



Group Policy

Anti-Money Laundering Policy

NTT Limited

01 April 2021 | Document Version 2.0

Governance, Risk and Compliance

sean.meisel@global.ntt

Information Asset Classification: General

Document Control

Document Name	NTT Limited Anti-Money Laundering Policy
Document Owner	Sean Meisel, Senior Vice President, Group Governance and Risk
Document Storage	https://nttlimited.sharepoint.com/sites/NTT-RiskManagement/SitePages/Compliance-and-Ethics.aspx
Last Reviewed	18 March 2021
Next Review Date	January 2021
Approved by	Sean Meisel, Senior Vice President, Group Governance and Risk
Version on release	V 2.0

Date	Version	Comments
March 2020	V 1.0	Published
December 2020	V 1.1	First Draft
March 2021	V 1.2	Review
April 2021	V 2.0	Published

Supporting Policy or Documentation	Owner
Code of Conduct and Business Ethics	Sean Meisel, Senior Vice President, Group Governance and Risk
Group Authorities Matrix	Sean Meisel, Senior Vice President, Group Governance and Risk
SpeakUp Policy	Sean Meisel, Senior Vice President, Group Governance and Risk
Anti-Bribery and Corruption Policy	Sean Meisel, Senior Vice President, Group Governance and Risk
Risk Management Framework and Policy	Sean Meisel, Senior Vice President, Group Governance and Risk



Table of Contents

- Document Control..... 2
- 1. Introduction..... 4**
 - 1.1. Purpose 4
 - 1.2. Scope..... 5
 - 1.3. Non-compliance with the AML Policy..... 5
 - 1.4. SpeakUp..... 5
 - 1.5. Local Variations and Exceptions..... 5
 - 1.6. Training 6
 - 1.7. Audit and Compliance 6
 - 1.8. Continual Improvement..... 6
- 2. Roles and Responsibilities 7**
- 3. Policy Requirements 10**
 - 3.1. Third Party Due Diligence and Know-Your-Client ('KYC')..... 10
 - 3.2. Suspicious Activity 10
 - 3.3. SpeakUp and Reporting Suspicious Activity..... 11
 - 3.3.1 SpeakUp 11
 - 3.3.2 Reporting suspicious activity..... 11

1. Introduction

NTT Ltd. and each of its subsidiaries and affiliates ('**NTT**', '**we**', '**us**', '**our**') want to create an ethical culture that empowers our people to do the right thing and act with integrity, even when no one is watching.

We all have a responsibility to protect our reputation and avoid any exposure to situations in which we could inadvertently become involved in any transactions that facilitate money laundering or unlawful diversion. Money laundering occurs when the proceeds of criminal activity are disguised by being funneled through legitimate business dealings, or when legitimately generated funds are used to finance criminal activities, including terrorism. Money laundering is internationally recognized as a serious financial crime, with strict regulations and associated penalties enforced across many of the locations in which we operate.

Terrorism financing involves dealing with money or property that may be used to finance terrorist activities. The money and property may be from either legitimate or criminal sources and may be of any amount. The methods used by terrorists to move money and/or assets are substantially the same as those used by other criminals, such a false invoicing and trading in high-value commodities that are easily converted to cash.

We take steps to detect and prevent unacceptable or illegal forms of payment and financial transactions. Anti-money laundering ('**AML**') laws and regulations require transparency of payments and the identity of all parties to transactions. We are committed to full compliance with AML laws and regulations throughout the world and will conduct business only with reputable clients and third parties who can demonstrate both the legitimacy of their activities and funding, and that they have effective AML controls in place.

Our Anit-Money Laundering Policy ('**AML Policy**') describes our commitment to conducting business in a transparent, ethical, and lawful way by ensuring that we have measures in place for AML throughout our business operations globally.

