1 INTRODUCTION

1.1 Accolade Holding, a.s. and any of its subsidiaries ("**Accolade**" or the "**Group**") are committed to conducting their business in full compliance with all applicable laws and regulations, including those relating to anti-money laundering ("**AML**"), counter-terrorist financing ("**CTF**"), and sanctions and export controls. This Policy reflects our unwavering commitment to ethical business practices and the promotion of a culture that does not tolerate money laundering, terrorist financing, or sanctions violations under any circumstances.

1.2 This Policy should be read in conjunction with applicable local internal AML/CTF and sanctions rules containing the detailed requirements relevant to each jurisdiction. Defined terms have the meanings assigned to them in the Definitions section of this Policy.

2 SCOPE AND PURPOSE

2.1 This Policy applies to, and shall be observed by, all companies within the Group, their employees and other natural persons performing work or similar activities for the Group, and their other Representatives. In addition, the Group is committed to communicating this Policy to all Business Partners and Representatives and ensuring that all of its dealings with any Business Partner or Representative comply with this Policy and with the applicable Sanctions.

2.2 The prior written approval of the Board of Directors of Accolade Holding is required for any deviation from this Policy, provided that such deviation would not breach any applicable laws.

2.3 The AML, CTF, and Sanctions policies and procedures of Accolade are designed to:

Establish a Zero-Tolerance Policy: Clearly affirm Accolade's unwavering stance against money laundering, terrorist financing, and sanctions violations.

Ensure Global Application: Ensure that all Representatives, regardless of their location, adhere to these standards.

Define Obligations: Offer clarity on what constitutes money laundering, terrorist financing, and sanctions non-compliance, including examples and warning signs.

Identify and Mitigate Risk Areas: Provide comprehensive guidance on areas of potential risk within the real estate investment sector.

Set Record Keeping Requirements: Detail the necessary documentation and record-keeping practices to ensure transparency and accountability.

Assign Responsibility and Oversight: Establish clear roles and responsibilities for the implementation, maintenance, and monitoring of AML/CTF compliance.

3 DEFINITIONS

3.1 Unless expressly stated otherwise herein or unless the context requires otherwise, the capitalised terms used in this Policy shall have the following meanings:

"Accolade Holding" means the company Accolade Holding, a.s.

"AML" means anti-money laundering.

"AMLD" means Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended.

"Business Partner" means any existing or prospective business partner of Accolade, including tenants, purchasers, suppliers, lenders, and joint venture collaborators.

"CDD" means customer due diligence.

"CTF" means counter-terrorist financing.

"Group" means Accolade Holding and its subsidiaries.

"KYC" means the "know your customer" principle.

"PEP" means any politically exposed person, i.e., any natural person who is or who during the preceding period prescribed by applicable law ceased to be entrusted with a prominent public function, such as a head of state, head of government, minister or deputy or assistant minister, member of parliament or of a similar legislative body, member of the governing body of a political party, member of a supreme court, constitutional court, or other high-level judicial body, ambassador, chargé d'affaires, or high-ranking officer in the armed forces, member of the administrative, management, or supervisory body of a state-owned enterprise, or director, deputy director, or member of the board or equivalent function of an international organisation.

"Policy" means this Group Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy.

"Representative" means any agent, consultant, contractor, sub-contractor, employee, and anyone else who works on behalf of the Group.

"Sanctions" means any measures adopted by international organisations (including the United Nations or the European Union) or individual states and their respective public authorities (including the United States of America, the United Kingdom, or Switzerland) that regulate the import and export of goods, services, software, and technology, as well as other economic and trade restrictions or prohibitions, export controls, embargoes, and international boycotts of any type.

"UBO" means the ultimate beneficial owner, i.e., any natural person who ultimately owns or controls a Business Partner, Representative, or other entity, or on whose behalf a transaction or activity is being conducted, as determined in accordance with applicable law and the AMLD.

