Catella Group Policy on Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF)

1. Introduction

This Catella Group Policy on Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) (the "**Policy**") applies to all subsidiaries and affiliated companies of Catella AB (the "**Catella Group**"). This Policy is prepared by the Group Management and approved by the board of directors of Catella AB. Deviations from this Policy may only be made if prescribed by local laws and regulations. Wherever local regulations or applicable regulatory requirements are stricter than the requirements set out in this Policy, the stricter standard shall be applied. Any deviation shall be reported to the Head of Group Legal.

1.1. Objective

The objective of this Policy is to describe more in detail what money laundering and terrorist financing is. It provides guidance on how to act in relation to counterparties (such as current and potential transactions, customers, business partners, suppliers etc.). Additionally, it clarifies general questions related to suspicion of actual or potential money laundering or terrorist financing.

The Catella Group complies with applicable laws and regulations, and we do not tolerate any form of money laundering or terrorist financing. By following rules, regulations, standard processes and being transparent in all our activities we aim to ensure that these are ethical and legal.

Money laundering and terrorist financing are activities that threaten the integrity and stability of the international financial system. We are all responsible to prevent the Catella Group from being used to facilitate the movement of criminal proceeds or the transfer of funds destined to finance terrorism. Each entity within the Catella Group is committed to identifying and managing the money laundering and terrorist financing risks that it is exposed to, and to take the proportionate measures required to manage these risks across all jurisdictions in which it operates.

Failure to comply with laws and regulations may have serious consequences for the group and individuals concerned, as involvement in or assisting with money laundering and/or terrorist financing are criminal offences in most countries. All Catella Group employees and Intermediaries must therefore take great care to exercise good judgement at all times. Never compromise ethics when doing business, and if in doubt consult this policy and the Code of Conduct.

.

2. Definitions

Customer Due Diligence (CDD)	means the act of performing background checks on and screenings of counterparties.
Intermediaries	Any person appointed to represent Catella in a particular matter and to whom Catella supplies money or other assets. The decisive aspect is not the title, but the intermediary's actual function. Intermediates may include agents, representatives, brokers, or business intermediaries.
Know Your Customer (KYC)	means the process of verifying the identity of counterparties. The objective is to prevent the Catella Group from being used for illegal activities.
Money Laundering	means the act of concealing the connection between criminal acts and money or other assets by making such proceeds appear to have come from a legitimate source. This may for example include, money obtained from drug or tax offences as well as fraud that is "laundered" in order to be used in the legitimate financial system.
Politically Exposed Person (PEP)	means an individual who is or has been entrusted with prominent public functions in a country or an international organization. Due to its position and influence, a PEP is considered to hold a position which per se constitutes a risk of being exploited for, among other things, bribery, and corruption.
Terrorist Financing	means the concealment of what a sum of money is to be used for. It involves the financial support of terrorism by collecting, providing, or receiving money or other property that is intended, or with the knowledge that it is to be used to finance terrorism. In terrorist financing schemes, so-called reverse money laundering is common, which means that instead of laundering criminal profits, legitimately earned money is often used for illegal activities. This does not rule out the possibility that the money comes from criminal activities, but the main goal of a terrorist financing scheme is to conceal the money transfer until it reaches its final destination.
Ultimate Beneficial Owner (UBO)	means an individual who ultimately owns or controls a company, association or other type of legal entity by, directly or indirectly, holding (i) > 25 % of the votes or (ii) the right to appoint or remove a majority of the board of directors.

3. What not to do - prohibited payments & actions

The Catella Group shall neither establish nor maintain a business relationship with a counterparty that is (i) listed on an applicable sanctions list[1] or (ii) involved in illegal activities.

The Catella Group shall neither engage in transactions that (i) involve unconnected parties, (ii) unusual payment methods (such as crypto currencies or cash) or (iii) unusual terms and conditions.

4. What to do - your obligations

We carry out all activities in a transparent and ethical way with a risk-based approach. Taking a risk-based approach means, in part, that you need to work with risk mitigation to prevent our business from being used for money laundering and terrorist financing.

When faced with current and potential counterparties and transactions, we do so in a professional manner. All Catella Group entities must have routines in place for identifying, documenting and reporting suspected activities of money laundering and/or terrorist financing. We conduct adequate KYCs as well as CDDs to ensure the legitimacy of the above-mentioned. The routines of each entity shall be proportionate and risk-based as well as taking into account applicable laws and regulations.