1.1. Purpose

The purpose of the AML Policy is to:

- demonstrate and reinforce our commitment to conduct business globally with the highest level of transparency, ethics and integrity;
- ensure compliance with all applicable AML laws and regulations that apply to our business operations;
- assign roles and responsibilities for AML across our business operations;
- manage the risk of serious financial loss, penalties, criminal liability, and other negative business impacts which may result from failure to detect, prevent, and report actual or suspected money laundering or terrorist activities;
- protect our reputation as a trustworthy and responsible business and maintain the confidence of our clients, third parties and communities; and
- maximize shareholder value and ensure sustainable business operations by protecting NTT's brand and reputation against any accusations of misconduct, criminal activity, or terrorist financing.

1.2. Scope

The AML Policy applies to NTT and all our people (including employees, directors, and contractors; hereafter referred to as '**our people**', '**employees**', '**you**', '**your**') and third parties (including partners, joint ventures, suppliers, vendors, service providers and consultants).

1.3. Non-compliance with the AML Policy

Any breach of the AML Policy is a disciplinary offence subject to disciplinary action and/or any action permitted by law.

The penalties for breaches of the AML Policy and/or applicable laws and regulations, which apply to both the employee concerned and NTT can include the imposition of sanctions, financial penalties, and criminal prosecution, resulting in prison sentences for the perpetrator and any other parties involved who fail to report suspicions of money laundering in addition to heavy fines.

1.4. SpeakUp

It is your duty to SpeakUp if you know of or suspect any unethical behaviour or misconduct that could be a breach of the AML Policy, our Code of Conduct and Business Ethics ('**our Code**') or any other NTT policies.

If you are unsure whether an activity or transaction is in contravention of the AML Policy, or if you have any queries, these should be raised with your line manager, local Governance, Risk and Compliance or Legal team, local executives, or Group Governance, Risk and Compliance.

You can report your concerns to our anonymous and confidential SpeakUp platform, online or over the phone, as follows:



For our people: www.speakupfeedback.eu/web/ntt

For our clients, third parties and other stakeholders:

www.speakupfeedback.eu/web/nttexternals



Over the phone by dialing your country specific SpeakUp number as outlined in Appendix A of our [SpeakUp Policy](#)

We operate a strict non-retaliation policy for all reports made in good faith, meaning that any act or threat of retaliation for reporting concerns (such as dismissing, transferring, demoting or publicly attacking someone) will not be tolerated.

We are committed to ensuring that no one ever suffers any detrimental treatment for refusing to take part in money laundering or terrorist financing, or reporting wrongdoing.

Our [SpeakUp Policy](#) describes our policies for reporting concerns about any unethical behaviour or misconduct in the business.

1.5. Local Variations and Exceptions

Our operating entities are responsible for compliance with any local laws and regulations that apply to their area of the business. If local laws and regulations establish more rigorous standards than provided in the AML Policy or prohibit any activities outlined in the AML Policy, then local laws and regulations must be followed by the relevant operating entity.

All local variations, additional requirements and/or exceptions to the AML Policy must be reviewed by Group Governance, Risk and Compliance and formally recorded in an addendum to the AML Policy.

1.6. Training

We are committed to building a transparent and ethical culture that ensures that our people, clients and third parties act with integrity in all that we do.

All of our people, clients and third parties must be aware of, understand and follow the AML Policy and any applicable addendums to it.

Our people will receive mandatory, periodic training on the AML Policy, related policies, controls, and practices, relevant to their role. In particular, all new employees will be required to complete mandatory training on the AML Policy and related policies and controls during induction.

1.7. Audit and Compliance

The design, implementation and operating effectiveness of the AML Policy and its associated controls is subject to ongoing monitoring, review, and audit through the performance of periodic self-assessments, compliance assessments and independent audits (including internal and external audit). Where required, updates and/or improvements to the AML Policy will be made based on the observations or findings of the self-assessments, compliance assessments and audits.

Compliance with the AML Policy is monitored on a periodic basis and reported to the NTT Ltd. Board, Group Audit and Risk Committee, Group Governance, Risk and Compliance Committee and senior management.