4 MANAGEMENT RESPONSIBILITIES

4.1 The overall responsibility for compliance with and enforcement of this Policy rests with the Board of Directors of Accolade Holding, which acts through the Group Legal Counsel. The Group Legal Counsel reports to the Board of Directors of Accolade Holding on a regular basis.

4.2 The specific role of the person designated to carry out AML/CTF and Sanctions compliance duties in each jurisdiction is governed by the specific national directives or other rules implementing this Policy. Each Group entity is required to adopt and implement a local internal AML/CTF policy covering all required AML/CTF procedures and elements in accordance with the applicable national AML/CTF legislation.

4.3 The management board of each Group entity is responsible for compliance with the applicable

national AML/CTF legislation and provides the tone from the top regarding the importance of AML/CTF topics. Local AML policies, procedures, and risk assessments are approved once at the level of Accolade Holding and apply to all Group entities in the relevant jurisdiction that are obliged persons under the applicable national AML/CTF legislation.

5 UNDERSTANDING MONEY LAUNDERING AND TERRORIST FINANCING

5.1 Overview

Money laundering and terrorist financing are serious criminal activities that threaten the integrity of the financial system and society as a whole. They can manifest in various forms and may involve complex, multi-layered transactions designed to conceal the origin of criminal proceeds or to fund illegal activities.

Accolade operates in multiple jurisdictions, each with its own set of laws and regulations that prohibit money laundering, terrorist financing, and related illicit activities.

Non-compliance with AML and CTF laws can lead to severe consequences for the Group, any Representatives, and any other involved individuals, including substantial fines, imprisonment, and significant reputational harm.

5.2 Money Laundering Defined

Money laundering is defined broadly and includes concealing, converting, transferring, acquiring, participating in, or using the proceeds of any crime. Proceeds of crime include any benefit which flows from any criminal offence, no matter how minor or insignificant.

5.3 Terrorist Financing Defined

Terrorist financing may be defined as providing money or other property where such money or other property is likely to be used for the purposes of terrorism or for the commission of acts of terrorism. Such money or other property does not necessarily need to come from illegal proceeds or activities. For the purposes of this Policy, terrorist financing also includes the financing of the proliferation of weapons of mass destruction.

5.4 Zero Tolerance Policy

Representatives are unequivocally prohibited from engaging in, facilitating, or ignoring any activity that may constitute money laundering or terrorist financing. The Group maintains a zero-tolerance approach and will take consistent and effective action against any individual found to have participated in or enabled such activities.

6 CORE AML AND CTF PRINCIPLES

6.1 In respect of AML and CTF, the Group never:

(a) tolerates money laundering or terrorist financing; and

(b) ignores or hides evidence or suspicions of money laundering or terrorist financing.

6.2 On the other hand, the Group:

(a) vigilantly looks out for any suspicious activity suggesting that money laundering or

terrorist financing is occurring or connected to any transaction;

(b) assesses money laundering and terrorist financing risks in its business and is committed to continually improving systems and processes to reduce money laundering and terrorist financing risk exposure;

(c) understands the AML and CTF obligations and ensures that its Business Partners, Representatives, and their UBOs are identified in accordance with CDD and KYC standards and applicable laws; and

(d) takes any breaches of AML and CTF regulations and policies seriously.

6.3 The Group has adopted an effective internal control system allowing for the prompt identification and mitigation of money laundering and terrorist financing risks, which is adequate to the type and scale of its business.

7 CUSTOMER DUE DILIGENCE AND KNOW YOUR CUSTOMER

7.1 Overview

The Group entities are required to conduct customer due diligence procedures with the aim of assessing risks related to a particular Business Partner or transaction and to apply appropriate measures to mitigate those risks. CDD procedures shall be conducted before entering into a business relationship and before the execution of the first transaction at the latest. The scope of CDD and KYC for particular categories of Business Partners (for example suppliers, lenders or tenants with low rent) is determined by the local internal AML/CTF rules, in line with the applicable national legislation and the risk-based approach.

