NTT DATA Payment Services Sdn. Bhd.

(formerly known as GHL Systems Sdn. Bhd.)

Group Anti-Money Laundering, Anti-Terrorism Financing, And Proceeds of Unlawful Activities ("AML") Policy

NTT DATA Payment Services Sdn. Bhd.
C-G-15, Block C, Jalan Dataran SD1,
Dataran SD, PJU 9, Bandar Sri Damansara,
52200 Kuala Lumpur, Malaysia.

www.nttdatapay.com

VERSION CONTROL

Version	Approval Date	Prepared By	Approved By
1.0	*/12/2019	-	Board of Directors
2.0	28/11/2022	Group Legal, Compliance & Sustainability	Board of Directors
3.0	27/02/2024	Group Legal, Compliance & Sustainability	Board of Directors
4.0	30/07/2025	Group Legal, Compliance & Sustainability	Board of Directors

COPYRIGHT AND OWNERSHIP

This Group Anti-Money Laundering, Anti-Terrorism Financing, And Proceeds of Unlawful Activities ("AML") Policy is issued by Group Legal, Compliance & Sustainability.

CONTENTS

1. INTRODUCTION

1.1 STATEMENT OF COMMITMENT

1.1.1 NTT DATA Payment Services Sdn Bhd, its related corporations as defined under the Companies Act 2016, and any other entities within the NTT DATA Group for which NTT DATA Payment Services Sdn Bhd provides management oversight and strategic direction as the regional headquarters, now and in the future, with each such company being a member of the NTT DATA Payment Services Group of Companies (the "Group") commits to protect its business operations and activities from any form of financial crime, particularly from laundering the proceeds of unlawful activities and financing terrorism under the Group's Code of Business Ethics. All directors and employees across the Group must demonstrate the commitment to respond to these threats. All directors and employees must comply with the anti-money laundering ("AML") and counter-financing of terrorism ("CFT") laws and regulations ("AML/CFT Laws") and stay vigilant for suspicious activities and report them in a timely manner.

1.1.2 This Group Anti-Money Laundering, Anti-Terrorism Financing, And Proceeds of Unlawful Activities ("AML") Policy ("Policy") sets out the guidelines and requirements of the Group relating to compliance with AML/CFT Laws. While the parent company, NTT DATA Japan Corporation, is located in Japan, NTT DATA Payment Services is incorporated in Malaysia. The Malaysian Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLA") sets the minimum standard which must be complied across its business and operations within the Group in the ASEAN region.

1.1.3 Notwithstanding the above, should there be any discrepancies between the anti-money laundering laws in any of the particular offices situated in other countries with the AMLA, then the said anti-money laundering laws of that country shall prevail.

1.2 PURPOSE

The purpose of this Policy is to define:

a) money laundering and terrorism financing;

b) the roles and responsibilities of Board of Directors, Senior Management and employees of the Group;

c) the preventive measures to prevent money laundering and terrorism financing;

d) consequences of non-compliance; and

e) breach of the Policy.

2. APPLICATION

2.1.1 This Policy applies to all the directors and employees within the Group and across all business and operations of the Group. The requirements in this Policy apply in addition to any local legal or regulatory requirements and must be observed even if the local law or regulation imposes less stringent requirements (or does not prescribe any specific requirements).

3. DEFINITION

3.1 MONEY LAUNDERING

3.1.1 Money laundering may be simply defined as a process to make 'dirty' money look 'clean'. It is intended to hide proceeds from an unlawful activity so that they appear to be from a legitimate source.

3.1.2 A money laundering operation commonly involves three (3) steps:

a) Placement

To separate the illicit funds from their illegal sources. For example, to deposit the money into a legitimate financial institution or breaking down transactions into smaller amounts.

b) Layering

To create multiple layers of transactions to further distance the illicit funds from their illegal sources. For example, multiple transfers, repeat invoicing for the same transaction or re-sale of assets originally purchased in cash by using the illicit funds.

c) Integration

To integrate illegal proceeds into the economy so it appears legitimate. For example, purchasing high values items or engaging in legal business by providing capital or loans.

