SYSTEM OF INTERNAL POLICIES AND RULES OF PROCEDURES TO PREVENT MONEY LAUNDERING & COUNTER-TERRORIST FINANCING PROCEDURES& ANTI-BRIBERY POLICY

Overview:

Name of the entity:	**Cloudpeak Systems s.r.o.**
Registration number:	**217 21 769**
Legal address:	**Na strži 1702/65, Nusle, 140 00 Praha 4, Prague, Czech Republic**
Type of authorisation:	**Virtual Asset Service Provider**
Website:	**Empresex.io**

Approved:	**Artur Tiunov**
Date of approval:	**17.03.2026**
Distribution:	**Internal**

TABLE OF CONTENTS

1. Cloudpeak Systems s.r.o. is committed to upholding the highest standards in AML and CTF practices.

The Cloudpeak Systems s.r.o. (“Empresex”) Anti-Money Laundering and Counter-Terrorist Financing Manual (the "Manual") has been created to ensure that Cloudpeak Systems s.r.o., its management, and employees fully comply with the requirements and obligations set forth by the legislation, regulations, and industry guidelines of the Czech Republic aimed at combating money laundering and the financing of terrorist organizations.

The Cloudpeak Systems s.r.o. Manual establishes the core principles to be applied within the company, including:

- ✓ **Appointing a Money Laundering Reporting Officer (“MLRO”) with appropriate authority to oversee compliance with all applicable laws, regulations, and industry guidelines.**
- ✓ **Implementing effective systems and controls based on a risk assessment to prevent money laundering and terrorist financing.**
- ✓ **Conducting business in accordance with high ethical standards with clients engaged in lawful activities.**
- ✓ **Developing and implementing customer verification procedures, including identification, verification, and “Know Your Customer” processes, as well as enhanced due diligence for high-risk customers. Cloudpeak Systems s.r.o. will ensure customer identities are verified before their acceptance.**
- ✓ **Establishing and maintaining procedures to monitor customer accounts and activities based on risk considerations.**
- ✓ **Assessing and documenting risks, taking into account potential threats associated with customers and communication channels, considering the company’s scale.**
- ✓ **Providing ongoing training for employees to ensure they are familiar with the Manual’s requirements and may fulfill their legal obligations regarding anti-money laundering and counter-terrorist financing. Regularly updating employees on legislative changes and requirements to combat money laundering.**
- ✓ **Complying with record-keeping requirements and retaining records for at least five years.**
- ✓ **Ensuring employees promptly report any suspicious activities to the MLRO, and to the relevant authorities as necessary.**
- ✓ **Providing regular reports to senior management regarding compliance with the Manual’s requirements.**
- ✓ **Regularly reviewing and updating all procedures outlined in the Manual to ensure strict adherence and alignment with changes in legislation and best industry practices.**

The Cloudpeak Systems s.r.o. Anti-Money Laundering and Counter-Terrorist Financing Manual establishes clear requirements and procedures to ensure full compliance with the legislation of the Czech Republic. This includes monitoring customer transactions, verifying their legitimacy, as well as training employees and ensuring timely reporting of suspicious activities. Through the continuous improvement of processes and procedures, the company ensures a high level of protection against risks related to money laundering and terrorist financing.

2. Introduction

Cloudpeak Systems s.r.o. recognises that the legal and regulatory framework for AML/CFT/CPF is continuously evolving. In particular, the Financial Action Task Force (FATF), the European Union and the Czech authorities periodically update their lists of high-risk jurisdictions, sanctions regimes and supervisory expectations. Therefore:
- this Manual must be reviewed at least once per year by the MLRO and Compliance;
- FATF public statements on "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring" must be checked after each FATF Plenary (typically February, June and October); and
- the internal country-risk matrix (Annex 1) and the list of jurisdictions with strategic deficiencies (Annex 2) must be updated whenever FATF or the European Commission issue new lists. Where there is any discrepancy between this Manual and applicable Czech or EU law, or FATF standards, the stricter requirement shall apply.
Cloudpeak Systems s.r.o. is committed to conducting its business in full compliance with the highest legal and ethical standards. To achieve this, the company has established stringent requirements in accordance with Czech and European regulations aimed at detecting and preventing money laundering and terrorist financing. This manual is designed to serve as a comprehensive guide to understanding the legal frameworks put in place to prevent financial institutions from being used as intermediaries for concealing or transferring funds derived from criminal activities. It also ensures that Cloudpeak Systems s.r.o., its management, and all employees strictly adhere to the requirements of Czech legislation, regulations, and industry guidance designed to combat money laundering and terrorist financing.

All Cloudpeak Systems s.r.o. employees are expressly prohibited from engaging in or facilitating money laundering schemes or providing advice or assistance to clients on how to circumvent anti-money laundering regulations. All staff are required to:

- ✓ **Maintain vigilance regarding transactions or customer activities reasonably suspected of involving money laundering or other criminal activities.**
- ✓ **Fully cooperate with competent law enforcement authorities in accordance with applicable law.**
- ✓ **Immediately report any knowledge or suspicions of money laundering to the appointed Money Laundering Reporting Officer (MLRO) of the company.**

This Compliance Manual is periodically reviewed by Cloudpeak Systems s.r.o. and its legal advisors, and you will be notified of any revisions to its terms. The Manual will be reviewed at least annually to ensure full compliance with newly enacted regulations, provide guidance on new products, systems, or tools introduced by Cloudpeak Systems s.r.o., and incorporate the latest developments and best practices in the field of Anti-Money Laundering and Counter-Terrorist Financing. Please ensure that you are familiar with the current terms of this Compliance Manual.

2.1 Obliged person

(1) Under the Anti-Money Laundering (AML) policy, the company is considered an obliged person when providing virtual asset services in accordance with § 2, paragraph 1, letter l) of the AML Act.

2.2 Object of adjustment

The company provides services that could be used by clients to conceal the illegal origin of financial resources or to support terrorist organizations. To prevent such illegal activities, Czech legislation imposes several obligations on the company. To fulfill these obligations, the company has developed a system of internal policies and procedures to combat money laundering and terrorist financing (AML policies), which adapt the legal requirements to the specific services provided. These include important elements such as a structure of internal policies and procedures aimed at preventing money laundering and terrorist financing, as well as a risk assessment regarding potential money laundering attempts.

Money laundering, or the legalization of illegal income, involves using the company's services to conceal the true origin of assets or make it difficult to trace them. This process is often combined

with financing terrorism, so the fight against both issues is carried out simultaneously using similar methods. Adhering to these standards is mandatory not only within the Czech Republic but also in an international context, as these crimes have a global dimension.

Furthermore, the company shall continuously verify whether its clients are subject to international sanctions and comply with other requirements set forth in this document. Failure to follow the procedures outlined in this manual may result in legal violations, leading to serious legal consequences for the company.

2.3 Personnel assignments

This document outlines the obligations that apply not only to responsible individuals but also to any employees or participants who may deal with suspicious transactions or perform tasks related to such activities. It is important to note that these requirements apply to everyone, regardless of whether they are official employees or working on another basis, including unpaid work.

If the company is unable to ensure full compliance with the requirements set out in this document and the money laundering risk assessment, it shall temporarily limit or suspend the provision of virtual asset services until the deficiencies are addressed. This is especially relevant in cases where, for example, the company experiences a sudden loss of staff, and they are replaced by less experienced workers. In such cases, it is essential that the anti-money laundering and counter-terrorism financing system is always staffed with a sufficient number of qualified specialists. The management of the company is responsible for ensuring the fulfillment of these obligations.

2.4 Binding for third parties

These procedures are also binding on individuals who provide virtual asset services or establish business relationships on behalf of or for the account of the company, including authorized representatives. The statutory body shall ensure that the representative adopts these procedures as their own or fully integrates them into their internal procedures and adheres to them. The statutory body shall also ensure that the obligations set out in this document are monitored in the representative's area of operation.

3. List Of Abbreviations

Abbreviation	Full Form	Description
AML	Anti-Money Laundering	Policies and practices aimed at preventing money laundering.
CDD	Customer Due Diligence	The process of assessing customers' risks to ensure their identity and activities are legitimate.

CNB	**Czech National Bank**	**The central bank of the Czech Republic overseeing financial stability and regulations.**
EDD	**Enhanced Customer Due Diligence**	**A more detailed form of due diligence applied to higher-risk customers.**
EEA	**European Economic Area**	**A group of European countries that ensures the free movement of goods, services, and people.**
EU	**European Union**	**A political and economic union of European countries.**
FATF	**Financial Action Task Force**	**An international organization that sets global standards for preventing money laundering and terrorist financing.**
FAO	**Financial Analytical Office**	**The government body responsible for analyzing financial transactions to detect suspicious activity.**
ML-FT	**Money Laundering and Terrorist Financing**	**The process of concealing criminal financial activities and financing terrorism.**
SAR	**Suspicious Activity Report**	**A report filed when a transaction or activity is deemed suspicious and potentially illegal.**

SDD	**Simplified Customer Due Diligence**	**A less stringent version of customer due diligence, applied to low-risk customers.**
PEP	**Politically Exposed Person**	**An individual who holds a prominent public position or has close ties to one.**
MLRO	**Money Laundering Reporting Officer**	**An appointed officer responsible for ensuring compliance with anti-money laundering regulations.**

4. **General Terms**

Legislative Acts Regulating Anti-Money Laundering and Countering the Financing of Terrorism

Anti-Money Laundering Act (AML Act)

According to the current legislation, the Anti-Money Laundering Act (Act No. 253/2008 Coll.) is the primary regulatory framework addressing measures against the legalization of proceeds from criminal activities and terrorist financing. The Act defines the terms and processes related to combating these crimes and establishes the necessary procedures for financial institutions and other entities that might be involved in such activities.

Sanctions Act

Another important act in this field is the Sanctions Act (Act No. 69/2006 Coll.), which regulates the implementation of international sanctions aimed at combating terrorist financing and other illegal financial activities. The sanctions imposed under this law may include freezing assets, restricting trade operations, and other measures designed to prevent unlawful activities.

Key Definitions:

Money Laundering

Money laundering refers to the process of concealing the illicit origin of financial assets acquired through criminal activities in order to create the appearance of lawfully obtained financial benefits. The key actions in money laundering include:

- ✓ **Converting or transferring property knowing it is the proceeds of crime, with the intent to conceal its origin.**
- ✓ **Concealing or disguising the true nature, source, location, or movement of property, knowing it is the proceeds of crime.**

- ✓ **Acquiring, possessing, using, or disposing of property knowing it is the proceeds of crime.**
- ✓ **Conspiring or cooperating with others to carry out any of the above actions.**

Terrorist Financing

Terrorist financing refers to the collection or provision of funds or other property, knowing that it will be used for acts of terrorism, terrorist attacks, participation in a terrorist group, or supporting terrorism.

This includes:

- ✓ **Financing acts of terror or individuals/groups preparing for such actions.**
- ✓ **Providing a reward or compensation to perpetrators of terrorist crimes or supporting individuals involved in such activities.**
- ✓ **Financing the proliferation of weapons of mass destruction, i.e., funding for the spread of such weapons in violation of international law.**

Key Aspects in Combating Money Laundering and Terrorist Financing:

Customer Identification

According to AML requirements, a customer refers to any natural or legal person with whom the company engages in business or has an intention to engage in business, including those expressing interest in entering into a transaction or business relationship. This also includes individuals who use the company's virtual assets or have the authority to act on behalf of another customer.

