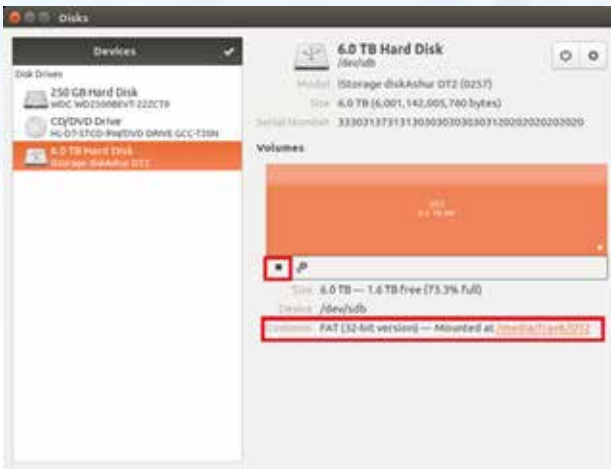
5. The drive will start to be formatted.



6. After the format process is finished, click  to mount the drive to Ubuntu.



7. Now the drive should be mounted to Ubuntu and ready to use.

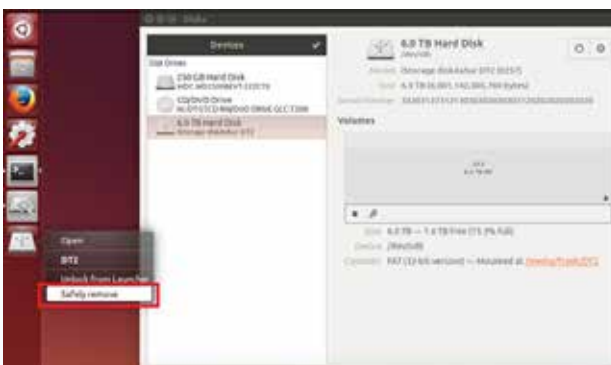


8. A disk icon will be shown as seen in the image below. You can click the disk icon to open your drive.



Lock diskAshur DT² for Linux (Ubuntu 14.04)

It is **strongly recommended** to right click your drive icon and then click **'Safely remove'** in the OS to eject (lock) your diskAshur DT², especially after data has been copied or deleted from the drive.



32. Hibernating, Suspending, or Logging off from the Operating System

Be sure to save and close all the files on your diskAshur DT² before hibernating, suspending, or logging off from the operating system.

It is recommended that you lock the diskAshur DT² manually before hibernating, suspending, or logging off from your system.

To lock, simply press the 'LOCK' button on the diskAshur DT² or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system.



Attention: To ensure your data is secure, be sure to lock your diskAshur DT² if you are away from your computer.

33. How to check Firmware in Admin mode


To check the firmware revision number, first enter the "Admin Mode" as described in section 7. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

<p>1. In Admin mode press and hold down "3 + 8" until GREEN and BLUE LEDs blink together</p>		<p>Solid BLUE LED will change to blinking GREEN and BLUE LEDs</p>
<p>2. Press the "UNLOCK" button and the following happens;</p> <ol style="list-style-type: none"> All LED's (RED, GREEN & BLUE) become solid for 1 second. RED LED blinks indicating the integral part of the firmware revision number. GREEN LED blinks indicating the fractional part. All LED's (RED, GREEN & BLUE) become solid for 1 second. LEDs return to solid BLUE 		

For example, if the firmware revision number is '1.2', the RED LED will blink once (1) and the GREEN LED will blink two (2) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to a solid BLUE LED.

34. How to check Firmware in User Mode

To check the firmware revision number, first enter the “**User Mode**” as described in section 23. Once the drive is in **User Mode** (solid **GREEN** LED) proceed with the following steps.