In line with the AMLD and based on the performed AML/CTF risk assessment while reflecting the risk-based approach, the Group applies three different levels of CDD and KYC, provided this is permitted by the relevant national legislation:

(a) Simplified CDD

The simplified level is applied where the Business Partner or Representative poses a low risk of money laundering or terrorist financing (e.g., companies listed on any European regulated market).

(b) Standard CDD

The standard level is applied to Business Partners and Representatives that do not fall in either the low or high-risk category.

(c) Enhanced CDD

The enhanced level is applied to Business Partners and Representatives that fall in the high-risk category, which includes the following:

(i) if they are PEPs, or if they are a corporate entity or structure owned or controlled by a PEP;

(ii) those established (in case of legal entities) or resident (in case of individuals) in jurisdictions designated by the European Commission in the delegated regulation pursuant to the AMLD, or those established in any other territory

under Sanctions;

(iii) those involved in a transaction that is very complex or where there is an unusual pattern of transactions with no apparent economic or legal purpose; and

(iv) any other case which by its nature can present a high risk of money laundering or terrorist financing.

Where enhanced CDD is applied, the Group shall perform additional procedures to those defined under standard CDD, such as obtaining additional information on the UBO or the source of funds and wealth, verifying such information from multiple reliable sources, or conducting more frequent monitoring of the business relationship.

7.2 **CDD Procedures – Minimum Requirements**

CDD procedures shall always include at least the following elements:

(a) Identification of the Business Partner and verification of their identity.

(b) In the case of a legal entity, identification of the Business Partner's representatives, members of the managing body, and UBOs, and determination of the ownership and management structure of the Business Partner.

(c) Obtaining information on the purpose and intended nature of the business relationship or transaction.

(d) Obtaining information on the source of funds and, in the case of a transaction or business relationship related to a PEP, also the source of wealth.

(e) Regular ongoing monitoring of the business relationship.

8 IDENTIFICATION AND VERIFICATION

8.1 The Group has implemented identification and verification procedures within the applied CDD measures in accordance with local laws, which may comprise:

(a) identifying the Business Partners and Representatives (and persons purporting to act on their behalf) and verifying their identity on the basis of documents, data, or information obtained from a reliable and independent source, including, where available, electronic identification means;

(b) identifying the UBO and taking reasonable measures to verify that person's identity, including understanding the ownership and control structure of the Business Partner or Representative, and, where no UBO can be identified, verifying the identity of the natural person who holds the position of senior managing official;

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship to ensure consistency with the Group's knowledge of the Business Partner or Representative, the business, and the risk profile; and

(e) obtaining information on the source of funds of the Business Partner or Representative.

8.2 Where the Group is unable to carry out the required CDD measures, it shall not establish the business relationship, shall not carry out the transaction, shall terminate the existing business relationship where applicable, and shall consider whether the circumstances give rise to an obligation to file a suspicious transaction report with the relevant competent authority.

9 UNACCEPTABLE BUSINESS PARTNERS

9.1 The Group entities shall not execute a transaction or establish a business relationship if any of the following conditions apply:

(a) the Business Partner refuses to undergo identification;

(b) a person acting on behalf of the Business Partner fails to provide evidence of their authority to act, unless such authority is evident from a public register;

(c) the Business Partner fails to provide the required cooperation during customer due diligence;

(d) customer due diligence or identification cannot be performed for any other reason;

(e) the Group has doubts about the accuracy of information provided by the Business Partner or the authenticity of submitted documents;

(f) the Business Partner is a PEP, or the UBO of a legal entity is a PEP, and the source of funds or other assets related to the business relationship is unknown; or

(g) the Business Partner is subject to Sanctions.

9.2 If any of the above-mentioned conditions arise during an already established business relationship, the relevant Group entity shall terminate the business relationship without undue delay.