Virtual Assets

A virtual asset under the AML Act is any electronic unit that may be used for making payments, exchanges, or investments, and which is not classified as a monetary instrument, security, or investment instrument under payment laws. Virtual assets may include cryptocurrencies, tokens, and other digital assets used in transactions.

Key Risk Assessment Criteria:

Risk-Based Approach

When conducting financial transactions, it is essential to assess the country and geographic risk. Cloudpeak Systems s.r.o. in particular considers the FATF "High-Risk Jurisdictions subject to a Call for Action" (the "black list"), the FATF "Jurisdictions under Increased Monitoring" (the "grey list"), the list of high-risk third countries identified by the European Commission, as well as any other jurisdictions that are subject to UN, EU, Czech or other relevant national sanctions. Customers with any nexus to FATF black-list jurisdictions are normally not accepted, and any existing relationships, if any, are subject to the most stringent restrictions and monitoring. Customers with a nexus to FATF grey-list or EU high-risk jurisdictions are treated as high-risk in the internal methodology and are always subject to Enhanced Due Diligence (EDD) and more frequent ongoing monitoring.

Source of Funds and Wealth

In the customer verification process, it is important to identify not only the source of funds for a particular transaction but also the source of wealth—the assets accumulated by the customer over time, representing their overall financial standing. This helps detect potential risks associated with illicit wealth sources.

Procedures for Financial Institutions:

Know Your Customer (KYC)
Financial institutions are required to conduct proper checks on their customers using identification documents that contain basic personal data, such as name, surname, date of birth, and a photograph. This is crucial for verifying the identity of the customer and preventing financial crimes like money laundering or terrorist financing.

Enhanced Due Diligence
In cases where high risks are detected, such as clients from high-risk countries or suspicious transactions, financial institutions shall apply Enhanced Due Diligence (EDD). This involves more thorough checks on the source of wealth, the client's history, and the nature of their operations.

The implementation of proper procedures for combating money laundering and terrorist financing is crucial to ensure the stability of the financial system and prevent criminal activities in international financial flows. The legislative acts and standards regulating these processes provide effective measures for fighting such crimes on a global scale.

This text now has a new structure and includes additional explanations about the importance of fighting money laundering and terrorist financing, as well as the role of various laws and procedures in this field.

5. **Money Laundering**

Money laundering refers to the process of concealing the origins of illegally obtained money, typically through transfers or transactions that make the funds appear legitimate. The goal is to make illicitly acquired money seem as if it was earned legally, often through complex financial transactions or by integrating the money into the legitimate economy. This is a criminal activity and is illegal in most countries.

Cloudpeak Systems s.r.o. is obligated to ensure the fulfillment of legal requirements outlined in these regulations within all its subsidiaries, branches, affiliates, and controlled organizations, both in the Czech Republic and abroad. If local regulations impose stricter requirements than those outlined in this Manual, the stricter standard shall be applied.

The responsibility for adhering to the provisions of this Manual lies with all employees who directly or indirectly interact with customers, conduct transactions, prepare necessary documentation, or have access to systems and tools that could reveal or prevent money laundering or terrorism financing activities. This applies not only to full-time employees but also to temporary, part-time employees, interns, and contractors who engage in these processes. The Management Board is ultimately responsible for approving and ensuring compliance with this Manual and for cultivating a culture of compliance within the company.

This Manual applies to all aspects of Cloudpeak Systems s.r.o.'s business and extends to any organizations or individuals with whom the company conducts business.

The procedures outlined in the Manual are designed to maintain high standards in the fight against fraud and corruption and to prevent criminal activities, including money laundering, from infiltrating the organization.

Cloudpeak Systems s.r.o. takes necessary steps to identify and address potential areas exposed to money laundering risks, establishing suitable controls to minimize these risks.

Cloudpeak Systems s.r.o. is committed to ensuring that the legal obligations set forth in these regulations are met across all its subsidiaries, branches, affiliates, and controlled entities, both within the Czech Republic and internationally. In cases where local regulations are stricter than those outlined in this Manual, the more stringent standard will take precedence, ensuring compliance with all applicable legal frameworks.

Every employee who interacts with customers, manages transactions, prepares essential documentation, or handles systems and tools that could indicate or prevent money laundering or terrorism financing is responsible for adhering to the provisions in this Manual. This includes not only permanent staff but also temporary and part-time employees, interns, and contractors who may be involved in any processes linked to these activities. By understanding and following the provisions of this Manual, all personnel contribute to safeguarding the company from illicit activities.

The responsibility for upholding these standards ultimately lies with the Management Board, which ensures compliance with the Manual and fosters a culture of integrity, transparency, and legal adherence within the company. The Management Board plays a vital role in setting the tone for compliance and ethical conduct, supporting the team to stay informed and proactive in preventing financial crimes.

This Manual is applicable to all facets of Cloudpeak Systems s.r.o.'s operations and extends to any third-party organizations or individuals the company engages with in its business activities. All business relationships, both domestic and international, are covered by these procedures to ensure uniformity in the company's approach to risk management.

The procedures outlined aim not only to prevent money laundering but also to ensure that the company operates with the highest level of transparency, ethics, and accountability. By instituting strong controls, Cloudpeak Systems s.r.o. prevents the infiltration of criminal activities into its operations, safeguarding both the organization and its customers.

Cloudpeak Systems s.r.o. remains vigilant in identifying potential risks related to money laundering and terrorism financing, continuously assessing and strengthening its internal controls. The company is dedicated to adapting its procedures to ever-evolving regulatory landscapes, ensuring long-term compliance and the trust of its stakeholders.

5.1 Explanation of the Concept of "Money Laundering"

Money laundering is a serious issue for the global financial system and the economies of different countries. It is the process by which illegally obtained funds are converted into legitimate assets, allowing wrongdoers to hide their criminal origins. Given the high level of organization in this activity

and its impact on national and international financial institutions, understanding this process is crucial for ensuring transparency and combating financial crimes.
Money laundering is the process of converting financial resources obtained through criminal activities into assets that appear legitimate. This process allows criminals to conceal the true origin of the funds and ensure their further use without suspicion. Crimes related to money laundering include, for example, fraud, theft, drug trafficking, corruption, organized crime, and other criminal offenses that serve as the basis for this process. The laws of a country define the specific crimes that fall under money laundering.

The process of money laundering typically consists of several stages:

- ✓ **Placement — This is the first stage, where illicit money or other valuables are introduced into the system, often through banks or other financial institutions.**
- ✓ **Layering — In this stage, proceeds from criminal activities are masked through numerous financial transactions to make it harder to trace their origin.**
- ✓ **Integration — At this stage, the laundered money is reintroduced into the economy as legitimate, allowing it to be used without suspicion.**

The money laundering process is not always linear and may involve repeated overlapping stages. These manipulations help ensure anonymity and complicate the tracing of the source of funds, often with the goal of further financing other criminal activities or retaining the assets within the system. Money laundering is a key element in the fight against international organized crime and terrorism. It impacts the stability of financial markets and the economic security of states, necessitating enhanced monitoring and compliance with regulations in this area. To prevent money laundering, it is essential to improve the control systems, refining both legislation and practical measures in the banking and financial sectors.

5.2 Instances of Money Laundering

According to the legislation, money laundering involves several types of criminal activities that are prohibited by law. Below is a more detailed explanation of the primary and secondary offenses related to money laundering:

Primary Money Laundering Offenses:

- ✓ **Concealing, disguising, converting, transferring, or removing criminal property: This includes any actions aimed at concealing or changing the nature of property obtained through illegal means to make it appear legitimate. Such actions may involve converting the property (e.g., changing cash into other assets such as real estate or securities), transferring the property to another person or company to hide its illegal origin, or simply removing the property from circulation to maintain anonymity.**

- ✓ **Engaging in or becoming involved in an arrangement that the employee knows or suspects facilitates the acquisition, retention, use, or control of criminal property by, or on behalf of, another person: This offense involves participating in any arrangement that facilitates the retention or use of property obtained through criminal activity. It may include being involved in business processes that allow funds to be kept or moved to accounts controlled by another person involved in criminal activity.**
- ✓ **Criminal property: The law defines criminal property very broadly, encompassing various forms of assets, including physical property (real estate, vehicles, valuable items), financial instruments (checks, stocks, bonds, currency), or even digital assets such as cryptocurrencies. This property, obtained illegally or used to fund criminal activity, is the subject of anti-money laundering efforts.**

Secondary Offenses:

In addition to the primary offenses directly associated with money laundering, the legislation also defines several secondary offenses that may be part of the money laundering process. These include:

- ✓ **Failure to report suspicious activity: Employees or organizations with access to financial transactions are required to report any suspicious activities or transactions that could be part of a money laundering scheme. Failure to meet this obligation may lead to liability.**
- ✓ **Assisting in the creation or maintenance of false accounts or transactions: Individuals who assist in creating fake accounts, transactions, or links as part of a money laundering scheme may also be held accountable. This may include providing advice or services that facilitate hiding the origin of funds or manipulating documents used in these schemes.**

All these actions fall under criminal prosecution and are violations of laws aimed at combating money laundering and other financial crimes. They may lead to serious consequences for both individuals and organizations that allow such actions or fail to meet their responsibilities to prevent financial crimes.

5.3 Instances of Potential Exposure of Cloudpeak Systems s.r.o.

Allowing illicit funds to pass through the Cloudpeak Systems s.r.o. system.

Processing large transactions through the Cloudpeak Systems s.r.o. system without proper verification.

Converting illicit funds into "clean" money due to inadequate user verification and monitoring.

In accordance with Act No. 253/2008 Sb. of June 5, 2008, on Measures Against the Legalization of Proceeds from Criminal Activities and the Financing of Terrorism (AML/CTF Law), Cloudpeak Systems s.r.o. has implemented strict standards to comply with these regulations and is committed to combating money laundering, as outlined in this Compliance Manual.

The purpose of this manual is to help staff understand how to follow the applicable legal and regulatory requirements. In case of complex compliance queries, the company provides support through the Money Laundering Reporting Officer Hovsep Kocharyan.

Contact email for the MLRO at Cloudpeak Systems s.r.o. — mlro@empresex.io
Contact Phone for the MLRO at Cloudpeak Systems s.r.o. — +420607890147

If any employee suspects that a customer is engaging in illegal activity, they shall not proceed with the transaction without obtaining the necessary consent from the FAO and the MLRO, if required. The company's priority is ensuring that all operations are transparent and legally compliant.

5.4 Obligations for Reporting and Record Retention

Employees shall take necessary steps to maintain and preserve appropriate documentation, including accounting records, that are suitable to the scale, type, and complexity of each customer's business. Documentation related to customer identification and transactions shall be retained for use as evidence in any investigation involving money laundering (see Section 11 – "Record Keeping").

The maintained records are required to be such that:

- ✓ **The requirements of the AML/CTF legislation are fully met.**
- ✓ **Third parties may assess the effectiveness of Cloudpeak Systems s.r.o.'s compliance with anti-money laundering policies and procedures.**
- ✓ **Any transaction conducted on behalf of any customer may be reconstructed.**
- ✓ **Each customer may be properly identified and located.**
- ✓ **All suspicious transaction reports received internally and made externally may be identified.**
- ✓ **The company may satisfy any enquiries or court orders from the authorities concerning the disclosure of information.**

Failure to comply with the record-keeping requirements under the AML/CTF legislation may lead to financial penalties, and in serious cases, prosecution and imprisonment.

