Security Procedures

iStorage diskAshur PRO² and diskAshur DT²

Issue No: 1.0
April 2018

The copyright of this document is reserved and vested in the Crown.

Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>April 2018</td>
<td>First Public Release</td>
</tr>
</tbody>
</table>
About this document
These Security Procedures provide guidance in the secure operation of iStorage diskAshur PRO² and diskAshur DT².

This document is intended for System Designers, Risk Managers and Accreditors. NCSC recommend you establish whether any departmental or local standards, which may be more rigorous than national policy, should be followed in preference to those given in these Security Procedures.

The Security Procedures come from detailed technical assessment carried out by NCSC. They do not replace tailored technical or legal advice on specific systems or issues. NCSC and its advisors accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed on this guidance.

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

Related documents
The documents listed in the References section are also relevant to the secure deployment of this product. For detailed information about device operation, refer to the product documentation for iStorage diskAshur PRO² [g] and diskAshur DT² [h].

Points of contact
For additional hard copies of this document and general queries, please contact:

NCSC Enquiries
Hubble Road
Cheltenham
GL51 0EX
United Kingdom
enquiries@ncsc.gov.uk
Tel: 0300 020 0964

NCSC welcomes feedback and encourages readers to inform NCSC of their experience, good or bad in this document. Please email: enquiries@ncsc.gov.uk
Contents

Chapter 1 - Outline Description ................................................................. 7
  Certification .......................................................................................... 8
  Components ......................................................................................... 9

Chapter 2 - Security Functionality ......................................................... 10

Chapter 3 - Secure Operation ................................................................. 11
  Pre-installation ...................................................................................... 11
  Installation ........................................................................................... 11
  Configuration ....................................................................................... 13
  Operation ............................................................................................... 16
  Maintenance and updates ................................................................. 17
  System logs ......................................................................................... 17
  User education ................................................................................... 17
  Disposal and destruction ................................................................. 17

Chapter 4 - Security Incidents ................................................................. 18
  Tampering and other compromises ................................................... 19
  Incident management ......................................................................... 19

Chapter 5 - Disposal and Destruction ................................................... 20

Chapter 6 - Password Policy ................................................................. 21

References .............................................................................................. 22

Glossary ................................................................................................. 23
iStorage diskAshur PRO² and diskAshur DT²

Chapter 1 - Outline Description

1. iStorage diskAshur PRO² and diskAshur DT² (in this document referred to collectively as ‘the Products’ or individually as ‘the Product’) have been certified as satisfying the requirements of NCSC’s Commercial Product Assurance (CPA) Scheme at Foundation Grade. The diskAshur PRO² is a portable hardware encrypted data storage product and the diskAshur DT² is a desktop version.

2. The major features and functionality provided by the iStorage diskAshur PRO² range are as follows:
   - USB 3.1 Encrypted Portable Hard Disk Drive (HDD) or Solid-State Drive (SSD):
     - https://istorage-uk.com/product/diskashur-pro2/
     - https://istorage-uk.com/product/diskashur-pro2-ssd/
   - Including the following product capacities for HDD:
     - 500GB, 1TB, 2TB (thin enclosure)
     - 3TB, 4TB, 5TB (thick-15mm enclosure)
   - Including the following product capacities for SSD:
     - 128GB, 256GB, 512GB, 1TB, 2TB, 4TB
   - AES-XTS 256-bit hardware encryption:
     - No external software or client software is required
   - OS & Platform independent;
   - Employs Enhanced Dual Generating Encryption (EDGE) Technology.

3. The major features and functionality provided by iStorage diskAshur DT² are:
   - USB 3.1 Encrypted Desktop HDD:
   - Including the following product capacities for HDD:
     - 1TB, 2TB, 3TB, 4TB, 6TB, 8TB, 10TB
   - AES-XTS 256-bit hardware encryption:
     - No external software or client software is required
   - OS & Platform independent;
   - Employs EDGE Technology.