<p>1. In User mode press and hold down “3 + 8” until GREEN and BLUE LEDs blink together</p>		<p>Solid GREEN LED will change to blinking GREEN and BLUE LEDs</p>
<p>2. Press the “UNLOCK” button and the following happens;</p> <ol style="list-style-type: none"> All LED's (RED, GREEN & BLUE) become solid for 1 second. RED LED blinks indicating the integral part of the firmware revision number. GREEN LED blinks indicating the fractional part. All LED's (RED, GREEN & BLUE) become solid for 1 second. LEDs return to solid GREEN 		

For example, if the firmware revision number is ‘1.2’, the **RED** LED will blink once (1) and the **GREEN** LED will blink two (2) times. Once the sequence has ended the **RED**, **GREEN** & **BLUE** LED's will blink together once and then return to a solid **BLUE** LED.

35. Technical Support

iStorage provides the following helpful resources for you:

iStorage's Website

<https://www.istorage-uk.com>

E-mail correspondence

support@istorage-uk.com

Telephone support with our Technical Support Department on **+44 (0) 20 8991-6260**.

iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m. GMT - Monday through Friday.

36. Warranty and RMA information

Two Year Warranty:

iStorage offers a 2-year warranty on the iStorage diskAshur DT² against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from iStorage or an authorised reseller.

Disclaimer and terms of warranty:

THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.

ISTORAGE WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF ISTORAGE.

THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM ISTORAGE OR AN AUTHORIZED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLIGENCE, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE; 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY ISTORAGE; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN ISTORAGE AND SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.

NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF ISTORAGE OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR. ISTORAGE SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT ISTORAGE WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

Appendix A

iStorage Security Directive #1 – Product Security Features & Secure Handling

This iStorage directive provides product support for use by commercial, public service, and government agencies alike of iStorage secure drive products, and applies the direction of the NCSC CESG document:

CPA Security Characteristic Hardware Media Encryption Version 1.2 Dated April 2012

This iStorage Directive #1 advises the security features supported by iStorage secure drive products, along with best security practices to be employed when using iStorage secure devices to protect sensitive and protectively marked information assets both in on-site accommodation, and when away from the operational premises; or when the iStorage secure drives are in transit.

Together, the secure drive supported features, and best practice advice accommodates robust mitigations against the risk of physical attack, theft, or the opportunity to compromise data assets stored on iStorage secure drives to deny the opportunity of unauthorised access to the protected content.

The Risk: iStorage secure drives are classified as valuable and attractive items, which may contain sensitive business, government related, or personal/protected data assets (GDPR related), and as such they represent a target for both physical and logical attack in the form of theft or compromise if:

- Left unattended
- Visible in public places
- When left in an open state
- When not secured correctly when in transit
- When commensurate controls are not applied to the sensitivity of the stored data asset

Within this iStorage Security Directive #1 we provide best advice, and pragmatic, workable mitigation to reduce the surface of attack.

Mitigations: The device security features and mitigations provided below document the recommended and best security practices which should be applied when handling iStorage secure drives, and are shown in **Table 1** below. This approach has the security objective to preserve the security mantra of **CIA+A** (Confidentiality, Integrity, and Availability + Accountability) and applies relevant security controls as outlined within the ISO/IEC 27001, and the referenced NCSC CESG document:

Table 1 – Mitigations – Product Features - Secure Handling

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
<p>1</p> <p>Integrity Availability Accountability</p>	<p>DEP.M311 DEP.1.M26</p>	<p>In Transit</p>	<p>Never leave a drive insecure in a vehicle, or on display when in transit;</p> <p>If the secure drive must be left unattended, ensure that it is not in view, and that the vehicle is locked between loading and unloading of the media;</p> <p>if an iStorage drive is operational, and contains data assets, always send via a tracked and trusted courier service;</p> <p>iStorage secure drives are issued in a tamper proofed box which is secured by a security seal – if upon receipt the security seal is broken, or showing indications of tampering the drive should be considered compromised. Thus, immediately report this to the iStorage support line on:</p> <p>+44 (0) 20 8991-6260</p> <p>Or send an email to: support@istorage-uk.com</p>