Cloudpeak Systems s.r.o. may retain records as original documents, photocopies of original documents, or in computerized or electronic form. This ensures that the business meets its obligations and may demonstrate compliance if requested, using this evidence in court proceedings.

If a third party is conducting customer due diligence for Cloudpeak Systems s.r.o., the company's staff shall ensure that they also comply with these record-keeping requirements.

Employees shall maintain copies of the identification documents obtained from customers and all materials collected during the account opening process, including but not limited to the account

application. They is required to also record a customer's transactions with Cloudpeak Systems s.r.o.

No business relationship is required to be established until all relevant parties to the relationship have been identified and the nature of the expected business has been understood. Once a business relationship is established, any regular business conducted for that customer is required to be assessed against the expected activity profile. Any unexplained activity is required to then be examined to determine if there is suspicion of money laundering.

Cloudpeak Systems s.r.o.'s personnel, especially those dealing with customers directly, will be most familiar with the customer's transaction profile. Once they determine that a request is outside of the customer's normal activities and either know or suspect, or have reasonable grounds to suspect, that any customer is involved in money laundering, they shall report these suspicions immediately to the MLRO.

Any personnel found to have deliberately failed to report suspicious money laundering or terrorist financing activities to the MLRO may be subject to disciplinary action. As mentioned, Cloudpeak Systems s.r.o.'s staff will receive ongoing training on detecting suspicious activity and the internal reporting process.

Cloudpeak Systems s.r.o. will file a Suspicious Transaction Report (STR) as soon as it knows or suspects that criminal proceeds exist in accordance with the following timeframes:

- ✓ **Immediately upon receiving information that a customer intends to carry out a suspicious operation or transaction.**
- ✓ **Once it is established that the customer is carrying out a suspicious operation or transaction, the operation or transaction shall be suspended, regardless of the amount, and reported to the FAO no later than within 3 working hours from the suspension.**
- ✓ **Immediately, but no later than within 2 working days from the emergence of such knowledge or suspicion, report to the FAO if they know or suspect that property of any value is, directly or indirectly, derived from a criminal act or involvement in such an act, or used to support one or more terrorists or a terrorist organization.**

Cloudpeak Systems s.r.o. will maintain an electronic copy of each STR filed along with supporting documentation for no less than five years. The FAO's preferred method for submission is through the electronic portal at https://www.financnianalytickyurad.cz/oznameni-o-podezrelem-obchodu.

6. Governance of Anti-Money Laundering and Counter-Terrorist Financing Compliance Program

The AML/CTF function at Cloudpeak Systems s.r.o. operates as an independent and integral part of the company's compliance structure, overseen by the appointed Chief AML Officer. This officer is responsible for ensuring the program's alignment with legal and regulatory standards and will provide regular updates to the management team on any significant issues or developments. The AML/CTF program covers a wide range of activities, including but not limited to customer identification procedures, the classification of permissible and impermissible activities, sanctions screening, ongoing transaction monitoring, conducting periodic risk assessments, reporting

suspicious activities, maintaining accurate records, staff training, and ensuring all other activities required by local and international regulations are followed.

In addition, the program aims to foster a culture of vigilance within the company, ensuring that all staff members are aware of their roles in preventing money laundering and terrorist financing. This ensures that Cloudpeak Systems s.r.o. remains committed not only to legal compliance but also to the integrity and ethical conduct of its operations. Through continuous improvement and adaptation to evolving threats and regulations, the company strives to mitigate risks and protect its business from any involvement in illegal activities.

The officer responsible for reporting money laundering activities

The Money Laundering Reporting Officer (MLRO) appointed by Cloudpeak Systems s.r.o. is responsible for the proper execution of the company's Anti-Money Laundering and Counter-Terrorism Financing Manual (AML/CTF) and ensuring the implementation of related processes.

The key responsibilities of the MLRO include:

- ✓ **Ensuring the proper implementation of the AML/CTF Manual and establishing necessary control mechanisms.**
- ✓ **Making updates to the AML/CTF Manual in accordance with new regulations, the introduction of new products, as well as results from AML/CTF audits and monitoring.**
- ✓ **Organizing training sessions for employees and maintaining attendance records.**
- ✓ **Coordinating the process of reporting suspicious activities and collaborating with law enforcement agencies.**
- ✓ **Constantly monitoring changes in legislation regarding AML/CTF and updating the company's internal systems to ensure full compliance with current requirements.**
- ✓ **Reporting on AML/CTF matters to relevant managers and the Board of Directors, providing support and guidance to senior management to address AML/CTF risks in a timely manner.**
- ✓ **Assisting in resolving AML/CTF issues raised by the AML or Risk teams.**
- ✓ **Participating in risk assessments and decisions regarding the termination of customer relationships.**

The MLRO also serves as the main point of contact for external regulators, law enforcement agencies, and other relevant authorities on matters related to anti-money laundering and counter-terrorism financing.

6.1 Compliance Function

At Cloudpeak Systems s.r.o., several teams and specialists are responsible for carrying out tasks related to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF). These individuals form the first line of defense ("FLOD") against risks related to these crimes.
Firstly, to ensure proper client verification and compliance with AML/CTF requirements, the operations, customer support, and KYC/onboarding specialists handle client data verification,

analyze events that may indicate violations, assess screening results, and respond to inquiries from other teams or departments regarding suspicious transactions.
Secondly, the Risk and AML Department is responsible for continuously monitoring client transactions and identifying any suspicious operations or signals that may indicate fraud or links to money laundering or terrorist financing.
The Business Development and Operations Department also plays a crucial role in working with partners and service providers. They gather necessary information from the company's partners to ensure they have the required licenses and effective controls in place for AML/CTF compliance.
The Product Development Department completes the chain of responsibility by ensuring the proper implementation of technical and organizational recommendations from the MLRO. They also test and monitor the effectiveness of the measures applied at the product level.
As a result, the structured approach to AML and CTF tasks at all levels within the company ensures a high level of protection against potential threats and guarantees compliance with regulatory requirements. This approach also enables the timely detection of any suspicious activities and protects the company from the risks associated with legal violations.

6.2 Senior Management Oversight

The Money Laundering Reporting Officer (MLRO) is tasked with sending regular reports to the management and Board, summarizing all signifimayt compliance issues. In addition to these routine reports, MLROs are also responsible for preparing ad-hoc reports on critical matters related to AML/CTF, such as regulatory changes, identified risks, and findings from compliance assessments.

Any substantial modifications to the AML/CTF Manual shall be approved by the Management Board. Smaller, tactical adjustments, like updates to sanctions lists or minor changes to internal tools, may be implemented through ongoing standard operating procedure (SOP) updates and job-specific training for the relevant teams.

For the AML/CTF compliance function to operate effectively, it is crucial that senior management ensures the following:

- ✓ **The compliance function operates independently, with the authority to escalate important issues or risks directly to the Management Board.**
- ✓ **The compliance function has a sufficient budget and resources, including staff and tools, to address any AML/CTF issues as they arise, based on the identified risk levels.**
- ✓ **The MLRO holds a position of sufficient authority within the organization to ensure full compliance across all levels.**
- ✓ **Compliance teams is required to have timely access to all relevant internal and external information to support their monitoring activities.**

In conclusion, the effectiveness of AML/CTF programs depends on the cooperation between the compliance function, senior management, and all relevant teams. This collaborative approach ensures that Cloudpeak Systems s.r.o. remains compliant with the law and actively mitigates any risks related to money laundering and terrorism financing.

Minimum Requirements for AML/CTF Compliance at Cloudpeak Systems s.r.o.

Cloudpeak Systems s.r.o. is committed to maintaining a comprehensive Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) framework, which includes specific requirements for risk assessment, customer identity verification, transaction monitoring, reporting obligations, and record keeping. Below is a summary of the key minimum requirements the company shall adhere to in order to meet legal obligations and mitigate the risks associated with money laundering and terrorist financing.

Risk Assessment

Cloudpeak Systems s.r.o. is required to conduct a thorough risk assessment related to its customers, products, services, geographic locations, transactions, and delivery channels. This assessment shall be proportional to the company's size, documentable, and regularly updated. The risk assessment is required to be available to the relevant authorities or registered bodies upon request, ensuring the company's activities align with current regulatory expectations.

Customer Identity Verification

The company is required to verify the identity of its customers in the following cases:

- ✓ **When establishing a business relationship.**
- ✓ **Before performing any one-off or related cryptocurrency transactions exceeding €10,000 or its equivalent, in accordance with Regulation (EU) 2023/1113 and FATF recommendations.**
- ✓ **Before accepting assets exceeding €10,000 (or its equivalent) in cases outside of existing relationships, including cases of transaction structuring (smurfing).**
- ✓ **When transferring funds from existing business relationships exceeding €1,000 (or its equivalent), in accordance with Regulation (EU) No 2015/847.**
- ✓ **When the customer expands their activity into new markets or territories.**
- ✓ **When there are doubts about the accuracy or authenticity of previously obtained identity information.**
- ✓ **In cases where there are suspicions of money laundering or terrorist financing.**

Additional Requirements:

- ✓ **Proof of Address (POA) is required if the customer's total turnover exceeds €5,000.**
- ✓ **Source of Funds (SOF) is required for transactions exceeding €10,000, in accordance with Regulation (EU) 2023/1113.These measures are implemented to ensure compliance with European Union regulations and to mitigate risks associated with financial crimes.**

Establishing Purpose and Scope of Relationship

When initiating a business relationship, it is essential to determine the purpose and scope of that relationship if it is not already apparent from the nature of the business engagement.

Beneficial Owner Identification

For every client, Cloudpeak Systems s.r.o. is responsible for identifying and verifying the beneficial owner—those who ultimately control or own the entity or who conduct transactions on its behalf.

This includes anyone who holds more than 25% of the shares or voting rights in the entity.

Monitoring Customer Accounts

Cloudpeak Systems s.r.o. will continuously monitor customer accounts for unusual or suspicious transactions. This ongoing monitoring is conducted through appropriate processes and systems designed for relevant business areas.

Reporting Obligations

The company shall promptly report suspicious transactions or one-off arrangements to the Financial Analytical Office (FAO). All reports shall be submitted unfiltered and in a timely manner unless there is a valid reason for delayed reporting, such as hindering investigations. The responsible Money Laundering Reporting Officer (MLRO) shall be informed of all suspicious activity reports.

Record Keeping

Cloudpeak Systems s.r.o. will retain customer records for a minimum of eight years. These records will include:

- ✓ **Copies or references to documents verifying the customer's identity.**
- ✓ **Supporting documentation for business relationships or one-off transactions subject to due diligence and ongoing monitoring.**
- ✓ **Detailed transaction records that form a clear audit trail, ensuring the ability to reconstruct financial profiles for suspected clients.**

AML Controls and Training

The responsible MLRO ensures that adequate controls are in place to comply with AML regulations, with a focus on customer and transaction monitoring. Additionally, all employees involved in onboarding and transaction processing shall undergo AML training, initially within three months of joining, followed by annual refreshers.

Ongoing Risk Analysis

The MLRO will continuously assess AML risks based on the company's product offerings, customer profiles, and geographical exposure. Appropriate security measures will be implemented based on the analysis to mitigate identified risks.

By fulfilling these requirements, Cloudpeak Systems s.r.o. ensures that it operates in compliance with anti-money laundering and counter-terrorist financing laws. These measures not only protect the company from legal and financial risks but also contribute to the global fight against money laundering and terrorism financing. Continuous monitoring, training, and risk assessments are critical components in maintaining a strong defense against financial crime and ensuring the integrity of the company's operations.