3.2 TERRORISM FINANCING

Acts of terrorism seek to influence or compel governments into a specific action or to intimidate the public or a section of the public. These acts require funding and terrorism financing is the act of providing or collecting property (whether directly or indirectly) with the intention or knowledge that the property will be used to commit an act of terrorism. For example, providing services for terrorist purposes, arranging for retention of terrorist property or dealing with terrorist property.

3.3 PROCEEDS OF UNLAWFUL ACTIVITIES

The proceeds of an unlawful activity are an act of deriving, obtaining, acquiring property or economic advantage from such property from the unlawful activity.

4. ROLES AND RESPONSIBILITIES

4.1 Board of Directors

The Board of Director are responsible to:

a) maintain accountability and oversight for establishing the policies and minimum standards related to AML and CFT;

b) approve the policies related to AML and CFT;

c) establish appropriate mechanisms to ensure the policies are periodically reviewed and assessed in line with development of the Group business as well as the trends in AML and CFT; and

d) assess the implementation of the approved policies through regular reporting and updates by the Senior Management.

4.2 Senior Management

The Senior Management are responsible to:

a) appoint an officer at the Senior Management level to carry out AML and CFT responsibilities;

b) be aware of and understand the money laundering and terrorism financing risks associated with the business and operations of the Group;

c) formulate the procedures to ensure they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken;

d) ensure proper implementation of the policies and procedures related to AML and CFT including customer due diligence, risk assessment, on-going due diligence, reporting of suspicious transactions and record keeping;

e) provide timely periodic reporting to the Board on the level of money laundering and terrorism financing risks being faced, strength and adequacy of risk management and internal controls implemented to manage these risks;

f) allocate adequate resources to effectively implement the policies and procedures related to AML and CFT;

g) provide appropriate levels of AML and CFT training for the employees at all levels

throughout the organization;

h) ensure that there is a proper channel of communication in place to effectively communicate AML and CFT policies and procedures to all levels of employees.

4.3 Employees

All employees of the Group are responsible to comply with this Policy, all applicable AML/CFT Laws and to ensure the effective management of money laundering and terrorism financing risk within the scope of their direct organizational responsibilities.

5. KNOW YOUR CUSTOMER-CUSTOMER DUE DILIGENCE (CDD)

5.1 The Group is required to conduct CDD and obtain satisfactory evidence and properly establish in its records, the identity and legal existence of any person applying to do business with it. CDD information is a tool to know and verify the identity of the customers and enable assessment of money laundering and terrorism financing risk.

5.2 The Group must conduct CDD when:

a) establishing business relationship with any customer;

b) carrying out cash or occasional transaction that involves a sum in excess of the amount specified by amount specified by the local regulator, for example, payment to customers and suppliers;

c) it has any suspicion of money laundering or financing of terrorism; or

d) it has any doubt about the veracity or adequacy of previously obtained information.

5.3 In conducting CDD, the measures undertaken by the Group should comprise of the following:

a) identify and verify the customers and the suppliers;

b) identify and verify beneficial ownership and control of such transaction;

c) obtain information on the purpose and intended nature of the business relationship or transaction; and

d) identify the source of funds or wealth if the customer is assessed as higher risk.

5.4 The Group is required to be aware of and gather the following information or documents from the potential customer or supplier before the commencement of the business and from the existing customer or supplier in conducting CDD:

a) name, IC/passport number, address, nationality, purpose of transaction, beneficial owner's details if any for individual customer;

b) company name, business registration number, business address/registration address, nature of business, location of business, directors and shareholders' details, purpose of transaction, beneficial owners' details if any for companies.

5.5 Unwillingness of the customer or supplier to provide the information requested and to cooperate with the Group for the CDD process may itself be a factor of suspicion. If the customer is a potential customer, the Group should not open any account or commercial business relationship or perform any transaction. If the customer is an existing customer, the Group should terminate the business relationship.

5.6 The Group is required to perform enhanced CDD where the money laundering or terrorism financing risks are assessed as higher risk and conduct on-going due diligence and scrutiny to ensure the information provided is updated and relevant.

6. SCREENING OF CUSTOMERS

6.1 The Group is required to do screening to check whether the new and existing customers are listed on the list of sanctioned individuals and entities.