1.8. Continual Improvement

The AML Policy is subject to continual review and improvement and will be reviewed by Group Governance, Risk and Compliance at least annually.



2. Roles and Responsibilities

The AML Policy is governed, supported, and implemented by the following roles within the company.

NTT Ltd. Board	<ul style="list-style-type: none"> • Ultimately accountable for the oversight and implementation of AML Policy and controls throughout NTT. • Ensure that NTT is committed to values of transparency, ethics, and integrity. • Ensure that our culture reflects our values and lives up to our Code. • Ensure that the organizational structures, systems, and management approaches support the implementation of our values and the AML Policy.
Group Audit and Risk Committee	<ul style="list-style-type: none"> • Ultimately accountable for the oversight and implementation of the Risk Management Framework and Policy. • Approve this Policy and any material local deviations, exceptions or variations, where required.
Group Governance, Risk and Compliance Committee	<ul style="list-style-type: none"> • Responsible for providing oversight and ensuring the effective management of the Business Conduct and Ethics programme. • Enforce non-compliance with the AML Policy.
Senior Vice President, Group Governance and Risk	<ul style="list-style-type: none"> • Owner of the AML Policy and responsible for the periodic review and update of the AML Policy. • Responsible for the management of our risk relating to money laundering and the financing of terrorism. • Responsible for supporting the implementation of the AML Policy through communication and training. • Responsible for investigating any reports related to known or suspected money laundering or terrorist financing activities in the business. • Maintain the confidentiality of all reports of which they are made aware and only share information relating to these reports on a need-to-know basis. • Ensure that any actual or suspected money laundering or terrorist activities are reported to relevant authorities in accordance with applicable laws and regulations.

Executive Vice President, Group Legal	<ul style="list-style-type: none"> • Ensure that any actual or suspected money laundering or terrorist activities are reported to relevant authorities in accordance with applicable laws and regulations. • Maintain the confidentiality of all reports of which they are made aware and only share information relating to these reports on a need-to-know basis.
Business Conduct and Ethics Forum	<ul style="list-style-type: none"> • Manage the Conduct, Ethics and Integrity Principal Risk and ensure that relevant policies, processes, frameworks, standards, and training are in place to support implementation in the business. • Ensure the adoption of and effective implementation of the AML Policy throughout the business. • Provide input and advise on any improvements that may be made to the AML Policy and associated controls in the business. • Communicate with executives and senior management about the AML Policy and associated controls.
Group Governance, Risk and Compliance	<ul style="list-style-type: none"> • Identify, assess, manage, monitor, and report on risks related to money laundering and terrorist financing in accordance with the Risk Management Framework and Policy on a periodic basis.
Group Legal	<ul style="list-style-type: none"> • Monitor regulatory changes that may impact the AML Policy and provide input into the AML Policy to ensure that it meets our legal obligations and is compliant with the relevant laws and regulations that apply to NTT. • Provide legal support and advice on any reports of actual or suspected money laundering or terrorist financing, including where necessary engaging appropriate outside legal counsel.
Regional / Services CEO's	<ul style="list-style-type: none"> • Accountable for ensuring that the AML Policy is implemented within their area of the business. • Provide management oversight over the implementation of the AML Policy in their area of the business. • Ensure that the organizational structures, systems, and management approaches support the implementation of the AML Policy in their area of the business.
Regional / Services Governance, Risk and	<ul style="list-style-type: none"> • Review the AML Policy and identify any local variations, additional requirements and/or exceptions that may be



Compliance Managers / Legal Counsel	required to support compliance with local laws and regulations.
	<ul style="list-style-type: none">• Create sub-policies, processes, standards, guidance, or training to support the implementation of local variations, additional requirements and/or exceptions.• Monitor the design, implementation and operating effectiveness of the AML Policy and its associated controls within their area of the business.• Identify, assess, manage, monitor, and report on local risks relating to money laundering or terrorist financing activities in accordance with the Risk Management Framework and Policy.
Our people and third parties	<ul style="list-style-type: none">• Responsible for ensuring that they have read, understood, and adhere to the AML Policy.• Do not take any actions that will circumvent the AML Policy and its associated controls.• SpeakUp when they know of or suspect any money laundering or terrorist financing activities in the business or breaches of the AML Policy.