<u>Act No 253/2008 Sb. Of 5 June 2008 on Selected Measures against Legitimization of Proceeds of Crime and Financing of Terrorism of the Czech Republic:</u>

- ✓ **Require companies to take measures to identify their Customers including beneficial ownership.**
- ✓ **Require businesses to carry out and document risk assessment.**

- ✓ **Specify the policies and procedures that financial institutions and other relevant businesses shall put in place to prevent and identify activities relating to money laundering and terrorist financing.**
- ✓ **Require businesses in the regulated sector to appoint a Nominated Officer to receive internal reports from staff with knowledge or suspicion of money laundering or terrorist financing.**
- ✓ **Set out the supervision and registration arrangements.**

Cloudpeak Systems s.r.o. "Know Your Customer (KYC)" Manual

Customer Identity: The Basics of KYC

One of the primary aspects of anti-money laundering (AML) policy is ensuring proper identification of customers. In accordance with KYC standards, the company shall verify the identity of its customers by gathering necessary information, including the nature of their business, source of funds, transaction details, and proof of identity documents.

All new customers undergo verification, and no transactions may be processed on behalf of any new customer without MLRO (Money Laundering Reporting Officer) approval. Employees are responsible for obtaining and submitting the necessary documentation for KYC verification, after which the MLRO reviews the application for completeness. In cases of incomplete applications, employees shall provide additional documentation. If suspicious activity is noted, employees shall report it to the MLRO and cease further transactions until guidance is provided.

Beneficial Owners: Who Stands Behind the Client

Beneficial owners are individuals who ultimately own or control a customer or on whose behalf a transaction is conducted. Identifying beneficial owners is a crucial part of the KYC process as the company shall know those who own or control more than 25% of assets or voting rights. For companies or trusts, the task is to identify who has control over the funds or makes decisions related to the business.

Employees shall verify and record information about beneficial owners, ensuring that any indirect ownership or control is also considered. If there is uncertainty about the required information, employees is required to consult with the MLRO for further assistance.

Politically Exposed Persons (PEPs): Increased Risk

Politically Exposed Persons (PEPs) are individuals holding prominent public positions and are considered high-risk due to their vulnerability to bribery and corruption. As part of its AML measures, Cloudpeak Systems s.r.o. conducts enhanced due diligence on all identified PEPs, regardless of whether they are domestic or foreign. Immediate family members and close associates of PEPs are also subjected to enhanced scrutiny.

Additionally, the company shall take further steps to ascertain the source of wealth and source of funds involved in transactions with PEPs and seek approval from senior management before establishing or continuing any business relationship with a PEP.

Types of Clients Subject to Enhanced Due Diligence

The company places particular attention on the following categories of clients:

- ✓ **Beneficial owners who control more than 25% of shares or voting rights.**
- ✓ **Partnerships where more than 25% of the capital or profits are controlled by one or more individuals.**
- ✓ **Limited Liability Companies where complex ownership or control structures exist.**
- ✓ **Trusts where it is necessary to identify the individuals exercising control over the assets.**

KYC procedures are fundamental for ensuring that the company complies with anti-money laundering (AML) and counter-terrorist financing (CTF) regulations. Proper identification of customers, beneficial owners, and PEPs helps mitigate the risks associated with financial crimes. Adhering to these standards not only ensures compliance with international regulations but also builds trust with clients and partners. A compliant business is one that maintains its reputation, a key factor in long-term stability and success in the global market.

Identification of Elevated Risks and Mitigating Factors in PEP Relationships

Cloudpeak Systems s.r.o. monitors Politically Exposed Persons (PEPs) for potential risks associated with money laundering and corruption. Below are the key red flags indicating high-risk relationships, along with mitigating factors and our approach to managing PEP-related risks.

Red Flags Signaling High-Risk PEP Relationships

Several indicators suggest a PEP relationship poses an elevated risk for the company:

- ✓ **Conflict of Interest: A PEP's public functions conflict with their role at Cloudpeak Systems s.r.o., raising concerns about undue influence.**
- ✓ **High-Risk Jurisdictions: A PEP is associated with a country known for AML/CFT regime weaknesses or high corruption levels.**
- ✓ **Corruption-Prone Industries: The PEP's economic interests lie in sectors prone to corruption, such as natural resources, defense, or government infrastructure projects.**
- ✓ **Complex Corporate Structures: Unusually complex corporate arrangements, including trusts and foundations established in tax havens, or entities controlled by PEP's family members but not by the PEP themselves.**
- ✓ **Negative Media Attention: The PEP has been involved in bribery, tax evasion, criminal investigations, or other legal disputes.**
- ✓ **Property Ownership Restrictions: The PEP is from a country that restricts public officials from owning assets abroad without proper disclosures.**

Mitigating Factors that Could Decrease Risk

While PEPs are always treated as high-risk clients, certain factors may reduce perceived risk:

- ✓ **Low-Risk Jurisdiction: A PEP from a low-risk country with minimal links to their status may be considered lower risk (e.g., PEP making casual personal purchases).**

- ✓ **Honorary Role: If a PEP's position is purely honorary (e.g., a board member in a non-profit organization), and they are not involved in daily operational or financial decisions.**
- ✓ **Low-Volume Activity: A PEP whose financial activity is low in volume and infrequent could present a reduced risk.**

Despite these mitigating factors, all PEPs remain categorized as high-risk, and they shall undergo enhanced due diligence. The factors mentioned above help determine the specific scope of due diligence required, but do not alter the necessity for thorough investigation.

Handling Former and Deceased PEPs

Cloudpeak Systems s.r.o. takes a stringent approach towards former PEPs, following the FATF recommendations.

The risks associated with former PEPs are evaluated based on their individual circumstances, considering factors such as:

- ✓ **Influence they may still exert post-retirement.**
- ✓ **Links between their previous roles and current business activities.**
- ✓ **Potential access by family members to illicit or improperly declared assets following the PEP's death.**

Due Diligence and Monitoring Process

All employees shall immediately notify the Money Laundering Reporting Officer (MLRO) when a customer's PEP status is identified. No accounts are to be opened for PEP clients without prior MLRO approval. Enhanced due diligence measures are implemented for all PEP relationships, including screening for PEP status and sanctions using automated tools and third-party services such as Sum&Sub.

Cloudpeak Systems s.r.o. adheres to the highest standards of due diligence and risk management when dealing with PEPs. By thoroughly evaluating red flags, mitigating factors, and conducting continuous monitoring, the company ensures compliance with AML/CFT regulations and effectively manages the risks associated with PEP relationships. The approach aligns with FATF recommendations, safeguarding the company from potential reputational damage, legal challenges, and involvement in illegal financial activities.

7. New Accounts

Before initiating any business relationship with a customer, Cloudpeak Systems s.r.o. shall ensure that the customer's identity is accurately verified and that proper documentation for the business is obtained. This process is essential to create a comprehensive "Customer Profile," which will allow the company to understand all aspects of the customer's intended relationship with the business while ensuring compliance with AML/CTF (Anti-Money Laundering and Countering the Financing of Terrorism) regulations.

Customer Verification Process

A relationship with an individual or a business will not be established unless the potential customer's identity is fully verified. If a prospective customer refuses to provide the required information, the relationship will be rejected. It is crucial to gather complete and accurate customer data. Shortcuts or incomplete information, such as "P.O. Box address," "No last name," or vague addresses like "Street, Prague," are considered unacceptable and will increase the risk of regulatory violations.

Exceptions for Specific Business Types

While the customer verification process applies to all, there are certain exceptions for specific types of businesses. These include:

- ✓ **Banks (excluding shell banks, as per the company's policy).**
- ✓ **Gatekeepers such as notaries, accountants, auditors, and solicitors.**
- ✓ **Government entities.**
- ✓ **Quasi-governmental entities.**

These exceptions shall be approved by the MLRO (Money Laundering Reporting Officer) before proceeding.

Registration Requirements

Participants registering on the company's website shall create a personal password. Individuals under the age of 18 are prohibited from registering. Additionally, individuals identified as problem gamblers will be excluded from registration, as well as those who have previously been excluded from the site. All registration records, including attempts and completions, will be carefully maintained.

Upon completion of the registration form and agreement to the terms and conditions, an email will be sent to the provided address for confirmation. Registration will not proceed if all fields are incomplete. To activate the account, the user will need to log in again using a provided link and input their password. No funds may be deposited and no bonuses will be allocated until the account is fully activated.

It is imperative that Cloudpeak Systems s.r.o. follows these stringent customer verification and registration processes to comply with legal requirements, mitigate the risk of fraud, and ensure the integrity of its business operations. Clear and complete customer profiles are essential in maintaining compliance with AML/CTF regulations and protecting both the company and its clients from potential risks.

8. Identification of New Customers and Customer Due Diligence

All Customers shall provide identification to establish accounts as described below. It is required to be kept in mind that identifying documents may be presented by persons not entitled to them.

Therefore, they shall be carefully examined for authenticity and accuracy of description. It is the responsibility of each employee to ensure that the appropriate identity documents are obtained for their Customers. Failure to do so will delay the accreditation of the Customer account by the MLRO.

8.1 Customer Due Diligence Stages

The customer verification process at Cloudpeak Systems s.r.o. is a crucial element for ensuring compliance with anti-money laundering (AML) and counter-financing of terrorism (CFT) legislation. Each customer undergoes verification to assess their risk level and ensure proper controls are in place.

Customer Identification and Simplified Due Diligence

The first step is identifying the customer during the registration phase. Customers provide basic information about themselves, their activities, and their intentions regarding the business relationship with the company. During this process, the customer shall accept the terms of use and relevant policies related to security and confidentiality.

Simplified due diligence is only performed in specific cases where the risk of money laundering or terrorist financing is low. This helps streamline the process for customers with minimal risk.

Collection and Verification of Data

For natural persons, simplified due diligence involves collecting the following data:

- ✓ **First and last name.**
- ✓ **Date of birth or other unique identification code.**
- ✓ **Residential address and nationality.**
- ✓ **Email address.**

For legal entities, the required information includes:

- ✓ **Company name.**
- ✓ **Legal form and company code (if available).**
- ✓ **Registered office address and actual place of business.**

A critical requirement is that the customer's first payment shall be made from an account held with a financial institution located in a Member State of the European Union or a third country that complies with AML/CFT standards.

Standard Verification and Further Actions

In cases of higher risk or doubts about the accuracy of the information provided, Standard Customer Due Diligence (SCDD) is carried out. This includes requesting additional documents such as passport copies, public registry information, questionnaires, and other documentation that helps verify the customer's information.

The verification process also includes automatic checks using accessible public databases, enabling more efficient risk monitoring and ensuring the reliability of the verification.

Maintaining Up-to-Date Information

Beyond initial verification, it is essential to regularly update customer information. This includes transaction monitoring and checking for suspicious activities. Based on these findings, additional measures such as Enhanced Due Diligence (EDD) may be applied to high-risk customers.

Operational Review and Documentation

All customer-provided data shall be verified and stored electronically in their files. Each document is required to be checked for accuracy. If minor discrepancies are found (such as typographical errors), corrections may be made in the database.

Transparency and reliability in the customer verification process are fundamental to mitigating risks associated with money laundering and other illicit activities. Simplified due diligence ensures efficiency in low-risk cases, while standard and enhanced due diligence enable the company to minimize potential threats and ensure full compliance with all legal requirements.