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
<p>2</p> <p>Confidentiality Integrity Availability</p>	<p>DEP.M1 DEP.M701</p>	<p>Unauthorised Access</p>	<p>To mitigate, and minimise the threat of compromise to data assets stored on an iStorage secure drive:</p> <p>Never leave the iStorage secure drive unattended in an authenticated in an open session;</p> <p>To avoid the potential of unauthorised access, put the drive in locked mode when not in operational use;</p> <p>Configure the iStorage Unattended Lock-Clock to secure drive after a prescribed time (Refer to the iStorage User Manual);</p> <p>When the iStorage secure drive is not required, ensure it is removed, and secured under appropriate physical security controls.</p> <p>Always ensure that the stored data assets on the iStorage drive have been backed up, and are available should a loss of the iStorage secure drive occur.</p>
<p>3</p> <p>Confidentiality Accountability</p>	<p>DEP.M703</p>	<p>Loss, Theft, Compromise</p>	<p>Ensure that a process <i>exists</i> to support notification to management of theft, loss, or compromise of the iStorage secure drive;</p> <p>Where Protectively Marked or Government data assets are stored on the iStorage drive, seek advice from the appropriate agency or authority;</p> <p>Confirm that data was encrypted at time of theft or loss (drive was not in an authenticated open session) - clarifying it will not compromise sensitive data assets, or other forms of related information.</p>
<p>4</p> <p>Integrity</p>	<p>DEP.1.M26</p>	<p>Tamper Proofing</p>	<p>The iStorage drives are protected by tamper proofing.</p> <p>Conduct regular checks of the iStorage secure drive outer casing for indications of tampering or direct physical attack.</p> <p>Note 1: If there are actual or suspected indications of tampering, report this as a security incident.</p>
<p>5</p> <p>Confidentiality Integrity</p>	<p>DEP.2.M12 DEP.2.M283 DEP.2.M285 DEP.2.M617</p>	<p>Robust Password Management</p>	<p>The Password is never displayed whilst being entered.</p> <p>Always set a complex password for both Admin, and User accounts on the iStorage secure drive to mitigate the potential of ease of logical attack, and/or compromise;</p> <p>Although the device accepts passwords of minimum 7 characters in length, we strongly recommend the user to set up a password with higher complexity, e.g. no less than 8 characters and using SHIFT key with digits;</p> <p>Choose a password construction which cannot be easily guessed;</p>

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
			<p>Choose a password construction which cannot be easily guessed;</p> <p>Avoid multiple use of password on multiple systems of differing security sensitivities;</p> <p>Never write down a password on paper;</p> <p>Never share a password;</p> <p>Be aware of overlooking when entering a password into the iStorage device in public places;</p> <p>If it is suspected that the password has been subject to compromise, it must be subject to change at the earliest opportunity;</p> <p>Where there is an operational reason to document a password in hard-copy, this must be done by secure means, or via the company Exception Process.</p> <p>Note 2: Secure storage of a password may be facilitated by a secure password locker application, or by use of a sealed envelope which is subject to robust physical access control, and secured within a high-grade combination lock safe.</p>
<p>6</p> <p>Confidentiality Integrity</p>	<p>DEP.2.M281</p>	<p>Administrator Password Management</p>	<p>The iStorage secure drive supports the functionality for an Administrator to be provisioned with a level of privileged access to manage the device.</p> <p>Only authorised and authenticated Administrators can add, or revoke any assigned accounts.</p>
<p>7</p> <p>Confidentiality</p>	<p>DEP.2.M277</p>	<p>Social Engineering</p>	<p>Be aware of the potential of indirect threat of Social Engineering attacks which may attempt to discover your password, and other business related, or personal credentials by means of social engineering techniques.</p>
<p>8</p> <p>Confidentiality Integrity</p>	<p>DEP.2.M280</p>	<p>Credential Distribution</p>	<p>Never communicate or issue any form of security credentials via the same channel, or which are packaged with an iStorage secure drive.</p> <p>Note 3: Where operational necessity dictates the requirement for distributing credentials, this should be achieved out-of-band (e.g by voice, text, secured email).</p>
<p>9</p> <p>Integrity</p>	<p>DEP.4.M348 DEP.1.M348</p>	<p>Authorised Updates</p>	<p>No automated process exists. Only approved updates which applicable to the iStorage products will be distributed as part of an upgrade or replacement process under the internal iStorage SDLC (Security Development Lifecycle) and their Vulnerability Management Policy/Process.</p>