10 SANCTIONS

10.1 Overview

The purpose of Sanctions is to change the behaviour of the targeted countries, regions, organisations, or individuals. Sanctions may be based on concerns relating to national or international security, terrorism, money laundering, human rights violations, development of weapons of mass destruction, or other relevant reasons.

10.2 Sanctions may arise from:

(a) Decisions of the United Nations Security Council taken pursuant to Article 41 of the Charter of the United Nations;

(b) Decisions of the Office of Foreign Assets Control of the US Department of the Treasury;

(c) Common positions, joint actions, or other measures adopted pursuant to the Treaty on European Union on the common foreign and security policy;

(d) Directly applicable regulations of the European Union implementing a common position or joint action; or

(e) Other decisions by a government or other authority to include a person on a national sanctions list pursuant to a relevant act on sanctions or similar measure.

10.3 **What Sanctions May Target**

Sanctions may target countries or regions, organisations or individuals, specific goods and services, or specific assets. In respect of countries or regions subject to Sanctions, the Group or its Representatives may be prohibited from travelling to, making investments in, or conducting business in such territories. In respect of organisations or individuals subject to Sanctions, the Group may be restricted from doing business with such parties and may face financial restrictions, including asset freezes and limitations on financial transactions.

10.4 **Sanctions Screening**

The Group entities shall perform sanctions screening before entering into a business relationship and on an ongoing basis throughout its duration. If a Business Partner or any other relevant person is identified on a sanctions list, the business relationship or transaction may only continue in strict compliance with the applicable sanctions legislation under which the sanction was imposed.

11 COMPLIANCE WITH SANCTIONS

11.1 The Group shall always operate its business in compliance with applicable laws, which also means compliance with the Sanctions. A failure to comply with the Sanctions may constitute a crime and the consequences for non-compliance could include fines for the Representatives or for the Group, or imprisonment for the Representatives. A failure to comply with the Sanctions further poses to the Group a risk of reputational damage, potentially resulting in reduced trust from the communities, Representatives, Business Partners, as well as other stakeholders.

11.2 Compliance with the Sanctions means, in particular, that the Group does not:

(a) in countries or territories that are subject to Sanctions, conduct business activities as a consequence of which the Sanctions would be breached or circumvented;

(b) provide services to individuals or organisations, or in countries or territories, that are subject to Sanctions, if the Sanctions would be breached or circumvented by such provision of services;

(c) export and import goods from and to, respectively, countries or territories that are subject to Sanctions without the required governmental approvals or licences; or

(d) engage, directly or indirectly, in any other activities that would breach or circumvent the Sanctions.

11.3 Compliance with the Sanctions further means that the Group:

(a) on a regular basis, assesses and analyses which Sanctions apply to it, monitors risks related to the Sanctions, and takes into account the potential consequences of its business activities from the Sanctions perspective;

(b) screens the Business Partners and Representatives, as well as potential business transactions, with respect to the Sanctions in line with the AMLD and based on the performed AML/CTF risk assessment; and

(c) has implemented identification and verification procedures within the applied CDD measures, including verifying identity, identifying entities under the Sanctions, and reporting of suspicions or confirmed breaches of this Policy.

11.4 Where permitted by the content of the respective Sanction and applicable local legislation, exceptions to the prohibition or restriction may be granted in the following cases:

(a) the payment of wages, wage compensation, severance pay, and other payments arising from an employment or similar employment relationship;

(b) compensation for damage caused by activities unrelated to the performance of the Sanctions;

(c) payments to an entity or person subject to Sanctions, owed on the basis of obligations incurred before Sanctions were imposed, provided that such payments are made to an account in a member state of the European Union in which all funds deposited become assets subject to Sanctions; or

(d) any other exception permitted under applicable law, subject to a request for such an exemption being submitted to the relevant local supervisory authority in accordance with the local legislation.

12 REPORTING OF SUSPICIONS

12.1 The Group has implemented a reporting process to be followed by all Representatives in all situations where they have knowledge, suspicion, or reasonable grounds for suspicion of money laundering or terrorist financing.