Onboarding and Verification Questions

Customer category	**Collect and verify**
Natural persons	**Email** **Full name (name and surname)** **National or foreign ID type, number and photo** **Residential address** **Personal identification code and/or Date of birth (include age validation)** **Place of birth** **Nationality** **Phone number** **Purpose and scope of the business relationship**
Business Accounts	**Email** **Legal entity name** **Legal form** **Date and place of incorporation** **Registered address** **Business address** **Registration number or Tax/VAT number (depending on what is commonly used in the country, VAT number mandatory for EU)** **Dated company register extract issued within the last 3 months** **Governance and organizational structure of the legal person** **Purpose and scope of the business relationship** **Contact phone number**

	Website **Account representative (including directors, managers, proxy-holders) – the following details must be collected:** **Full name;** **Personal code and/or Date of birth;** **Place of birth (country);** **Address;** **National or foreign ID; document type, number, photo;** **Nationality;** **Phone number.** **Beneficial owners. Minimum information to be collected for all beneficial owners in excess of 25% ownership:** **Full name;** **Personal code and/or Date of birth;** **Country of residence;** **Nationality.** **Industry category and type/nature of business activities**
Customer representatives	**For every natural or legal person – ask and verify if the Customer is acting through a representative or is otherwise controlled by someone else** **For every representative that is a natural person:** **Full name;** **Personal code and/or Date of birth;** **Country of residence;** **National or foreign ID; document type, number, photo.** **For every representative that is a legal person:** **Legal entity name;** **Legal form;** **Date and place of incorporation;** **Registered address;** **Business address;** **Registration number or Tax/VAT number (depending on what is commonly used in the country, VAT number mandatory for EU);** **Dated company register extract issued within the last 3 months;** **Governance and organizational structure of the legal person;** **Industry category and type/nature of business activities.**

Remote Identification

After identifying the persons who must be verified (individual clients or a legal entity's directors, managers, authorized representatives, and beneficial owners), the identification is completed via Sum&Substance. An employee sends the client a time-limited link and the client follows the steps (document upload/checks and biometric verification). Once the process is completed, Sum&Substance provides a confirmation and a report, which Cloudpeak Systems s.r.o. stores in the client file. Access to the platform and the start of onboarding are automatically blocked for users from prohibited jurisdictions listed in Annex 1.

Proof of Identity (POI) Document Review

The following documents are accepted as proof of identity: passport, ID card, or resident card. The documents shall be valid at the time of submission and include essential data: name, date of birth, issuing authority, issue date, and expiration date. Minor errors (such as typos) may be corrected by the employee, but signifimayt ones shall be clarified with the client.

The photo of the document shall be taken during live identification (not a screenshot or photo of the screen). The passport and ID card shall include a photograph and relevant security features.

Verify that the name, date of birth, and nationality of the client match the data on the POI document.

Ensure that the POI is not expired.

Check if the phone country, address, and IP address match. In case of discrepancies, the cause is required to be clarified.

Verify that the selfie of the client matches the photograph on their document. The verification is also performed manually.

Proof of Address (POA) Document Review

The following documents are accepted as proof of address: utility bills, bank statements, letters from government authorities, rental contracts. The POA document shall not be older than 3 months and is required to clearly state the client's name and address.

Verify the authenticity of the POA documents (logos, stamps, government seals, website of the issuing authority). They shall be valid for the last 3 months and match the information in the system.

Business Clients

For business clients, it is necessary to verify:

- **The name of the legal entity;**
- **The date and place of registration;**
- **The unique company number (registration or VAT number).**

It is important to check whether the provided information aligns with changes in the business or its activities.

Screening

Every client shall undergo a screening against sanction lists, PEP (Politically Exposed Persons) lists, and criminal records using Refinitiv World-Check One. The results of the screening are stored in the client’s folder.

Back-end Checks and Smayning

At the moment of Customer onboarding these checks shall be done:

Data Provided by the Customer	"Silent checks" – not visible to the Customer	Follow up, if there is an alert
Full name (or legal entity name and all names associated with the account)	- All names associated with the account must be scanned against sanctions lists and PEP lists, including at least the following: • Natural person name; • Company name; • Company representative/proxy-holder; • Company director; • Company owners with at least 25% shareholding; • Company directors/board members, supervisory boards and other heads if identified; • Company business partners that are known or declared; • Beneficial owners; • Declared family members or close associates (politically exposed persons); • Any other legal or natural persons who are relevant to be screened.	- If there is a partial match from scanning (e.g. name matches, but country is different, or date of birth is different), an account must not be opened, until the investigation is completed. - No need to look at the account by the responsible employee before the Customer has uploaded the documents (because without the documents we won't be able to resolve the partial match). - If the Customer does not react, account remains inactive. - Account status must be "waiting for information" and inactive.
Date of birth	- Validation that the Customer is 18 years old	- Block if the Customer is under 18
Address	- Ensure that the address is from an eligible country - Check for consistency between IP, geolocation and resident address and phone prefix	- Flag inconsistencies, but no action required, until a transaction attempt occurs (e.g. Customer received funds or added funds to their account)

	- **Detect if VPN or other disguising techniques were used**	- **Flag Customers from high-risk countries, block disputed territories or territories where Cloudpeak Systems s.r.o. does not offer services**
Nationality	- **Block North Korea, and any other country nationals Cloudpeak Systems s.r.o. does not support** - **Flag cases where the nationality is different from the residence country (excluding mismatches between EU countries), because there will be a need to ensure legitimate residence status, where nationality does not equal residence.**	- **In cases where the nationality is different from the residence, ensure we will ask for the proof of visa/legal status**
E-mail	- **Confirm email by reverse link** - **Detect temporary emails and bots** - **Scan emails for references in commercial registers, social media and other public databases**	- **Flag bots and temporary emails**
Phone number	- **Check consistency with country info, flag inconsistencies**	- **Phone must be confirmed later at the stage of 2-Factor Authentication setup**

Data Verification

All data related to clients, their representatives, and beneficial owners shall be obtained from reliable and independent sources. These may include official documents confirming identity (passport, ID card, registration certificate, etc.) containing identification codes, nationality, photo, and signature of the person.

Escalation Process

If there are suspicions during the verification, a report is required to be prepared with the following details: • The reason for suspicion; • Date of client registration and verification; • Communication with the client (email, support); • Transaction history (if any); • Documents (source of funds, certificates); • Linked accounts (same email, frequent transactions, etc.).

Risk Assessment

Clients shall be classified based on risk level: low, standard, or high. The verification measures are determined accordingly.

Beneficial Owner

A beneficial owner is a natural person who controls the client or conducts transactions on their behalf. For corporate entities, these are individuals owning more than 25% of shares, and for funds or other entities, those controlling 10% or more of the property.

Cloudpeak Systems s.r.o. collects data on beneficial owners, including their name, nationality, date of birth, and country of residence. This data is verified through public registers or other sources.

Actions in Case of Doubts

If a client does not provide necessary information or is uncooperative, Cloudpeak Systems s.r.o. will cease providing services, freeze the account, and file a report on suspicious transactions if there are concerns about money laundering or terrorist financing.

Reduced verification requirements for beneficial owners may apply to publicly listed companies, government institutions, international organizations, and other regulated entities.

8.2 Verification Triggers

Customer Due Diligence and Risk Assessment Procedures

Cloudpeak Systems s.r.o. applies simplified due diligence (SDD) for low-risk customers, such as those making low-value transactions for goods and services, but this does not exempt the company from continuously monitoring business relationships and identifying suspicious behavior. To qualify for simplified due diligence, the customer's transactions shall meet specific criteria, including transaction limits, funding methods, and smayning clearance. All customer identity verification is triggered if certain conditions occur, such as transactions exceeding 1,000 EUR, or if there are suspicions of money laundering or terrorist financing. If a customer fails to complete identity verification within 10 days, account activities will be restricted.

Customer Screening and Sanctions Lists
Cloudpeak Systems s.r.o. uses Sum&Substance for customer screening against various sanctions lists, including UN, USA, EU, and others. Screening occurs at onboarding, when there is a change in personal information, or periodically depending on the customer's risk. The screening includes evaluating whether the customer or related parties are on any sanctions list.

Remote Customer Verification
Remote verification is done through live video transmission, capturing the customer's image and identity documents. This verification process is outsourced to Sum&Substance, and all necessary documents, including utility bills and other personal identification, are gathered and validated. If discrepancies arise, the account will be restricted, and further investigation or documentation may be required.

Enhanced Due Diligence (EDD)
For higher-risk clients, Cloudpeak Systems s.r.o. performs Enhanced Due Diligence (EDD). This involves obtaining detailed information about the customer's wealth, sources of funds, business

activities, and any adverse media related to the customer. A higher level of scrutiny is applied, especially for politically exposed persons (PEPs) and cross-border transactions. For PEPs, senior management approval is required to establish or continue relationships, and ongoing monitoring is enforced.

Cross-border and High-Risk Relationships
In cases of high-risk relationships, such as those involving countries with insufficient anti-money laundering measures, additional due diligence is performed. This includes stringent identification procedures, enhanced reporting, and close scrutiny of transaction purposes. Relationships with high-risk countries demand further investigation and documentation to ensure full compliance with global AML/CTF standards.

Establishing Customer Relationships
To establish customer relationships, Cloudpeak Systems s.r.o. requires the completion of an application form, collection of identification, and verification of business documentation. A risk assessment is performed, and the customer is screened against relevant sanctions and lists. Once all information is reviewed and approved by the Money Laundering Reporting Officer (MLRO), the account file is created, and the account is officially opened.

Account Files
An account file shall be maintained for each customer, including a compliance checklist, identification evidence, proof of address, verification against sanctions lists, and any other relevant documentation based on the business type. Reviews and decisions made during the account-opening process shall also be documented.

9. Dormant Accounts

Dormant Accounts Policy

Dormant accounts at Cloudpeak Systems s.r.o. may arise due to various circumstances, such as account owners abandoning accounts with minimal or no balance, or the death of a customer. In accordance with AML/CTF and regulatory requirements, Cloudpeak Systems s.r.o. has implemented several procedures to manage dormant accounts, guided by principles of loyalty, good faith, diligence, and due care.

An account will be considered dormant if:

- ✓ **There are no active transactions, logins, or sessions for 1 year (automatic transactions or those not requiring the account holder's active participation are excluded from this condition).**
- ✓ **There has been no communication or instructions from the customer or their authorized representative, including no contact with customer support via email, chat, or other channels attributed to the specific account for the last year. If a customer has multiple accounts, activity on one account prevents the others from being classified as dormant.**

As part of Cloudpeak Systems s.r.o.'s AML/CTF obligations, it is required to apply customer due diligence to dormant accounts. This includes monitoring these accounts to prevent unauthorized

access or manipulation of balances. Any sudden activation of a dormant account will be treated as high risk, unless the customer provides a valid explanation.