4. The Product permits one User and one Administrator to be defined; both are referred to as “users” if no distinction is required. The user interfaces on the Product are:
   - The keypad for user input;
   - The LEDs for status output.
5. Once a User or Administrator has been authenticated, the Product can be used as a normal unencrypted drive from the host computer. If the Product is unauthenticated, the contents are not available in plaintext and will remain securely encrypted without further action required by a user. The same applies if the Product is de-authenticated by any one of the following actions or events:

- automatic timeout;
- pressing the ‘Lock’ button;
- pulling out the USB cable for the diskAshur PRO\textsuperscript{2};
- switching off or pulling out the power cable for the diskAshur DT\textsuperscript{2};
- clicking “Safely Remove Hardware” (or equivalent) in the operating system.

6. Although the Products have different enclosures, they share identical security components, firmware, and cryptographic algorithm design. Data from the host computer is encrypted and decrypted on the fly by the AES-XTS 256-bit hardware encryption module of the encryption controller.

7. The Products do not use or require any client software on the host computer because all the features and functionality are fully contained within the physical enclosure surrounding the product.

8. These Security Procedures cover the features and functionality of the Products. The host computer is not covered here, as it is outside the scope of the CPA certification.

Certification

9. iStorage diskAshur PRO\textsuperscript{2} version 1.6 and diskAshur DT\textsuperscript{2} version 1.6 have undergone CPA assessment and have been certified as meeting the Augmented Grade requirements as described in the CPA Security Characteristic (SC) for Hardware Media Encryption, Version 1.2, April 2012 [a].

10. Later versions of the Products are automatically covered by this certification until the certificate expires or is revoked, as stated on the CPA website.

Components

12. Each Product has the following major components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Protective Marking</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Controller</td>
<td>None initially, but during use it will be the maximum classification of the data stored on the Product</td>
<td>Data may be stored or accessible</td>
</tr>
<tr>
<td>Security Controller</td>
<td>None initially, but during use it will be the maximum classification of the data stored on the Product</td>
<td>Data may be stored or accessible</td>
</tr>
<tr>
<td>HDD or SSD</td>
<td>None initially, but during use it will be the maximum classification of the data stored on the Product</td>
<td>Data may be stored or accessible, but it will be encrypted</td>
</tr>
<tr>
<td>Keypad</td>
<td>(None)</td>
<td>No data is stored</td>
</tr>
<tr>
<td>LEDs</td>
<td>(None)</td>
<td>No data is stored</td>
</tr>
<tr>
<td>Enclosure</td>
<td>(None)</td>
<td>No data is stored</td>
</tr>
</tbody>
</table>

Table 1 – Components of the Products
Chapter 2 - Security Functionality

13. The security features and functionality provided by diskAshur PRO² and diskAshur DT² are as follows:

- independent of the host computer, operating system, and platform;
- does not require any external software or host computer client software;
- does not require any administrator rights on the host computer;
- has a microprocessor with memory scrambler;
- uses AES-XTS 256-bit hardware encryption;
- provides Read-Only and Read-Write modes;
- provides 7 to 15 digits configurable PIN authentication;
- provides a countermeasure to a brute force attack which leads to a deadlock frozen state;
- provides a Drive Reset function which clears PINs and data, and creates a new encryption key;
- provides an Auto Lock function which automatically locks the drive after a defined, configurable, time period;
- provides a Self-Destruct PIN which leads to a deadlock frozen state;
- is designed to be immune to the BadUSB attack;
- employs Enhanced Dual Generating Encryption (EDGE) Technology;
- has tamper evident top and bottom covers and internal frangible clips;
- provides tamper resistance via the epoxy resin coating of the chips;
- has a wear resistant epoxy coated keypad which hides key usage, to avoid indication of commonly used keys and hence provides PIN security;
- has a desk lock slot, for use in conjunction with a Kensington-type lock, for physical security;
- diskAshur PRO² is Ingress Protection IP56 certified, providing resistance to water and dust, and diskAshur DT² has air vents;
- has an integrated cable which uses Super Speed USB 3.1.

14. The security functionality of the Product is consistent with the requirements stated by the Mitigations in the CPA SC for Hardware Media Encryption [a].
Chapter 3 - Secure Operation

15. The configuration outlined below is in line with that recommended in the CPA SC for Hardware Media Encryption [a]. These recommendations should be followed unless there is a strong business requirement not to, which has been discussed with your Accradiator.

16. This chapter summarises the security aspects of the Products. Full information about the Products, for the User and Administrator, is provided by:

- Quick Start Guide [e] and [f];
- User Manual [g] and [h].