12.2 Any knowledge or suspicion of money laundering or terrorist financing must be first reported to the Legal Department (or other person specified in the relevant national internal AML/CTF rules) or via Accolade's whistleblowing procedure, without undue delay.

12.3 The Legal Department (or other person specified in the relevant national internal AML/CTF rules) will then assess the disclosure and will determine, having investigated the particular facts and circumstances surrounding the reported knowledge or suspicion, any follow-up reporting action to the competent authorities in accordance with the requirements of the respective jurisdiction.

12.4 The Group has implemented appropriate measures to be taken in case a transaction is suspected to be related to proceeds of criminal activity or terrorist financing, including measures to prevent the dissipation of proceeds of crime, measures to refrain from execution or to postpone the transaction, and the provision of documents and information to competent authorities on request.

12.5 Representatives are subject to confidentiality obligations and must avoid tipping-off, i.e., disclosing to a Business Partner or third party that a suspicious transaction report has been or may be submitted.

13 GROUP-WIDE INFORMATION SHARING

13.1 The companies within the Group and their Representatives use best endeavours to share information about Business Partners and Representatives among the Group companies and their Representatives, where technically and legally possible, to ensure the Group's compliance with applicable AML, CTF, and Sanctions laws.

14 RECORD KEEPING AND DISCREPANCY REPORTING

14.1 Record Keeping

The Group entities shall keep records of documents and information related to AML/CTF procedures for at least 5 years (or for such longer period as required by local legislation) after the performance of the last transaction or the termination of a business relationship with a Business Partner.

The Group ensures that risk assessment and CDD data (including records of the actions taken and records of any difficulties encountered during the CDD process) are securely stored to comply with obligations on records retention and data protection.

14.2 Discrepancy Reporting

Any knowledge of a discrepancy between the beneficial ownership information available in central registers and the beneficial ownership information available to Representatives must be reported to the Legal Department, which ensures that appropriate actions are taken in accordance with the requirements of the respective jurisdiction.

15 EMPLOYEE TRAINING

15.1 The Group provides AML and CTF training to all Representatives who are, due to the nature of their role, likely to encounter money laundering or terrorist financing in their day-to-day conduct. Training is conducted at least once every twelve calendar months and upon each material change to this Policy.

15.2 Training includes information on:

(a) typologies and indicators of suspicious transactions;

(b) requirements for identification and customer due diligence;

(c) procedures for detecting customer risk factors and suspicious transactions;

(d) confidentiality obligations and the prohibition on tipping-off; and

(e) the applicable whistleblowing and reporting procedures.

15.3 Each Group entity shall continuously amend and update the training courses to reflect developments in applicable laws and changes to this Policy.

16 INFORMATION DUTY

16.1 Each Group entity shall designate a responsible person for communication with the local state authority in connection with AML/CTF matters. This designation shall be made in accordance with the requirements of the applicable national AML/CTF legislation.

17 FINAL PROVISIONS

17.1 Accolade's COO and Group Legal Counsel shall regularly review and update this Policy at least once every two years, taking into account the ongoing development of Accolade's activities and changes in legislation.

17.2 Any violation of this Policy must be immediately reported to the Group Legal Counsel or via the Group's whistleblowing procedure laid out in the Group's Whistleblowing Policy.

17.3 The Group will take seriously and investigate all reports of potential violations of this Policy to ensure that this Policy is enforced.

17.4 Violation of this Policy by any Representative may constitute a breach of the terms and conditions of employment or other relationship of such Representative with the Group, and thus such Representative may be subject to disciplinary action, which, depending on the nature of the violation, may range from a warning or reprimand to termination of employment or other relationship and, in appropriate cases, civil legal action or referral for regulatory or criminal prosecution.

17.5 This Policy replaces all previous policies and other internal regulations of the Group dealing with anti-money laundering, counter-terrorist financing and sanctions.