For accounts marked as dormant, the following actions will be taken:

- ✓ **Standard communications will continue to be sent to the customer's designated email address (e.g., updates, mandatory terms, etc.).**
- ✓ **For dormant accounts with a balance of at least 5,000 EUR (or equivalent in cryptocurrencies), a registered reminder letter will be sent to the customer's last known postal address. The letter will serve as a reminder to log in or contact customer support. These reminders will be sent at least annually, unless the address is found to be invalid.**
- ✓ **A negative media and social media search will be conducted annually for dormant accounts with balances of 5,000 EUR or more, and the results will be recorded and retained.**
- ✓ **Dormant accounts will be included in mandatory regulatory reports as required.**
- ✓ **Reactivation of a dormant account will only occur after completing a thorough due diligence process and re-assessing all information previously collected to meet KYC requirements.**
- ✓ **No automatic withdrawals or debits will be allowed from dormant accounts, though credit transactions may occur, and any suspicious transactions will be investigated.**
- ✓ **Cloudpeak Systems s.r.o. may charge the customer for any additional costs incurred in managing dormant accounts, such as research, registered mail, or investigative costs.**
- ✓ **The dormancy of an account does not impact Cloudpeak Systems s.r.o.'s obligation to retain documents.**

Managing dormant accounts is crucial to ensure full compliance with regulatory requirements and safeguard against the potential risks of unauthorized access or fraudulent activities. By implementing these procedures, Cloudpeak Systems s.r.o. aims to protect both customers and the company from possible exploitation, while maintaining a transparent and efficient system for account management.

10. Ongoing Monitoring of Customer Relationships

Ongoing Monitoring of Customer Relationships

Cloudpeak Systems s.r.o. is committed to maintaining effective ongoing monitoring of its customers to ensure that the transactions conducted remain consistent with the company's knowledge of the customer's business, risk profile, and status. The aim is to ensure that customers continue to fit within their assigned risk categories, such as standard risk, and that any collected corporate background information is kept up to date. Cloudpeak Systems s.r.o. conducts ongoing due diligence by monitoring customer transactions, screening against sanctions lists, tracking account activity and behavioral patterns, analyzing "machine fingerprints," and reviewing customer identification records and communication histories. Information gathered during customer onboarding is periodically reviewed to identify any changes in the customer's business activities or ownership structure. Customers classified as high risk undergo this review at least once a year.

Risk Indicators for Periodic Review

Several factors may trigger the need for a periodic review of a customer relationship, including:

- ✓ **A substantial increase in activity, high transaction volumes, or a signifimayt shift in transactional patterns.**
- ✓ **Reactivation of a dormant account with a sudden surge in activity.**
- ✓ **An increased number of chargebacks or disputed transactions.**
- ✓ **Receipt of complaints or inquiries from authorities.**
- ✓ **Discrepancies between the customer's name and the payment method used (e.g., using an e-wallet or mobile wallet not associated with the customer).**
- ✓ **Changes in the customer's business activities or website URL.**
- ✓ **Modifications to the customer's ownership structure or management, or news indicating a merger or acquisition.**
- ✓ **Inconsistencies in geographical data, such as mismatches between the customer's IP address, card BIN country, or billing address.**
- ✓ **Suspicious activities identified in transactional messages.**

When a triggering event occurs, the responsible analyst will identify it through standard monitoring reports or via notification from another department (e.g., the complaints department or risk monitoring team). The analyst will then review the customer's data, ensure any required updates are obtained, and determine whether the customer's risk rating needs to be adjusted.

Handling Sanctioned Individuals

If, during the customer onboarding process, ongoing monitoring, or enhanced due diligence (EDD), it is discovered that a customer is a sanctioned individual or has links to sanctioned entities or individuals, the employee shall take immediate action. This includes:

- ✓ **Freezing all the client's available funds or economic resources.**
- ✓ **Ceasing all financial transactions or services with the client.**
- ✓ **Applying Enhanced Due Diligence measures.**
- ✓ **Informing the Money Laundering Reporting Officer (MLRO) and filing an internal report.**
- ✓ **Suspending the client's account until further instructions from the MLRO.**

It is prohibited to notify the client or any third parties (other than senior managers or the MLRO) about the freezing measures in advance. Upon receiving the internal report, the MLRO shall review the case as soon as possible. If there is reasonable suspicion that the customer is a sanctioned individual under the relevant sanctions lists (OFAC, EU, UN, or national sanctions), the MLRO will cease all business activities with the client and report the matter to the Financial Intelligence Unit (FIU).

Ongoing monitoring is an essential part of Cloudpeak Systems s.r.o.'s commitment to ensuring compliance with AML/CTF regulations and safeguarding against potential risks, including those associated with customers linked to sanctions or other suspicious activities. By continuously reviewing customer data and transactional behavior, the company may quickly identify any changes in a customer's risk profile and take appropriate action to mitigate potential threats.

11. Record Keeping Procedures

Cloudpeak Systems s.r.o. is committed to maintaining comprehensive records of Customer Due Diligence (CDD) information and records related to account activities and transactions. The primary objective is to ensure that, is required to an investigation arise, the company may provide authorities with an accurate audit trail. All CDD information and transaction records related to a customer will be preserved within the customer's file.

All customer-related data will be stored and managed in accordance with relevant laws and regulations. Documents acquired during the Know Your Customer (KYC) process, screening results, risk assessment summaries, and transaction details will be retained throughout the business relationship and for a period of 10 years after the conclusion of the relationship. This period may be extended if required by applicable authorities or regulations.

Record Keeping Requirements

The AML Compliance team is responsible for retaining the following records:

- ✓ **Physical or electronic records of customer identification and verification documents, including those related to beneficial owners, representatives, and any connected parties.**
- ✓ **Additional information regarding the customer or beneficial owner collected during Enhanced Due Diligence (EDD) or ongoing monitoring.**
- ✓ **Documents that outline the purpose and intended nature of the business relationship.**
- ✓ **Records related to the customer's account, such as the account opening form, risk assessment form, and any signifimayt business correspondence related to CDD or changes to the account's operation.**

Cloudpeak Systems s.r.o. is also required to maintain records of transactions, which is required to include the following details:

- ✓ **The identity of the parties involved in the transaction.**
- ✓ **The nature, date, and value of the transaction, including the order date and execution date.**
- ✓ **The type and amount of currency involved.**
- ✓ **The origin and destination of the funds.**
- ✓ **The form of instruction and the authority given for the transaction.**
- ✓ **The type and identifying number of any account involved (if applicable).**
- ✓ **A unique transaction identifier.**

Retention and Deletion of Records

Records is required to be maintained for a period of 10 years from the end of the business relationship, unless the customer consents to a longer retention period or there are legal grounds for retaining the records. After this period, personal data is required to be deleted unless required by law or court order, or if there are reasonable grounds to retain the data for legal proceedings.

Transaction records shall be stored in a format that enables investigating agencies to track the details of any suspected criminal activity and establish a financial profile for further investigation. Employees will receive training on the filing and record-keeping system used by Cloudpeak Systems s.r.o.

Logs to be Maintained:

- ✓ **Log of suspicious monetary operations or transactions.**
- ✓ **Log of all monetary transactions performed by customers.**
- ✓ **Cash transaction log.**
- ✓ **Log of customers whose business relationships have been terminated.**

Effective record-keeping is an essential aspect of Cloudpeak Systems s.r.o.'s commitment to regulatory compliance, ensuring the company may respond to investigative inquiries and maintain a clear audit trail. By retaining detailed and organized records, the company upholds its responsibility to monitor, assess, and act on customer transactions in accordance with anti-money laundering (AML) and counter-terrorist financing (CTF) regulations.

12. Risk-Based Approach to Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF)

Cloudpeak Systems s.r.o. has adopted a risk-based approach to effectively combat money laundering (ML) and terrorist financing (TF), in accordance with applicable regulations. This approach involves tailoring customer due diligence (CDD) measures and AML/CTF controls based on the assessed risk associated with each customer relationship. The company mandates compliance with the procedures outlined in this Manual, and non-compliance may result in disciplinary actions, including termination for employees or contractors.

Customer Categorization and Risk Assessment

Cloudpeak Systems s.r.o. categorizes each customer based on the perceived risk of ML/TF, which is assessed before the customer is allowed to use the company's services and at regular intervals thereafter. This assessment considers factors such as the nature of the customer's business, the geographic locations involved, the products or services offered, and customer behavior. As new information becomes available, the risk assessment is updated accordingly.

The risk-based categorization directly impacts the customer due diligence measures, including the level of approval needed for business transactions and the frequency of due diligence activities. Customers are classified into three risk categories:

- ✓ **Low-Risk Customers: These customers present a very low risk of ML/TF and are subject to simplified procedures and monitoring.**
- ✓ **Standard-Risk Customers: These customers are considered to present a sufficiently low risk, with standard procedures and monitoring applied.**

- ✓ **High-Risk Customers: These customers present an elevated risk of ML/TF, requiring enhanced due diligence and approval from senior management to proceed with the business relationship.**

Risk Factors for Classification

The assessment of a customer's risk level is based on multiple criteria:

- ✓ **Country of Origin: Customers from high-risk jurisdictions or countries subject to sanctions are considered higher risk.**
- ✓ **Legal Form: Certain legal structures, such as trusts or foundations, may pose a higher ML/TF risk.**
- ✓ **Business Line: The type of business a customer engages in is assessed, with activities such as online marketplaces, gambling, telecom services, and luxury item sales considered higher risk.**
- ✓ **Politically Exposed Persons (PEPs): Customers or their beneficial owners identified as PEPs are categorized as higher risk and subject to enhanced scrutiny.**

Prohibited Customers

Cloudpeak Systems s.r.o. strictly prohibits certain customer relationships, including those involving:

- ✓ **Applimayts from sanctioned countries or individuals on sanction lists.**
- ✓ **Customers involved in illegal activities or operating businesses without the necessary licenses or permits.**
- ✓ **Those dealing in restricted or prohibited goods, including stolen items, illegal drugs, weapons, or counterfeit goods.**
- ✓ **Individuals who refuse to provide accurate KYC information, or those who provide false or incomplete information.**

Mitigation Measures for Non-Face-to-Face Relationships

For new customers with no established transactional history, Cloudpeak Systems s.r.o. may implement additional measures, such as:

- ✓ **Limiting transaction amounts until a proven track record is established.**
- ✓ **Requiring a small fund transfer from a regulated institution.**
- ✓ **Performing additional scrutiny of the customer's digital footprint, such as IP address and device analysis.**

By adopting a risk-based approach to customer due diligence, Cloudpeak Systems s.r.o. may effectively mitigate the risks associated with money laundering and terrorist financing. The company ensures that all customers are classified based on their risk profile, allowing for tailored due diligence measures. Ongoing monitoring, periodic risk reassessments, and stringent controls help maintain compliance with regulatory requirements while protecting the company from financial crimes.

12.1 Assessing Risk

The tables below highlight some indicators that employees may use to determine the risk posed by a Customer. The table is not exhaustive, and employees shall liaise with the MLRO if they are concerned about any Customer.

Risk Category	Higher Risk	Lower Risk
Transaction Type	Large one-off transactions by new customers. Transactions involving significant cash, e.g., MSBs, casinos, and betting shops. Customers from outside the business's local region. Customers with complex ownership structures, making it difficult to identify the underlying beneficiaries. Groups of customers making frequent transactions to the same individual or group. A sudden spike in business activity from an existing customer. Transactions that appear uncharacteristic of the customer's usual behavior. Customers with significant assets or engaging in transactions outside the typical scope.	Low-value transactions or those involving minimal assets. Transactions of a standard size, without sudden increases or inconsistencies. Customers regulated under jurisdictions with robust Anti-Money Laundering standards. Publicly owned companies traded on recognized exchanges and their subsidiaries. Long-standing customers making regular transactions. Consistent transactional behavior in line with known activities. Business relationships involving frequent, recurring transactions.
Customer Behavior	Reluctance to provide identity verification or submitting inadequate identification documents. A refusal to disclose the identity of the person they represent, when acting on behalf of someone else. A willingness to pay unusually high penalties or charges. Difficulty verifying the source of funds involved in transactions. Using intermediary corporate vehicles or structures with no clear rationale.	Full cooperation and submission of required documentation. Openness in providing requested information. Transactions with reasonable and explainable charges. Transparent and verifiable sources of funds. Simple, transparent structures for transactions.
Method of Customer Acquisition	Occasional, one-off transactions rather than a long-term business relationship. Business introduced without substantial market research or prior engagement. Non-face-to-face transactions.	Ongoing and frequent transactions between the customer and business. Customers who come to the business after thorough vetting and market research. In-person transactions or face-to-face interactions.