Pre-installation

17. Before installing the Products, NCSC recommends that you perform the following actions:

- Ensure that there is a secure physical environment for the Product:
  - It is recommended that customers and end users store and use the Product in a secure physical environment to reduce the potential for the device to be physically compromised.
- Perform a physical inspection of the Product’s enclosure:
  - The Product has a tamper-evident top and bottom cover on the enclosure. On receipt of the Product, and regularly thereafter, the covers should be inspected for any signs of physical interference or damage. If there is evidence of tampering, this should be reported as soon as possible (see Chapter 4 Security Incidents) and the product must be removed from use immediately. Any product that shows evidence of tampering must not be returned to service.
- Verify the version of the Product:
  - The version of the Product can be verified by following the “How to Check Firmware” procedure in the User Manual [g] and [h]. This is also briefly described in the Configuration subsection below.

Installation

18. Instructions to setup and install the Products are provided in the Quick Start Guide [e] and [f], and in the User Manual [g] and [h] which is pre-installed on the Products.

19. As explained in the Quick Start Guide [e] and [f]:

- The Products are preformatted with NTFS;
- The Products are shipped with the iStorage default Administrator PIN;
- A new Administrator PIN must be created immediately:
  - PIN length must be a minimum of 8 and a maximum of 15 digits. This can be configured, see the Configuration section below.
Cannot contain all sequential numbers (e.g. 2345678 or 9876543).
Cannot contain all repeating numbers (e.g. 1111111 or 88888888).
The SHIFT key can be used for additional characters (e.g. SHIFT+1 is a separate value to just 1), so there are 20 characters in total.
The blue letters on the Keypad can be used to create a memorable mnemonic password (with the above constraints).

In addition to the Quick Start Guide information provided above, the Administrator and the User must follow the Password Policy which is provided in Chapter 6.

20. The LED lights on the Product indicate whether a PIN has been entered correctly or not. The relevant light patterns are described in the User Manual [g] and [h], and are included in the Configuration section below.

21. To unlock the Product for the first time:
   - Insert the integrated USB 3.1 cable to a powered USB port.
   - Wait for the self-check to finish and display the RED LED.
   - Enter the default Administrator PIN.
   - Press the UNLOCK button.

22. As explained in the Quick Start Guide [e] and [f], before allowing the User to use the Product, change the Administrator PIN to a new secure Administrator password\(^1\) as follows:
   - In the Standby mode, simultaneously press UNLOCK and 1.
   - Enter the default Administrator PIN 11223344 and then press UNLOCK.
   - In the Administrator mode, simultaneously press UNLOCK and 2.
   - Enter the new secure Administrator PIN and then press UNLOCK.
   - Re-enter the new secure Administrator PIN and then press UNLOCK.
   - Press LOCK to exit the Administrator mode.

23. A new secure User password can be created by using a similar procedure to the one above but replacing “2” with “3”. The new secure Administrator and User passwords should conform to Chapter 6 Password Policy.

24. Locking the Product is via any of the de-authentication events described in Chapter 1. Unlocking the Product is as follows:
   - Administrator: Enter PIN and Press UNLOCK
   - User: Press UNLOCK, Enter PIN, and Press UNLOCK

\(^1\) In this document, for the purposes of the Products, the terms “PIN”, “password”, and “passphrase” are equivalent.
25. In the Standby state, in which the Product has not yet been authenticated, the Product will not be recognised by the host operating system. Therefore, without the User or Administrator PIN, there is no way to access data on the drive.

Configuration

26. The User Manual [g] (and the User Manual [h] allowing for minor changes in section numbering and heading description text, which don’t affect security aspects) offers the following secure functionality, from which guidance on the secure configuration options are provided in sub-bullet points in *blue italic text* (where relevant):

