



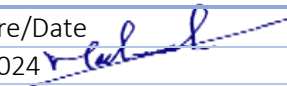
Physical Media Transfer Procedure

Doc. Control Number	Version
SNL-41	0.2



Document Reference

Item	Description
Title	Physical Media Transfer Procedure
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	23 May 2024
Revision-Date	23 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/23/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/23/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/23/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May 2023	Muhaned Ali	First Release
0.2	23 May 2024	Muhaned Ali	The document has been reviewed



Contents

1. Overview	4
2. Scope.....	4
3. Physical media transfer procedure	4

1. Overview

There are occasions when SNLC needs to share sensitive information with other parties. This may be for a variety of purposes including day-to-day commercial arrangements, merger and acquisition projects and joint ventures.

Under such circumstances it is important that the method by which information is transferred is understood and documented and that all parties involved are fully aware of the precautions that must be taken to ensure the confidentiality, integrity, and availability of the information.

2. Scope

This procedure specifies the methods by which appropriately secure physical media transfers will be made in the SNLC.

3. Physical media transfer procedure

Media containing information should be protected against unauthorized access, misuse, or corruption during transportation. The following guidelines should be considered to protect media containing the information being transported:

- Reliable transport or couriers should be used.
 - A list of authorized couriers should be agreed with management.
 - Procedures to verify the identification of couriers should be developed.
 - Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers 'specifications.
 - Logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.
- Information to be transferred.

This procedure describes the steps involved in performing the following media transfer:

INFORMATION TO BE TRANSFERRED	[Customer order information, including names and addresses]
INFORMATION CLASSIFICATION	Restricted
TRANSFEROR	[Name of Transferor company]
RECIPIENT	[Name of Recipient company]
PURPOSE OF TRANSFER	Allow outsourced picking and dispatching of customer orders
FREQUENCY OF TRANSFER	Weekly
TRANSFER SERVICE LEVEL	24 hours
MAIN TRANSFER METHOD	Physical transfer via courier

- Triggering the procedure
This procedure will begin upon the Sender being provided with the packaged physical media by the information producers.
Due to the sensitive nature of the information, the media will be encrypted using standard encryption methods specified by the company. This will involve the use of a pre-shared key between the Sender and the Receiver.

The physical media will be packaged using bubble wrap and a padded envelope. The address of the Receiver will be written on the outside of the package and checked by more than one person.

- Notifying transmission, dispatch, and receipt

When a package is ready to be sent, the Sender will inform the Receiver via email at the following address:

To Khobar mlh@saudinetlink.com Mark Dave Hernandez

To Riyadh hsm@saudinetlink.com Mohammed Hendy

The Receiver will confirm via email that they are aware that a package is being sent.

- Use of couriers

Only couriers on the approved list will be used to transfer the information. Under no circumstances should other couriers be used.

The courier should only be contacted using the telephone number detailed on the approved list. The Sender will check the courier's identification, give the package to the courier personally and obtain a signature for it. The level of service for the delivery and the tracking information should be confirmed by the courier as part of the handover. The dispatch documentation should then be placed in the physical transfer record file as evidence of traceability.

- Chain of custody

A signature must be obtained at each point in the process where the package changes hands. Where available the package should also be tracked electronically by both parties (Sender and Receiver).

On dispatch a further email will be sent by the Sender to the Recipient specifying the courier details, including the tracking reference.

- Incident management procedures

The package should arrive within the transfer service level stated. If the package is lost or becomes damaged in any way, the Recipient must inform the Sender as soon as this becomes clear. The circumstances of the loss or damage should be recorded, and the information security manager informed.

Appropriate action will then be taken to address the situation. This may include:

- Informing senior management
- Informing regulatory authorities
- Beginning a forensic investigation

Full cooperation will be required from all parties to the physical media transfer.

- Access control

On arrival at the Receiver, access to the package must be strictly controlled. Only employees with sufficient clearance should be allowed to handle it. The package should be received in an area that has been assessed and cleared for the purpose and ideally to which public access is not permitted.

The package should be signed by an authorized individual only.

- Decryption and processing

Once received, the file will be decrypted using the appropriate key and passed to the relevant department for processing.