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
<p>10</p> <p>Confidentiality Accountability</p>		<p>Data Classification</p>	<p>Ensure that the value of data assets stored on the iStorage secure drive are classified, or protectively marked as is appropriate their use, and/or custodianship.</p>
<p>11</p> <p>Confidentiality</p>		<p>Cleared Staff/Access</p>	<p>Ensure that those who are provisioned access to the data assets stored on an iStorage secure drive possess a clear need-to-know, and are suitably cleared as appropriate to the level of data asset, or protectively marked materials stored thereon.</p>

Appendix B

iStorage Security Directive #2 – Sanitisation and Secure Disposal

This iStorage directive provides product support for use by commercial, public service, and government agencies alike of iStorage products. This iStorage Directive #2 advises the best security practices to be employed for sanitisation and secure disposal of iStorage secure drives.

This directive also advises on the reissue of secure drives to mitigate the risk of object reuse, or compromise of data assets stored on such iStorage secure drives.

The Risk: If any data assets stored on an iStorage secure drive are not subject to security controls when the drives are reissued, or disposed of at operational end-of-life, they could be subject to compromise implicating organisational security, and data protection mandated controls such as GDPR. For example:

- Exfiltration and circulation of sensitive data to unauthorised external actors
- Accidental disclosure
- Disclosure of Protectively Marked or Government Classified data assets

Objective: Whilst iStorage secure drives enforce protection over their stored data assets by means of robust encryption, it is nevertheless best security practice to ensure that on occasions when iStorage secure drives are reissued to other parties, custodians, department, or when they reach their operational end-of-life, the drives are subject to robust processes to ensure that any remanence of previously stored data assets are securely deleted and purged from that drive to mitigate the likelihood of compromise of such data assets.

Within this iStorage Security Directive #2 we provide best advice, and pragmatic, workable mitigations to counter this threat.

Mitigations: The mitigations provided below are the recommended and best security practices which should be applied when handling iStorage secure drives, and are shown in **Table 1** below. This approach has the objective to preserve the security mantra of **CIA+A** (Confidentiality, Integrity, and Availability + Accountability) and applies relevant security controls as outlined within the ISO/IEC 27001 and applies the direction of the NCSC (CESG) document.

CPA Security Characteristic Hardware Media Encryption Version 1.2 Dated April 2012

Process: At **Fig 1** below is a representation of the high-level data flow which relates to:

- Secure disposal
- Sanitization
- Protectively Marked and Government Security Classified data assets
- Reissue of iStorage secure drives