- **diskAshur PRO² LED States**
- **How to use the diskAshur PRO² for the first time**
- **Unlocking the diskAshur PRO²**
- **Locking the diskAshur PRO²**
- **Entering Administrator Mode**
- **Changing the Administrator PIN**
  - *Follow the Password Policy in Chapter 6.*
- **Setting a User PIN Policy**
  - *Follow the Password Policy in Chapter 6.*
  - In Standby, press **UNLOCK** and 1, then enter the Administrator PIN and press **UNLOCK**. In Administrator mode, press **UNLOCK** and 7, then type three digits, where the first two are the minimum PIN length and the last is 0 for no special characters or 1 for special characters (e.g. default policy is **070** but CPA requires at least **081**). Press **SHIFT** button to finish.
  - Setting a new User PIN Policy will automatically delete the User PIN
  - The complexity setting for the Self-Destruct PIN and Administrator PIN is always 7-15 digits, with no special character required
- **How to check the User PIN Policy**
- **Adding a new User PIN in Administrator Mode**
  - *Follow the Password Policy in Chapter 6.*
- **Changing the User PIN in Administrator Mode**
  - *Follow the Password Policy in Chapter 6.*
- **Deleting the User PIN in Administrator Mode**
  - In Administrator mode, press **SHIFT** and 3, then press **SHIFT** and 3.
- **Set Read-Only in Administrator Mode**
  - *Depending on the associated environmental risks, this feature of the Product, which is operating system independent, can be used to ensure the enduring integrity of the data on the Product.*
  - In Administrator mode, press 7 and 6 (for the mnemonic “RO” for Read-Only), and then press **UNLOCK**.
  - This should be the first action after a successful authentication. It cannot be changed by the User.
- **Enable Read/Write in Administrator Mode**
- **This is the default or normal mode.**
  - In Administrator mode, press 7 and 9 (for the mnemonic “RW” for Read-Write), and then press UNLOCK.

- **How to create a Self-Destruct PIN**
  - **This is optional.**
  - In Administrator mode, press UNLOCK and 6, type the Self-Destruct PIN and then press UNLOCK.

- **How to delete the Self-Destruct PIN**
  - In Administrator mode, press SHIFT and 6, and then press SHIFT and 6.

- **How to Unlock with the Self-Destruct PIN**
  - In Standby mode, press UNLOCK, enter SD PIN, and press UNLOCK.
  - The SD PIN will become the new User PIN and the Product will need to be partitioned and formatted before it can be used.

- **How to Create an Administrator PIN after a Brute Force attack or Reset**
  - In Standby mode, press SHIFT and 1, enter new secure Administrator PIN, and press UNLOCK.; re-enter Administrator PIN and press UNLOCK.

- **Setting the Unattended Auto-Lock Clock**
  - Set this in accordance with the Organisational Security Policy.
  - In Administrator mode, press UNLOCK and 5, then enter two digits representing a time between 05 and 99 minutes, and press SHIFT.

- **Turn off the Unattended Auto-Lock Clock**
  - **This is not recommended.**
  - In Administrator mode, press UNLOCK and 5, then enter 00, and press SHIFT.

- **How to check the Unattended Auto-Lock Clock**
  - In Administrator mode, press SHIFT and 5, and press UNLOCK.

- **How to Unlock diskAshur PRO² with User PIN**
  - In Standby mode, press UNLOCK, enter User PIN, and press UNLOCK.

- **Changing the User PIN in User Mode**
  - In User mode, press UNLOCK and 4, enter new User PIN, press UNLOCK, re-enter new User PIN, press UNLOCK.

- **Set Read-Only in User Mode**
  - Depending on the associated environmental risks, this feature of the Product, which is operating system independent, can be used to ensure the enduring integrity of the data on the Product.
  - In User mode, press 7 and 6 (for the mnemonic “RO” for Read-Only), and press UNLOCK.
  - This should be the first action after a successful authentication. It can be changed by the Administrator.

- **Enable Read/Write in User Mode**
  - **This is the default or normal mode.**
In User mode, press 7 and 9 (for the mnemonic “RW” for Read-Write), and press UNLOCK.

- Brute Force Protection
  - If a PIN is entered incorrectly 5 consecutive times, the Product must be unplugged and re-plugged into the host computer.
  - If a PIN is entered incorrectly 5 more consecutive times (i.e. 10 in total), the Product must be unplugged and re-plugged into the host computer while holding the SHIFT button, enter 47867243 and press UNLOCK.
  - If a PIN is entered incorrectly 5 more consecutive times (i.e. 15 in total), the Product’s brute force defence mechanism will be activated, which deletes all encryption keys, User and Administrator PINs, and user data.