6.2 If the customer's name matches with the list of sanctioned individuals and entities, the Group is required to freeze funds for existing customers, reject transactions for new customers and report to the relevant authority.

7. RISK ASSESSMENT

The Group is required to take appropriate steps to identify and assess money laundering and terrorism financing risks in relation to the customers, that is, to conduct risk profiling by identifying those customers associated with high risk of money laundering and financing of terrorism.

7.1 CUSTOMER RISK PROFILING

7.1.1 In conducting the Customer Risk Profiling, the Group should take into consideration risk factors including but not limited to:

a) <u>Customer Risk</u>

i. Resident or non-resident;

ii. Individual or company;

iii. Structure of company;

iv. Political Exposed Person (PEP);

v. Types of occupation or nature of business;

vi. Customer from high risk countries.

b) Geographical Risk

i. Business location

ii. Country of origin;

iii. Country on sanction list

c) Risk associated with transaction/delivery channels

i. Mode of payment such as cash, e-payment;

ii. Face to face or non-face to face;

iii. Cross border transaction;

iv. Occasional or one-off transaction.

d) Any other information suggesting that the customer is of higher risk.

7.2 RISK MONITORING

Following the initial acceptance of the customer, the Group is required to regularly monitor, review and update the customer's risk profile based on their level of money laundering and terrorism financing to ensure it is in line with the customer's profile. Unreasonable differences should prompt the Group to reassess the customer's risk profile.

8. SUSPICIOUS TRANSACTION REPORTING

The Group is required to promptly submit a Suspicious Transaction Report ("STR") facilitated by Group Risk Department to the local regulator in charge when any of its employees suspect that the transaction involves proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism.

8.1 REPORTING MECHANISMS

8.1.1 The Group should appoint one officer at the Senior Management level to be the person responsible for the submission of STR to the local regulator in charge.

8.1.2 Upon receiving any internal STR whether from the head office, branch or subsidiary, the officer should evaluate the grounds for suspicion and if suspicion is confirmed, promptly submits the STR to the local regulator in charge immediately and no later than within the next working day from the date of establishing the suspicion. In the case where the officer decides that there are no reasonable grounds for suspicion, he or she should document his or her decision, ensure it is supported by the relevant documents and file the report.

8.1.3 In the case of Malaysia, the STR submitted must comprise the following information in the STR (please refer to Appendix I and this Appendix shall be amended accordingly in accordance with the laws and regulations of the particular country):

a) information on the person conducting the transaction;

b) information on the account holder or beneficiary of the transaction;

c) details of the transaction, such as the type of products or services and the amount involved;

d) a description of the suspicious transaction or its circumstances; and

e) any other relevant information that may assist the relevant authority in identifying potential offences and individuals or entities involved.

9. RECORD-KEEPING

9.1 The Group is required to keep the relevant records including any account, files, and business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and beneficial owners, and results of any analysis undertaken.

9.2 The Group is required to keep the records for at least seven (7) years following the completion of the transaction, the termination of business relationship or after the date of occasional transaction.

9.3 In situations where the records are subjected to on-going investigations or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.

10. EMPLOYEE TRAINING AND AWARENESS PROGRAMME

10.1 The Group is required to conduct an awareness and training program on AML and CFT practices and measures for its employees.

10.2 The training conducted for employees must be appropriate to their level of responsibilities in

detecting money laundering and terrorism financing activities and the risks faced by the Group.

10.3 Training may be provided to specific categories of employees:

a) Front-Line Employees

Employees who deal directly with the customers are the first point of contact with potential money launderers and financiers of terrorism. Hence, they must be trained to conduct effective ongoing customer due diligence, detect suspicious transactions and the measures that need to be taken upon determining a transaction as suspicious.

b) Employees that Establish Business Relationship

Employees who are responsible for acceptance of new customers must receive the equivalent training given to "front-line" employees. The training should be focused on customer identification, verification and customer due diligence procedures, including when to conduct enhanced due diligence and circumstances where there is a need to defer establishing business relationships with new customers until customer due diligence is completed satisfactorily.

c) Heads of Department and Managers

The training on Heads of Department and Managers may include overall aspects of AML and CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customers, and enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures.

d) New Employees

Provide a general background on money laundering and terrorism financing, the requirement and obligation to monitor and report suspicious transactions to and the importance of the CDD.