Fig 1 – Sanitisation/Disposal Process

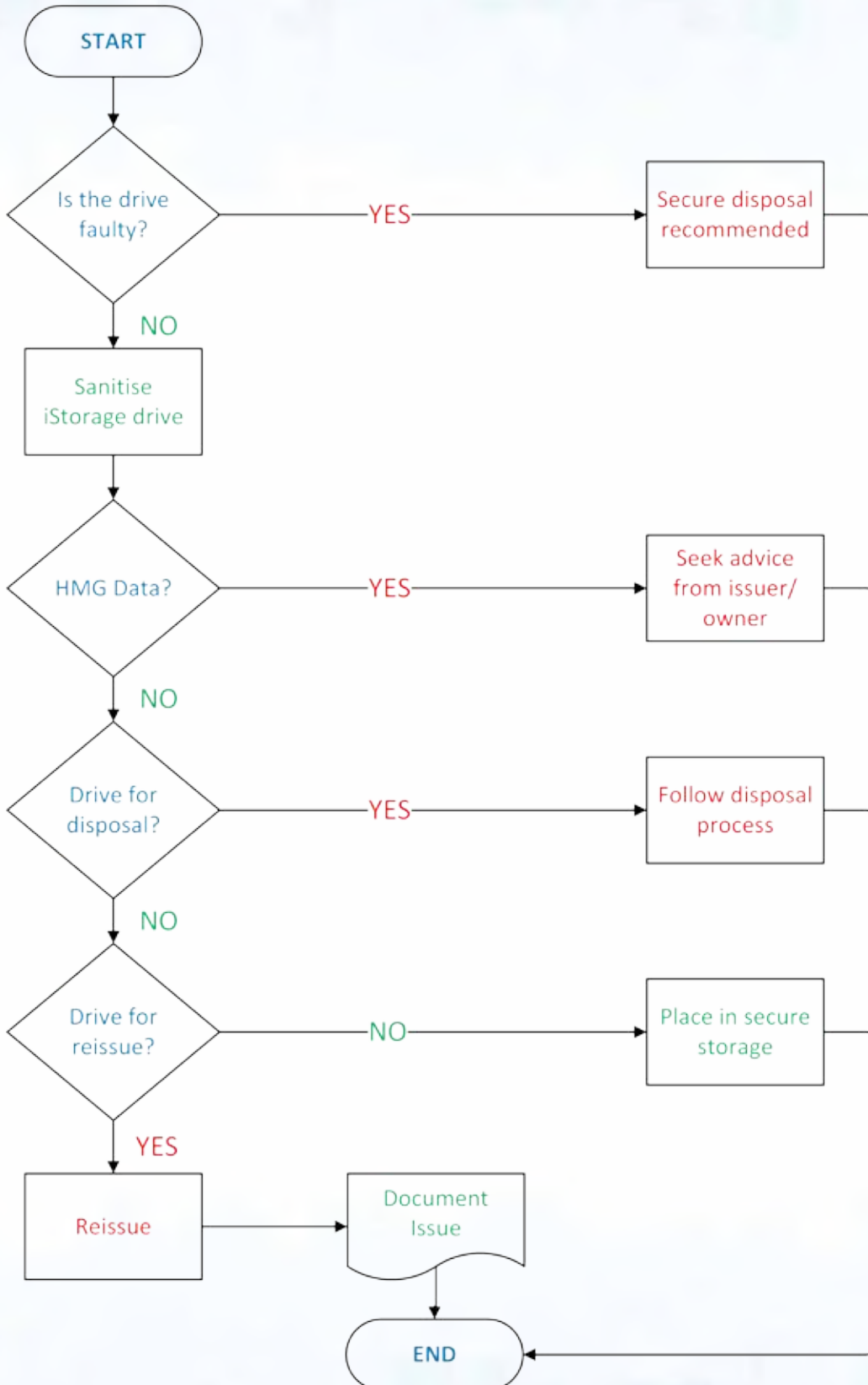


Table 1 - Mitigations - Sanitisation and Secure Disposal

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
<p>1</p> <p>Confidentiality Accountability</p>	<p>DEP.M1</p>	<p>Storage</p>	<p>Ensure that all iStorage secure drives awaiting sanitisation, or secure disposal are fully documented and accounted for;</p> <p>That they are stored in a secure facility provisioned with robust physical, and access control security mechanisms and procedures.</p> <p>Note 1: Dependent on the amount awaiting processing, this could be a locked room, or a security cabinet.</p>
<p>2</p> <p>Confidentiality Accountability</p>	<p>DEP.M311</p>	<p>In Transit</p>	<p>When in transit to secure a disposal facility, never leave a drive insecure in a vehicle, or on display when in transit;</p> <p>If the drives must be left unattended, ensure the iStorage secure drives are not in view, and that the vehicle is locked between loading and unloading of the media;</p> <p>All iStorage secure drives destined for processing by a secure destruction facility should be tracked, and handled only by a trusted vendor, or courier service;</p> <p>Where iStorage secure drives have stored Protectively Marked and Government Classified information assets, advice should be sought from the relevant department, or agency to confirm if a requirement exists to apply additional controls (e.g. in transit communications, contact with the emergency services, or a stand-by vehicle)</p>
<p>3</p> <p>Confidentiality Accountability</p>		<p>Protective Marking</p>	<p>Where iStorage secure drives have stored Protectively Marked, Government Classified data assets, guidance should be sought from the owner department or agency as to the requirements for recording and secure disposal of secure drives</p>
<p>4</p> <p>Confidentiality Accountability</p>		<p>Accountability</p>	<p>All iStorage secure drives awaiting sanitisation, or secure disposal should be fully accounted for in a register, recording:</p> <ul style="list-style-type: none"> • Serial number • Owner/department • Date received • Data asset classification, or protective marking • Any special handling caveats • Dispatch date for processing <p>Note 2: In circumstances where the iStorage drive has been sanitised for reissue, it should be then documented in a separate register awaiting distribution to a new owner/custodian/department.</p>

Mitigation	NCSC (CESG) CPA	Risk	Best Practice
5 Availability		Business Continuity	Prior to any iStorage secure drive being subject to sanitisation, or secure disposal, confirmation should be sought to assure that any data assets held thereon are accounted for, and backed up as required to avoid unintentional disposal of the stored operational data assets.