- How to perform a complete reset
  - This is for emergency erasure or for re-purposing the Product.
  - In Standby mode, press and hold 0 until all LEDs blink, press and hold 2 and 7 until all LEDs are solid, and then solid RED.
  - A new Administrator PIN will need to be created and the Product will need to be partitioned and formatted.

- Initialising and formatting the diskAshur PRO
  - For security, it is recommended that there is only one partition on the Product and the formatting is performed.
  - This is performed by using the Administrator account on the host computer, once the product has been unlocked, using the functionality provided by Disk Management in Windows (7, 8, or 10).

- diskAshur PRO Setup for Mac OS
- diskAshur PRO Setup for Linux (Ubuntu 14.04)
- Hibernating, Suspending or Logging off from the Operating System
  - Lock the Product before hibernating, suspending, or logging off, by either clicking the ‘Safely Remove Hardware/Eject’ icon in the host operating system, or by pressing LOCK.

- How to check Firmware in Administrator Mode
  - In Administrator mode, press 3 and 8, and then press UNLOCK.
  - Red LED blinks indicate the integer part of the firmware revision number and Green LED blinks indicate the fractional part.

- How to check Firmware in User Mode
  - In User, press 3 and 8, and then press UNLOCK.

- Technical Support
  - The iStorage Website is at https://www.istorage-uk.com
  - E-mail correspondence at support@istorage-uk.com

- Warranty and RMA information
  - iStorage offers a 2-year warranty for HDD products and a 3-year warranty for SSD products.

2 The PIN “47867243” spells “istorage” with respect to the blue letters on the digit keys of the keypad. It is hard coded and hence it is not configurable by the Administrator.
Operation

27. The User Manual [g] and [h] offers the following guidance for secure use:
   - Protect the Product at all times.
   - Ensure that there are adequate backups.
   - Protect the User or Administrator PIN at all times.
   - Ensure that password changes are performed securely.
   - If a User PIN is lost or forgotten, the Administrator user can reset it.
   - Be aware of Social Engineering attacks in relation to the Product.
   - Check the Product regularly for any evidence of malicious tampering.
   - Follow the security incident procedure in Chapter 4 when it is required.
   - It is important to change PIN regularly, to avoid indication of wear and tear usage on the keypad, although this is reduced due to the resin coating.

28. The Product is primarily for the security of Data At Rest. Therefore, once a User or Administrator has been successfully authenticated on the Product, responsibility for the secure use and protection of the data on the Product passes to that User or Administrator.

29. The User or Administrator must ensure that:
   - USB interception of data, via the host Operating System or the Internet, is adequately protected against in accordance with the Organisation’s Security Policy.
   - There is physical protection and possession of the Product at all times.
   - A secure backup of the data is available, in case of physical loss or malicious reset of the Product.

30. The Product does not provide an audit log, but if an audit log is required, it can be arranged on the host operating system(s). However, bear in mind that the Product is operating system independent and hence the Product could potentially be used on multiple host operating systems.

31. A design feature of the Product is that it does not permit any software or firmware updates. Any exploitable vulnerability will be addressed by a Recall and Replacement process. The warranty period is 2 years for HDD products and 3 years for SSD products. However, all users must be aware of the potential risk of receiving a tampered or fake Product from malicious third parties, and the appropriate countermeasures that are necessary.

32. The User and the Administrator should be aware that, in common with all electro-magnetic devices, there is an ongoing risk of degaussing for HDD products, but not for SSD products.
33. The administrator can delete or change the user’s PIN. Wrapped keys will be sanitised when the administrator deletes or changes that PIN, but the Data Encryption Key for user data encryption and decryption will not be changed.

**Maintenance and updates**

34. The Products should be entered in an Asset Register and fully accounted for during their usage lifecycle, up to either re-use or destruction.

35. The iStorage drives are protected by tamper evident components. Schedule regular inspections of the drive’s outer casing for indications of tampering or direct physical attack. No other maintenance activities are required.

36. The Products are designed such that updates are not required, and not provided, either online or on CD/DVD or other media. However, in the event of the discovery of an exploitable vulnerability, a Recall and Replacement (also called Re-Issue) service will be provided by iStorage; as described in Appendix A of the User Manual [g] and [h], and summarised as follows:

- Two working days in advance of the dispatch of the new replacement product, TOE customers will receive an email including the product serial number, which can be verified on receipt.

