	No of Pages	1 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
STORAGE MEDIA HANDLING	Doc No	ISMS-PHY-02
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release



	No of Pages	2 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
STORAGE MEDIA HANDLING	Doc No	ISMS-PHY-02
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE.....	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES	3
PROCEDURE.....	3
1 USE OF REMOVABLE MEDIA	3
2 DATA TRANSFER TO THIRD PARTIES	3
3 DATA BACKUPS.....	3
4 MANAGEMENT OF REMOVABLE MEDIA FOR THE STORAGE OF CONFIDENTIAL DATA	4
5 SECURE RE-USE OR DISPOSAL OF STORAGE MEDIA.....	4
FORM	5

	No of Pages	3 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
STORAGE MEDIA HANDLING	Doc No	ISMS-PHY-02
	Revision	1.0

PURPOSE

The purpose of this document is to ensure secure disclosure, storage, deletion or destruction of information on storage media.

SCOPE

This control applies the lifecycle of the storage media authorized for use in the organisation.

REFERENCE

ISO/IEC 27001 Standard Annex A 7.10 Storage Media

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The MR shall ensure consistent implementation and communication of the controls stated here for the use of storage media.

PROCEDURE

1 Use of Removable Media


Where storage media is required to be used, it should be assessed whether an alternative, more secure method can be used and if not, how best to secure the current method so that the risk to information is minimised. Any removable media device inserted into company-issued devices will be automatically scanned.

ISMS-ORG-05 Information Classification, Labelling & Transfer shall be observed with regards to information inside the storage media.

2 Data Transfer to Third Parties

The most secure method of data transfer to third parties will be via company email or authorized cloud transfer with proper access rights set up depending on the information classification level. Only in exceptional circumstances where this is not possible, an encrypted / password protected storage media may be suitable, ideally taken to the third party by the authorized personnel. If not, it should be sent by an approved courier with a tracking facility and requiring a signature at the other end.

3 Data Backups

	No of Pages	4 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
STORAGE MEDIA HANDLING	Doc No	ISMS-PHY-02
	Revision	1.0

Where users are taking their own backups of data onto removable storage media, they should be advised that this contravenes the organisation's policies and should refrain from doing so.

4 Management of Removable Media for the Storage of Confidential Data

Confidential information including personal data stored on removable storage media (e.g. USB storage devices, portable hard drives, SDs) must be encrypted to protect its confidentiality.

The DPO shall ensure that any use of removable media, if approved for use, for the storage of personal data is documented. Only storage media that permits encryption shall be authorized for storing personal data.

All incoming and outgoing physical media containing personal data (if unavoidable) should be recorded, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Encryption measures shall ensure that the data can only be accessed at the point of destination and not in transit. Decryption capabilities must be restricted only to authorized recipient.


Where removable media on which personal data is stored is disposed of, the user shall ensure that previously stored personal data will not be accessible.

5 Secure Re-Use or Disposal of Storage Media

The following guidelines shall be ensured to minimize the risk of information leakage to unauthorized persons during re-use or disposal of storage media:

- Equipment for disposal or re-use that could possibly contain storage media will be verified to ensure whether or not storage media is contained.
- For storage media containing personal data, copyrighted information or licensed software, or any sensitive information, it should be verified to ensure that this type of information and software has been removed or securely overwritten prior to disposal or re-use.
- If external party will be engaged for collection and disposal, care should be taken in selecting a suitable external party with adequate controls. Agreements shall be signed accordingly covering confidentiality and if applicable, data protection prior to the start of engagement. A certificate of disposal / destruction shall be obtained from the external party once the disposal / destruction has been completed.
- Whilst awaiting disposal, the device must be stored securely to prevent unauthorised access e.g., locked room or cabinet.
- Damaged devices containing personal data and other sensitive information may require an assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.
- Media storage on leased equipment shall be removed before equipment is returned. The media that was removed should be sanitized prior to re-use, or destroyed if no longer needed.

Re-use of laptops is only allowed for employees (new or temporary staff). The following are performed prior to handover of equipment.

	No of Pages	5 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
STORAGE MEDIA HANDLING	Doc No	ISMS-PHY-02
	Revision	1.0

- Physical search and review of files and folders to ensure there is no non-operating system files / folders that remain.
- Factory reset Windows installation (remove everything)

Secure disposal may be performed in-house or by a 3rd party who can provide a certificate of data destruction. The following are approved methods of destruction:

- For disposal of magnetic storage media, shall use DoD 5220.22-M secure overwriting. For magnetic storage media that is faulty and cannot be overwritten, it shall be degaussed and shredded or incinerated.
- For disposal of non-magnetic storage media, (e.g., optical or solid-state media such as CD, DVD, memory card, thumb drive, etc), shall physically destroy the non-magnetic storage media by disk shredding (for 3rd party disposal) or hammering (for internal disposal).

The following procedures shall be adhered to as part of the secure erasure of storage media:

- Only authorised staff or approved 3rd party disposal vendor shall perform destruction;
- Media shall continue to be:
 - Physically secured at all times based on its security classification; and
 - Under the custody of authorised staff until data has been sanitised beyond recovery. and
- Disposal details shall be recorded in the *ISMS-PHY-02-F1 Asset Disposal Form* to maintain an audit trail.

FORM

ISMS-PHY-02-F1

Disposal Form