6 Confidentiality Accountability	DEP.M137	Sanitisation Methods	<p>The sanitisation methods which are employed to process any iStorage secure drive should be supported by documented sanitisation procedures and Security Operating Procedures (SyOps);</p> <p>Such procedures should follow appropriate processes relevant to the media type and any Protective Marking, or other Government Classification of the data asset being sanitised to meet as a minimum HMG Standards.</p> <p>The selected Service Provider must demonstrate that these procedures are followed in practice.</p> <p>NCSC (part of GCHQ) advice available at the following URL: https://www.ncsc.gov.uk/index/topic/164</p>
7 Integrity	DEP.M137	Sanitisation and Disposal	<p>All Sanitisation/Destruction iStorage secure drives products should be conducted in line with Manufacturer's documented operating procedures, user guides and any published Security Procedures;</p> <p>The personnel or teams who are conducting the sanitisation, or secure disposal process should be trained in the correct usage of such equipment;</p> <p>Processes must be in place to verify that equipment is being used correctly and in accordance with the manufacturers recommendations.</p>
8 Confidentiality Accountability		Reissue of Media	<p>On occasions where the iStorage secure drive has been subjected to sanitisation, and is required for reissue to a new user, custodian, or department, checks should be conducted prior to issue to assure that the media is fully blank;</p> <p>An iStorage secure drive user manual should be issued to the recipient user, with clear instructions of secure operational use;</p> <p>The issue of the iStorage secure drive should be fully accounted for, and entered in an asset register.</p>

Mitigation	NCSC (CESG) IAS5	Risk	Best Practice
<p>9</p> <p>Confidentiality Accountability</p>	<p>DEP.M703</p>	<p>Loss, Theft, Compromise</p>	<p>Ensure that a process exists to support notification to management of theft, loss, or compromise of the iStorage secure drive awaiting processing;</p> <p>Where Protectively Marked or Government data assets are stored on the iStorage drive, seek advice from the appropriate authority or agency;</p> <p>Confirm that data was encrypted at time of theft or loss - clarifying it will not compromise sensitive data assets, or other forms of related information.</p>
<p>10</p> <p>Confidentiality</p>	<p>MIT003</p>	<p>Cleared Staff/ Access</p>	<p>Ensure that those who are provisioned access to the data assets stored on an iStorage secure drive possess a clear need-to-know, and are suitably cleared as appropriate to the level of data asset, or Protectively Marked, Government Classified data assets and materials stored thereon.</p>

iStorage®

© iStorage, 2017. All rights reserved.
iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com