- TOE customers should be aware of the potential risk of receiving a tampered or fake iStorage product from third parties, by ensuring that appropriate Security Education and Awareness Training is provided to users regarding such risks.

- TOE customers can report any actual or suspected indications of product tampering or falsification to iStorage Support on: +44 (0) 20 8991 6260 or send an email to: support@istorage-uk.com

**System logs**

37. There are no system event or audit logs.

**User education**

38. Follow the NCSC Password Guidance [c].

39. Read Appendix A and Appendix B of the User Manual [g] and [h].

40. Deliver appropriate Security Education and Awareness Training to users.

41. Ensure that all users of the Product have a clear Need-To-Know and are suitably cleared as appropriate to the classification level of the stored data.

**Disposal and destruction**

42. Follow the process described in Chapter 5 Disposal and Destruction.
Chapter 4 - Security Incidents

43. It is assumed that a generic management and handling procedure for security incidents already exists in the end user’s environment in accordance with their Organisational Security Policy. It is assumed that the end user’s organisation will have the following:

- IT Security Manager
- Incident Response Team
- Security Review Committee (e.g. the Board of Directors)

44. It is assumed that the end user’s organisation will utilise formally documented Incident Response procedures covering Policy, Plan, Procedures, Work Instructions, Guidelines and Forms & Records. Therefore, in that context, the details provided below are specifically related to the Product.

45. The primary focus of the security aspects of the Incident Response procedure is based on the following stages:

- **Detection**: A security incident may be reported by any internal or external user (or even a third party) by phone, email or directly in person. Evidence may be gathered from error messages, log files, configuration settings, etc.
- **Analysis**: A technical employee will examine the reported security incident, confirm that it is valid and pass it on to the next stage of the procedure. (The procedure will be halted there if the report does not indicate a valid security incident; for example, due to an obvious misunderstanding or some confusion about the security policy and its objectives).
- **Prioritisation**: A manager who is authorised to make decisions regarding security incidents will assess the priority, severity, impact, timescales and other relevant factors. Where necessary, the product and environment will be isolated, contained or quarantined to avoid further security incidents.
- **Handling**: A technical employee will be assigned to resolve the security incident, with appropriate documentation updates, regression testing and concluding report, as required.
- **Management**: A manager will approve and authorise the full and final resolution of the security incident. The product can then be released back into the live environment.
- **Lessons Learnt**: In accordance with the Process Improvement principle of the organisation’s Quality Management System (QMS), any lessons learned from the handling and management of the security incident will be merged back into the formal QMS documentation for future reference. It may also be useful to provide security awareness training, arrange periodic testing, improve the security response capability and use additional security tools.
Tampering and other compromises

<table>
<thead>
<tr>
<th>Component</th>
<th>Protective Marking</th>
<th>Action if lost or compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>diskAshur PRO\textsuperscript{2}</td>
<td>OFFICIAL</td>
<td>Invoke the Security Incident procedure as described previously in this section. Inspect the Product tamper-evident covers regularly following deployment.</td>
</tr>
<tr>
<td>diskAshur DT\textsuperscript{2}</td>
<td>OFFICIAL</td>
<td>Invoke the Security Incident procedure as described previously in this section. Inspect the Product tamper-evident covers regularly following deployment.</td>
</tr>
</tbody>
</table>

**Table 2 - Actions to be taken after actual or suspected communications security incident**

**Incident management**

46. In the event of a security incident that results in the compromise of information protected by the Products, the local IT security incident management policy should ensure that the Department Security Officer (DSO) is informed.

47. Subsequently, the Factory Reset function should be applied to the Product, as described in the User Manual [g] and [h], and the security configuration for the Product should be re-established in accordance with the Security Procedures and the original or current usage requirements.

48. Contact NCSC if a compromise occurred that is suspected to have resulted from a failure of the Products.

49. Also see row 3 of the table in Appendix A of the User Manual [g] and [h].
Chapter 5 - Disposal and Destruction

50. Specific procedures are required if the Product contains sensitive data, or has been used for sensitive or classified purposes, and needs to be purged in accordance with the Organisational Security Policy, before Disposal (including re-purposing) or Destruction.