Product/Service Usage Risk	Products that facilitate third-party payments or that could involve inappropriate asset transfers. Risk of improper or suspicious assets moving through the business.	Products that are straightforward and involve little to no third-party transactions. Regular, low-risk asset transactions.
Country of Origin Risk	Customers from countries subject to UN sanctions or other international embargoes. Customers from countries identified by FATF as posing higher ML/TF risks. Customers from countries with known terrorism support or funding risks. Customers from high-risk jurisdictions, identified by credible organizations like Transparency International.	Customers from countries listed on the White List. Countries with low risk of corruption or criminal activity. Countries with high economic development and strong anti-corruption practices.

If any employee considers a customer or transaction to be high risk for money laundering or terrorist financing, they shall immediately report the matter to the Money Laundering Reporting Officer (MLRO). Based on this report, the MLRO may direct further due diligence or investigation into the customer's identity or source of funds.

It is important to note that being classified as higher risk does not necessarily mean a customer is engaged in illegal activities. Similarly, a lower-risk classification does not rule out the potential for money laundering or terrorist financing. Employees shall remain vigilant and report any suspicions of improper conduct.

By classifying customers based on the various risk indicators, Cloudpeak Systems s.r.o. may apply appropriate due diligence measures tailored to the specific risk profile of each customer. Regular monitoring and timely updates to risk classifications are essential to maintain the effectiveness of the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) framework.

12.2 Ongoing Risk Assessment

The MLRO and the senior management team will carry out regular assessments of the risks posed by Cloudpeak Systems s.r.o.'s Customers and the services provided by Cloudpeak Systems s.r.o.. The procedures set out in this Compliance Manual will be regularly assessed against the risks posed by Cloudpeak Systems s.r.o.'s Customers.

The Compliance Manual and the procedures contained in it will evolve in accordance with Cloudpeak Systems s.r.o.'s risk profile.

12.3 Risk Client Matrix

Risk Level	Characteristics	Geographical Scope	Source of Capital	Transaction Limits
Prohibited	Entities or individuals under sanctions Clients flagged as medium or high risk but not fulfilling due diligence standards Individuals associated with illicit financing activities	Restricted regions or countries with operational bans Locations under international restrictions	Suspected illegal origin of funds Cash transactions with inadequate documentation	Exceeds approved thresholds Fails to meet compliance checks
High Risk	Individuals with political exposure (PEP) Parties identified in international advisory lists High-income individuals or those with unusual financial behavior Individuals involved in professional gambling activities	Nations flagged on global high-risk lists Territories with significant financial monitoring gaps	Reliance on numerous payment instruments (5 or more) Capital sources triggering concern	Exceeds EUR 10,000 (or equivalent) in deposits or withdrawals over any timeframe
Middle Risk	Individuals generating scrutiny through public presence, media reports, or inconsistent information - Customers with unclear profiles or negative associations	Countries listed for increased vigilance by global AML organizations Areas assessed by internal policies as potentially risky	Use of unconventional payment methods like prepaid cards or vouchers Withdrawal patterns differing from deposits Reliance on three or more payment channels	Transactions surpassing EUR 5,000 (or equivalent) over 30 days
Low Risk	Fully compliant clients without any red flags No history of activities requiring additional checks	Regions without specific regulatory or financial concerns	Standard payment methods such as bank transfers or credit cards Approved financial channels	Within all pre-set thresholds for deposits and withdrawals

Additional Notes:

- ✓ **Each customer is assigned a risk level that determines the extent of due diligence to be performed.**
- ✓ **Monitoring of accounts is continuous, ensuring compliance with the company's AML policies.**
- ✓ **The Compliance Officer evaluates the risk framework annually or as needed when business operations evolve.**

13. Reporting and Monitoring Suspicious Transactions

Cloudpeak Systems s.r.o. follows strict procedures to identify and report suspicious transactions. If a Customer's transaction raises concerns, such as partial or inconclusive sanctions list hits or a partial/full PEP match, the account will be restricted, and the Customer will be asked to provide further information to help determine if the business relationship is required to continue. If the Customer does not respond, the account will remain restricted, and an assessment will be made on whether a suspicious transaction report (STR) is required to be filed.

The MLRO is responsible for ensuring that the company:

- ✓ **Appropriately documents all STR decisions.**
- ✓ **Seeks the FAO's consent to process transactions if suspicion arises before the transaction occurs.**
- ✓ **Files or amends STRs within the FAO's prescribed timeframes.**
- ✓ **Retains appropriate records related to reported activities.**
- ✓ **Complies with all FAO and regulatory STR filing guidelines.**

Employees are prohibited from tipping off customers that they are under investigation or that an STR has been filed. The MLRO ensures that all staff are trained on how to report suspicious activities and on the prohibition of tipping off, as part of the AML/CTF training program. Internal access to STR-related information is restricted to AML/CTF compliance personnel, authorized management, and the Management Board to avoid unnecessary disclosure.

Employees are obligated to report to the MLRO if they know, suspect, or have reasonable grounds to suspect that a person is engaged in money laundering or terrorist financing. This obligation also extends to situations where, in hindsight, the employee is required to have known or suspected money laundering. Any knowledge or suspicion shall be reported promptly.

Common risk indicators include transactions just below due diligence thresholds, those with no apparent economic basis, routing through third parties or tax havens, and false or contradictory information accompanying payments. Structuring—where transactions are broken down to avoid identification or reporting requirements—is also a key red flag.

Suspicion does not require proof but is required to be based on a reasonable foundation, such as unusual or inconsistent transaction patterns, reluctance to provide required information, or efforts to expedite large transactions. Employees is required to be cautious of customers who avoid necessary inquiries or provide insufficient or false information.

Terrorist financing may differ from money laundering in that it often involves lower amounts of money and may use legitimate sources of funds, like donations or businesses. However, similar to money laundering, the aim is to remain undetected, and employees is required to be vigilant for signs of behavior designed to avoid detection.

If an employee suspects suspicious activity or structuring, they shall report it to the MLRO immediately, and such reports is required to be documented. The MLRO shall evaluate the report and decide whether to forward it to the FAO. Employees is required to not inform customers that an STR is being filed (i.e., "tipping off"). All internal inquiries related to a report shall be documented, as this may later serve as evidence for regulatory reviews.

The MLRO will file the STR to the FAO within the required timeframes: within one business day for suspected criminal activity or terrorist financing, within three business hours for suspected suspicious transactions, and immediately if a suspicious transaction is about to take place.

SUSPICIOUS ACTIVITY REPORT

Identification details of the suspicious activity reporter:

- **Reporter:**
  (Enter the full name or the entity's name of the person reporting the suspicious activity)
- **Registered office or place of business:**
  (Provide the full registered office address or place of business of the reporting entity)
- **ID:**
  (Enter the identification or registration number of the reporting entity)
- **Subject of business related to the report:**
  Enter:
  Virtual Assets Services Provider or any other relevant business category.
- **Correspondence address:**
  (Provide the address for correspondence or communication)

Details of the person to whom the report relates:

If the customer is a natural person:

- **Full name:**
  (Enter the full name of the individual)
- **Identification details of the natural person:**
  Fill in the identification data of the individual on the "Identification details of the natural person" page.

If the customer is a legal entity:

- **Trade name or name of the legal entity:**
  (Enter the name or trade name of the legal entity)
- **Identification details of the legal entity:**
  Fill in the identification data of the legal entity on the "Identification details of the legal entity" page.
- **Name and surname of all persons who represented the legal entity in the transaction:**
  (Provide the identification details of each person who represented the legal entity during the transaction)
  Fill in the identification details of these individuals on the "Identification details of the natural person" page.

Description of the object and material circumstances of the suspicious activity:

- **Description of the suspicious activity:**
  Provide a detailed account of the circumstances or facts that raised suspicion regarding the activity or transaction, which may indicate money laundering or terrorist financing. For example, describe any unusual client behavior, anomalous transactions, or suspicious interactions.
- **Key aspects that raised suspicion:**
  Include specific reasons why the client's actions or behavior appear suspicious. This may include unexpectedly large sums of money, lack of clarity about the source of funds, structured payments designed to avoid detection, and other related activities.

List of documents and other materials annexed to this notice:

- **Documents:**
  List all documents attached to the report, such as copies of contracts, invoices, bank statements, identification documents (e.g., passport, ID card), etc.
- **Other materials:**
  List any additional sources of information that support the suspicion, such as internal reports, call records, or email exchanges, if applicable.

Information on whether the execution of the customer's order has been postponed:

- **Postponement of execution:**
  If the execution of the transaction or order has been delayed due to suspicious activity, provide the date, time, and reasons for the delay. For example, delay due to the verification of the source of funds or other concerns.

Contact information and details of the person submitting this report on behalf of the obliged entity:

- **Full name:**
  (Enter the full name of the person submitting the report)
- **Job title:**
  (Job title of the person submitting the report, e.g., Compliance Manager, Risk Officer, etc.)
- **Phone:**
  (Provide the contact phone number for follow-up inquiries)
- **Fax:**
  (Provide the fax number, if applicable)
- **Email:**
  (Provide the email address for communication)
- **Contact outside working hours:**
  (Provide contact details for reaching the person outside of normal working hours)

Date and time of filing of this notice:

- **Date and time:**
  (Enter the exact date and time the report is being filed)

Place of notification:

- **Place:**
  (Enter the location where the report is filed, such as the office, city, country, etc.)

Signature of the Contact Person:

- **Signature:**
  (Signature of the person submitting the report)

This expanded Suspicious Activity Report (SAR) form contains all the necessary fields to collect and submit detailed information regarding suspicious transactions or potentially illegal activities.

14. List of prohibited parties to Cloudpeak Systems s.r.o. transactions

Cloudpeak Systems s.r.o. operates across multiple jurisdictions and is, therefore, subject to the laws and regulations of several countries, including, but not limited to, the Czech Republic. Among the most signifimayt regulations is that enforced by the U.S. Office of Foreign Assets Control (OFAC), which administers a variety of laws that prohibit business dealings with hostile nations and sanctioned or blocked persons. These laws are critical for ensuring that financial institutions do not facilitate or enable activities that violate national security, human rights, or international peace efforts. Severe civil and criminal penalties exist for any violations of these sanctions.

OFAC Lists and International Sanctions: OFAC maintains a comprehensive master list of individuals, entities, and organizations that are blocked from conducting financial or commercial transactions with U.S. entities. These Blocked Persons include individuals or organizations that are linked to activities such as terrorism, money laundering, and those in countries that are subject to U.S. sanctions. Cloudpeak Systems s.r.o. shall adhere strictly to these prohibitions, ensuring that no transactions are made with any person or entity listed on the OFAC List.