Where laws and regulations do not require stricter measures, each entity within the Catella Group shall apply the below steps as their risk assessment.

A. Risk assessment

Local management shall regularly, at least annually, conduct a risk assessment to determine the risk profile of the entity. The risk assessment shall be properly documented. The outcome of the risk assessment shall be reflected in the actions or mitigation taken.

B. Initial confirmations

The following must be confirmed before entering a business relationship/engaging in a transaction:

The counterparty is, to the best of your knowledge, **not**:

- ☐ listed on an applicable sanctions list[2]; or
- ☐ involved in illegal activities.

The transaction does, to the best of your knowledge, **not**:

- ☐ involve unconnected parties;
- ☐ unusual payment methods (such as crypto currencies or cash); or
- ☐ unusual terms and conditions.

C. KYC and CDD

Based on the outcome of A and B above, entities shall perform a general KYC and CDD in relation to current and potential counterparties and transactions.

[1] Such as official sanctions lists by the European Commission, the United Nations and the Office of Foreign Assets Control.
[2] Such as official sanctions lists by the European Commission, the United Nations and the Office of Foreign Assets Control.

Make a general risk assessment of the counterparty/transaction to determine whether further investigation or actions are required. You may use Appendix 1 as a basis for your assessment.

If no red flags arise, document the risk assessment, and proceed.

If red flags arise, consult your local manager, and ask the concerned party for a certificate of incorporation and an ownership structure chart evidencing ownership up to the Ultimate Beneficial Owner.

Furthermore, review the documentation and assess whether further investigation or actions are required. If the documentation is satisfactory and does not give rise to further questions, document the risk assessment, and proceed. If there are red flags, please document the risk assessment and follow the steps under D (Monitoring and reporting) below.

D. Monitoring and reporting

If you suspect that a transaction is being used for money laundering or terrorist financing, follow the below steps.

- **Do not inform** the suspected party, or any third party, of your suspicions,
- **Consult** local instructions and act accordingly. If no such instructions exist, immediately report your suspicions to your local manager. The local manager shall thereafter report to the Catella Group CFO.

The above does not require that you have evidence that money laundering or terrorist financing has in fact taken place or that the funds originate from criminal activity. It is enough that you have reasonable grounds for your suspicions.

Contact person(s):

Head of Group Legal Group CFO

Revisions

DATE:	VERSION, CHANGES MADE AND NAME OF PERSON WHO MADE THEM
2022-05-05	Version 1.0, Created policy, Mattias Brodin, Group CFO, Mattias.Brodin@catella.se
2023-05-10	Version 1.2, New policy template, Michel Fischier, acting CFO and Head of IR and Group Communications
2024-05-22	Version 1.2, no updates, Johanna Bjärnemyr, Head of Group Legal

Appendix 1 – Risk assessment

The below may serve as a basis for determining whether a counterparty or transaction is to be deemed illegitimate. The below factors indicate, but are not equal to, increased risk.

Red flags (indicating increased risk)

- The party or representative is domiciled in a high-risk third country (as determined by the European Commission), such as North Korea, Iran, Cayman Islands and Panama.
- The party or representative is domiciled in a jurisdiction under increased monitoring (greylist) or subject to a call for action (blacklist) by the Financial Action Task Force (FATF), such as the United Arab Emirates and Turkey.
- The party or representative is domiciled in a country with a high corruption index or in a country where the index has drastically increased, as in the Transparency International's Corruption Perception Index (CPI).
- The party's ultimate beneficial owner (UBO) is a Politically Exposed Person (PEP) or is a family member or known employee of such a person.
- The party or representative presents identification documents that are obsolete or questionable.
- The party or representative is unable to present any documents that identify the company and the representative.
- The party is unwilling to have personal contact with you and wishes to conduct the business relationship in another way, for example, through intermediaries.
- The party or representative discontinues the business relationship after being asked to submit identity documents.
- The party wishes to transfer crypto currencies or cash.
- The party wishes to send money in a way that cannot be explained or tracked based on what is known about the party's financial position.
- The party wishes to send money to recipients to whom the party has no natural connection or to many different recipients.