11. CONSEQUENCES OF NON-COMPLIANCE OF AML/CFT LAWS

Enforcement action can be taken against the Group including its directors, officers, and employees for any non-compliance of AML/CFT Laws. In the case of Malaysia, penalties for breach under AMLA include:

a) Section 14A provides that any person who fails to disclose suspicious transaction report and related information shall be liable for a fine of not exceeding RM3 million or to imprisonment for a term not exceeding 5 years or to both;

b) Section 17(4) provides that failure of retention of records shall be liable to a fine of not exceeding RM3 million or to imprisonment for a term not exceeding 5 years or to both;

c) Section 22 provides that officer appointed who fails to takes all reasonable steps to ensure its compliance under Part IV of the Act commits an offence and shall be liable to a fine not exceeding RM1 million or to imprisonment for a term not exceeding 3 years or to both;

d) Section 66E(5) provides that any person who contravenes any direction or guidelines issued by the relevant regulatory commits an offence and shall be liable to a fine not exceeding RM1 million;

e) Section 86 provides that any person who contravenes any provision of the Act or any regulations made under the Act commits an offence and shall be liable to a fine not exceeding RM1 million if no penalty is expressly provided for the offence under the Act or the regulations;

f) Section 92 empowers Bank Negara Malaysia to compound with the consent of the Public Prosecutor, any offence under the Act or its regulations by accepting from the person reasonably suspected of having committed the offence such amount not exceeding 50% of the amount of the maximum fine for that offence including the daily fine if in the case of a continuing offence;

g) In the case of a continuing offence, a further fine may be imposed not exceeding RM3,000 for each day during which the offence continues after conviction.

12.BREACHES OF THE POLICY

Any employee who identifies a breach of this Policy must report it immediately to their immediate direct reporting Head of Department or any of the Senior Management to carry out AML and CFT responsibilities. Failure to comply with this Policy, including reporting expediently any breach which has occurred may subject the employee to disciplinary action up to and including dismissal. Depending on the severity of the breach, it may lead to criminal prosecution and/or sanctions.

13.REVIEW OF THE POLICY

This Policy and any of its appendixes may be reviewed and updated when necessary by the Group Legal, Compliance and Sustainability Department. Reviews will take into account changes in laws and regulations, changes in the Group's businesses and operations, as well as changes in the general business environment.

APPENDIX I

SUSPICIOUS TRANSACTION REPORT TEMPLATE (MALAYSIA)

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Please send completed form to:
Financial Intelligence & Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur
Fax: 03-2693 3625 E-mail: str@bnm.gov.my

Reference No: _____
CO Reg. No: _____

SUSPICIOUS TRANSACTION REPORT

FOR MONEYLENDERS AND PAWNBROKERS

a. This report is made pursuant to the requirement to report suspicious transaction under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)
b. Under section 24 of the AMLA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith

PART A: INFORMATION ON CUSTOMER

Account Holder

1)

Nationality				
Name				
Other/previous name	(1)			
	(2)			
	(3)			
New NRIC no			Old NRIC no	
Other identification			Other identification type	
Gender				

Contact information

Residential/Business Address	Correspondence Address

Other Address	Previous Address

Email address:					
Contact No.		-(Off)		-(Res)	-(Mob)
Fax No.					

Employment information

Business/employment type	
Occupation	
Occupation description	
Employer name	
Employment area	
Other known employment	

Marital Information

Marital status	
Spouse name	

Spouse identification

New NRIC no		Old NRIC no	
Other identification		Other identification type	
Passport no		Place/country of issue	

PART B: TRANSACTION DETAILS

Attempted but not completed transaction	
Customer ref no	
Transaction type	

Transaction date	
Transaction amount (MYR)	

Other information

Type of loan	

PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION

Grounds for suspicion	Client settles loan with one lump sum payment
	Client continuously borrows and settles the loan in a short period of time
	Client repays the loan with a cheque from a third party, other than spouse or family members
	Client refuses to disclose mode of repayment for the loan
	Others (please specify)
Description of suspected criminal activity	
Details of the nature and circumstances surrounding it	
Date of reporting	