51. Disposal or destruction should be carried out in accordance with the secure sanitisation guidance in HMG IA Standard No. 5 (IS5) [b]. Appendix B of the User Manual [g] and [h] provides guidance on Sanitisation and Secure Disposal.

52. It is recommended that a Factory Reset of the Product is completed first, followed by either the Disposal of Equipment procedure or the Destruction of Equipment procedure, as summarised below.

Reset of Equipment

53. The Product supports a Factory Reset function, which resets all configuration and permission settings. Therefore, before disposal or destruction of a Product, NCSC recommends that customers and end users follow the “How to perform a complete reset” procedure, as described in the User Manual [g] and [h], and then verify that the reset has been completed by reviewing the configuration settings.

54. If the Product has failed and it is not possible to perform the Reset function, then the choice of destruction method must take into account that the memory has not been securely erased (even though it is encrypted).

Disposal of Equipment

55. The correct sanitisation procedures for Disposal (including Re-Purposing) should be determined by using Annex A of IS5 [b].

Destruction of Equipment

56. For Destruction of the Product in accordance with IS5, there are two options:

- Destroy only the Security Controller and the Cryptographic Controller.
- Destroy the entire Product.

Emergency destruction

57. The Products provide a Self-Destruct function, as described in Chapter 3, which can be used when secure emergency destruction is required.
Chapter 6 - Password Policy

58. Passwords for the User and Administrator must be changed from the default value and be defined in accordance with the Organisational Security Policy. The default password must never be used on a deployed Product.

59. The Password Policy is that a password must be:

   - At least eight characters in length;
   - Include complexity using the **SHIFT** key to access additional characters, as described in paragraph 19;
   - Unique for every Product and not generated in a way that would allow the password for one product to be derived if the password for another product was determined;
   - Changed whenever there is an identified risk that it has been compromised;
   - Stored in an appropriate location for the highest classification of data on the Product or the host computer that the Product is connected to (if it is necessary to record passwords);
   - Not disclosed to anyone who does not have a business need-to-know.

60. When using words mnemonics (to simulate a character-based password) to initially define a PIN, note that there is a potential risk of multiple duplicate digits, which may subsequently result in an invalid PIN. In such cases, different words mnemonics must be chosen to ensure a valid PIN.

61. Ensure that the threat of Shoulder Surfing (i.e. direct observation of a password) is reduced, especially in public or untrusted areas, by adequately shielding the keyboard during password entry.

62. General guidance is provided in NCSC’s Password Guidance – Simplifying Your Approach [c].
References

Unless specifically stated otherwise below, these documents are available from the NCSC IA Policy Portfolio or from https://www.ncsc.gov.uk/cisp.


[b] HMG IA Standard No. 5, Secure Sanitisation, Version 5.1, December 2014, NCSC.

[c] NCSC Password Guidance, including infographic: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

   https://www.iso.org/isoiec-27001-information-security.html


# Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CPA</td>
<td>Commercial Product Assurance</td>
</tr>
<tr>
<td>DSO</td>
<td>Department Security Officer</td>
</tr>
<tr>
<td>DT</td>
<td>The desktop diskAshur range</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Dual Generating Encryption</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>Host Computer</td>
<td>The computer on which the diskAshur product is being used.</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LOCK / UNLOCK</td>
<td>Specific buttons on the keypad of the diskAshur products.</td>
</tr>
<tr>
<td>IP</td>
<td>Ingress Protection</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PRO</td>
<td>The portable diskAshur range</td>
</tr>
<tr>
<td>QMS</td>
<td>Quality Management System</td>
</tr>
<tr>
<td>QSG</td>
<td>Quick Start Guide</td>
</tr>
<tr>
<td>RMA</td>
<td>Return Merchandise Authorisation</td>
</tr>
<tr>
<td>RO</td>
<td>Read-Only</td>
</tr>
<tr>
<td>RW</td>
<td>Read-Write</td>
</tr>
<tr>
<td>SC</td>
<td>Security Characteristics</td>
</tr>
<tr>
<td>Security Characteristic</td>
<td>A standard which describes the necessary mitigations which must be present in a completed product, its evaluation or usage, and which are particular to a type of security product.</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>UM</td>
<td>User Manual</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>XTS</td>
<td>XEX-based tweaked codebook mode with ciphertext stealing; a mode of AES.</td>
</tr>
</tbody>
</table>