3. Policy Requirements

The sections below outline the requirements of the AML Policy and the activities that are prohibited or must be subject to additional control or oversight when undertaken in the business.

Risks associated with money laundering and terrorist financing tend to exist in relation to our clients and third parties. Therefore, it is important that we pay attention to how we assess, select, onboard, and monitor our clients and third parties.

3.1. Third Party Due Diligence and Know-Your-Client ('KYC')

Before engaging in any commercial transaction we must obtain and assess satisfactory evidence of the identity and source of funds of any new third party or client, to ensure that all of their business activities are legitimate, conducted in an ethical manner and free from any involvement with criminal activity or the proceeds of crime. This applies to:

- single transactions;
- new business relationships with third parties or clients which are intended to become ongoing;
- existing third parties or clients that have undergone a change in ownership or management, or operating location; or
- longstanding third parties or clients who have changed the type or volume of business which they provide to NTT.

We must never knowingly deal with any client or third party involved or suspected of involvement with criminal activity or the proceeds of crime.

All third parties with whom NTT has business dealings are required to agree to our Code and the AML Policy, and demonstrate that they have adequate policies and controls in place internally to ensure that they are not exposed to potential money-laundering or terrorist financing activity. All third party due diligence must be performed in accordance with the third party risk management policy and framework.

Each operating entity is expected to develop and implement an appropriate KYC programme to support effective due diligence of our clients at the time of onboarding and on a periodic basis thereafter.

3.2. Suspicious Activity

There is no simple way to identify money laundering or terrorist financing activity, but we all have a duty to be vigilant and ensure that we report any suspicions that we have, even if we cannot be certain that they are correct.

It is better to make a report in good faith that turns out not to require any further action than to fail to report unusual or suspicious transactions. Reports made in good faith that are not confirmed, will not result in any detriment to the individual who has made the report.

Examples of the kind of red flags that could indicate that there is a higher risk of money laundering or terrorist financing include:

- a transaction that is unusual in size, type, or frequency;
- a transaction involving an unusual third party or client due to its size, location, or type;

- a transaction involving a third party or client located in a country that scores below 60 on the Corruption Perception Index (<https://www.transparency.org/en/cpi>);
- a substantial payment made in cash;
- transactions with sanctioned or embargoed third parties, clients or countries;
- a transaction involving the movement of funds overseas, or into or out of a foreign currency;
- a transaction without an obvious legitimate purpose or which appears uneconomic, inefficient, or irrational;
- an absence of obvious legitimate sources for the funds employed in the transaction;
- the cancellation or reversal of an earlier transaction;
- concerns about the honesty, integrity, or identity of the third party or client;
- a poor business record or internal accounting controls; or
- a previous transaction involving the same third party or client that has been, or should have been, the subject of a SpeakUp report.

3.3. SpeakUp and Reporting Suspicious Activity

3.3.1 SpeakUp

If money laundering or terrorist financing activity, is known or suspected it must be reported immediately to the Senior Vice President, Group Governance and Risk and Executive Vice President, Group Legal, or alternatively through our SpeakUp platform as outlined in [section 1.4 of the AML Policy](#).

All oral or written reports made should include as much information as is available in order to enable NTT to determine whether there are reasonable grounds to believe that money laundering or terrorist financing may be taking place and to enable the preparation of the matter.

3.3.2 Reporting suspicious activity

Only the Senior Vice President, Group Governance and Risk and Executive Vice President, Group Legal, or an authorized person appointed by them, are authorized to report any suspicious or actual money laundering or terrorist financing activity to the relevant authorities and can submit a Suspicious Activity Report ('**SAR**').