OFAC regularly updates its sanctions list**, which includes embargoed nations and blocked parties, and these are available on OFAC's official website at https://sanctionssearch.ofac.treas.gov/. In addition to the OFAC sanctions list, Cloudpeak Systems s.r.o. also checks transactions against other relevant international sanctions lists, which include those maintained by the** United Nations, Australia, Canada, the European Union, the Czech Republic**, and other countries.**

Transaction Screening Process: **Cloudpeak Systems s.r.o. has implemented stringent procedures to ensure that transactions involving blocked or sanctioned entities do not proceed undetected. Before any transaction is authorized, the company's compliance team performs a thorough comparison of the Customer's name and transaction details against the various sanctions lists mentioned above. This process involves cross-referencing the details with the master lists to identify any potential matches with restricted individuals or entities.**

If a match or partial match is detected, the Money Laundering Reporting Officer (MLRO) at Cloudpeak Systems s.r.o. is responsible for reviewing the matched entries and determining whether they are legitimate or false positives. A false positive is a case where the name or details of the entity in question appear similar to those on the sanctions list but do not, in fact, represent a sanctioned party. In these instances, the transaction may be cleared and processed.

Handling True Matches: In cases where a true match with a listed blocked person or entity is confirmed, the transaction maynot proceed without further action. The MLRO is required to report the match to the relevant regulatory authority that maintains the sanctions list in question. Depending on the specific legal requirements, this may include submitting any funds associated with the transaction to the government agency responsible for the sanctions program. In some cases, Cloudpeak Systems s.r.o. may be required to freeze or hold the funds pending further instructions from the regulatory authority.

Before proceeding with any transaction, the company may need to request additional information from the Customer to better assess the situation and determine whether the transaction may be legally processed. This could involve verifying the identity of the parties involved, understanding the purpose of the transaction, or reviewing the source of funds.

Cloudpeak Systems s.r.o. takes a firm stance in adhering to global sanctions regulations and ensuring that all transactions comply with international and national anti-money laundering (AML) and counter-terrorism financing (CTF) laws. The company's robust screening process helps prevent transactions with prohibited parties, reducing the risk of legal repercussions and financial crimes. By continually monitoring and cross-checking against various sanctions lists, Cloudpeak Systems s.r.o. strives to maintain a transparent and legally compliant business environment, safeguarding its operations from inadvertent violations of international law. Furthermore, this diligent approach supports global efforts in combating financial crimes and promoting peace and stability in the international community.

15. Other internal controls and procedures

In addition to the core elements of the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance program, Cloudpeak Systems s.r.o. has implemented a comprehensive range of internal controls and procedures designed to mitigate the risks of illegal financial activities. These controls ensure that the company adheres to relevant laws and regulatory requirements, while maintaining a robust framework for detecting and preventing financial crimes. Below is a detailed overview of the key internal controls and procedures in place at Cloudpeak Systems s.r.o.:

16. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

One of the fundamental components of the company's internal controls is the Customer Due Diligence (CDD) process, which involves thoroughly verifying the identity of customers before any business relationship is established. The following procedures are followed as part of CDD:

- ✓ **Basic Identification: For all customers, basic information such as name, address, date of birth, and identification documents (e.g., passport, national ID, or utility bills) are verified.**
- ✓ **Risk Profiling: Based on the nature of the customer's activities and the geographical regions involved, the company performs a risk assessment. Higher-risk customers are subject to Enhanced Due Diligence (EDD) procedures. This includes more detailed checks, such as:**
- ✓ **A deeper investigation into the source of funds**
- ✓ **Analysis of the customer's business activities**
- ✓ **Verification of the customer's purpose for transactions**
- ✓ **Scrutiny of their relationship with high-risk countries or jurisdictions**
- ✓ **Additional scrutiny of politically exposed persons (PEPs) and their close associates**

Transaction Monitoring and Alerts

Cloudpeak Systems s.r.o. has implemented a robust transaction monitoring system that continuously tracks and analyzes all transactions conducted through its services. The system is designed to flag any unusual or suspicious activity that could potentially involve money laundering or terrorist financing. Key features of this system include:

Real-Time Monitoring: Transactions are monitored in real time for any irregularities or patterns that might indicate fraudulent or illegal activity.

Risk-Based Alerts: Alerts are automatically generated based on certain risk parameters, including:

- ✓ **Transactions that exceed set thresholds**
- ✓ **Transactions involving high-risk countries or entities**
- ✓ **Unusual patterns such as rapid or frequent transactions**
- ✓ **Transactions that do not align with the customer's usual behavior**
- ✓ **Review and Escalation: Once an alert is triggered, the compliance team reviews the transaction. If the transaction is deemed suspicious, it is escalated to the Money Laundering Reporting Officer (MLRO) for further investigation.**

Employee Training and Awareness

One of the core principles of any successful AML/CTF program is ensuring that employees are adequately trained and equipped to recognize suspicious activities and report them in a timely and accurate manner. Cloudpeak Systems s.r.o. conducts the following employee training programs:

- ✓ **AML/CTF Awareness: All employees, regardless of their role, receive basic AML/CTF awareness training. This includes recognizing red flags, understanding the company's internal reporting procedures, and being familiar with the legal implications of money laundering and terrorist financing.**
- ✓ **Specialized Training for Compliance Staff: Employees working in compliance-related roles undergo specialized training, which covers topics such as risk assessment, transaction monitoring, handling suspicious activity reports (SARs), and adherence to regulatory requirements.**
- ✓ **Ongoing Education: Training is not a one-time event. Regular updates and refresher courses are conducted to keep employees informed about changes in regulations, emerging risks, and best practices in compliance.**

Reporting and Record-Keeping Procedures

Cloudpeak Systems s.r.o. ensures that proper record-keeping and reporting mechanisms are in place to comply with regulatory obligations. The company is committed to maintaining detailed records of all transactions, customer due diligence information, and any reports related to suspicious activities. These records are securely stored for a prescribed period as required by law. Key aspects of the reporting and record-keeping process include:

Transaction Records: All financial transactions are logged, and the relevant details are stored in a secure, auditable manner.

Suspicious Activity Reports (SARs): If a suspicious transaction is detected, it is immediately reported to the Financial Analytical Office (FAO) or other relevant regulatory authorities. These reports are carefully documented and tracked throughout the investigation process.

Retention of Records: All documents related to customer identification, transaction history, and suspicious activity reports are retained for the legally mandated period, typically five years. These records may be accessed for audit or regulatory inspection when required.

Independent Audits and Reviews

To ensure the effectiveness and integrity of the AML/CTF program, independent audits are conducted regularly by external or internal auditors. These audits evaluate the following:

- ✓ **The effectiveness of the company's AML/CTF controls and procedures**
- ✓ **The adequacy of employee training programs**
- ✓ **Compliance with internal policies and legal requirements**
- ✓ **The company's ability to detect and prevent illicit activities**
- ✓ **The implementation of corrective actions based on prior audits or inspections**

The results of these audits are reviewed by the senior management and any necessary corrective actions are taken promptly.

Whistleblower Protection Mechanism

Cloudpeak Systems s.r.o. is committed to fostering a transparent and ethical environment where employees feel empowered to report any concerns or violations without fear of retaliation. A whistleblower policy is in place to protect employees who report suspicious activities or breaches of compliance. This ensures:

- ✓ **Confidentiality for the whistleblower**
- ✓ **Protection against retaliation or discrimination**
- ✓ **Clear procedures for reporting concerns internally**
- ✓ **A safe and supportive environment for addressing potential issues**

Management Oversight and Governance

The Management Board of Cloudpeak Systems s.r.o. plays an active role in overseeing the effectiveness of the company's compliance program. Regular meetings are held to review compliance reports, audit findings, and any emerging risks. The board ensures that the AML/CTF program is adequately resourced and that sufficient measures are in place to mitigate risks.

- ✓ **Board-Level Responsibility: Senior management is ultimately responsible for ensuring that the company adheres to regulatory requirements, implements best practices, and maintains an effective compliance program.**
- ✓ **Oversight Committees: Specialized committees, such as the Compliance Committee and Risk Committee, assist the board in overseeing specific areas of compliance and risk management.**

Risk-Based Approach

Cloudpeak Systems s.r.o. follows a risk-based approach to its AML/CTF efforts, which means resources and attention are focused on higher-risk areas where the likelihood of illicit activity is greater. This includes:

- ✓ **Enhanced scrutiny for customers from high-risk jurisdictions or industries**
- ✓ **Additional monitoring for high-value transactions or complex business structures**
- ✓ **Proactive identification of emerging risks and updating internal controls accordingly**

By adopting a dynamic, risk-based approach, the company ensures that its resources are allocated efficiently, focusing on areas of higher potential risk.

Cloudpeak Systems s.r.o. has put in place a wide range of internal controls and procedures to prevent money laundering and terrorist financing. These procedures cover all aspects of customer interaction, from the initial onboarding process to the continuous monitoring of transactions. The company's commitment to employee training, rigorous record-keeping, independent audits, and robust reporting mechanisms ensures that it remains compliant with both domestic and

international regulatory requirements. By continuously evaluating and updating its controls and practices, Cloudpeak Systems s.r.o. may effectively manage emerging risks and maintain a strong reputation for compliance and integrity in its operations.

17. Exercise of Audit: Detailed Description

The exercise of audit serves as a fundamental internal control mechanism for ensuring the effectiveness and compliance of a company's Anti-Money Laundering (AML) policies and procedures. This process is essential for monitoring adherence to regulatory standards, identifying potential breaches, and safeguarding the company against risks related to money laundering and terrorist financing (ML-FT). Below is a detailed breakdown of the steps involved in the exercise of audit as outlined in the document.

Responsibility of the Statutory Body

The Statutory Body (typically the board of directors or other governing entity of the company) holds the primary responsibility for ensuring that the company complies with its AML policies and procedures. This body is tasked with:

- **Overseeing Compliance: The Statutory Body shall continuously monitor the implementation and enforcement of the AML regulations within the company to ensure that all processes are being followed properly.**
- **Delegation of Control: While the Statutory Body is ultimately responsible for compliance, it may delegate certain aspects of the audit and control processes to an Authorised Person. This delegation ensures that audits may be carried out effectively and on time, allowing the Statutory Body to focus on strategic and high-level decision-making.**

Obligations of Responsible Persons

The Responsible Persons, or employees designated with compliance-related duties (such as the AML Officer, Risk Manager, or MLRO), are required to undergo internal audits regularly. These individuals shall provide complete access to necessary data and documents to facilitate the audit process. This includes:

- **Providing Data and Documentary Evidence: Responsible Persons shall ensure that all records related to their activities are available for inspection by the internal auditor. This data may include transaction records, customer identification files, due diligence reports, and any other relevant documents related to AML compliance.**

Regularity and Methodology of the Audit

- **Frequency: The internal audit shall be conducted regularly, ideally once per quarter, to maintain ongoing monitoring and ensure that any compliance issues are identified in a timely manner.**
- **Selection of Audit Sample: The auditor shall select an audit sample for each review period. This sample serves as a representative subset of the company's business activities during the audit period. The preferred approach is to examine all business relationships or services rendered during the audit period, as this would provide the most comprehensive insight into the company's compliance. However, given resource constraints, a random sample is typically used, which remains effective in providing a reasonable assurance of overall compliance.**

Protocol on Internal Audit

Once the audit has been completed, the individual conducting the audit (referred to as the auditor) shall create a detailed record of the audit. This audit protocol document serves as a formal report of the findings, including:

- **Audit Findings: Documentation of the audited areas, the sample selection, and the results of the compliance checks.**
- **Non-Conformance: If any non-compliance or breach is discovered during the audit, the auditor shall record these findings and recommend corrective actions.**
- **Audit Recommendations: Suggestions for improvements, whether they involve revising procedures, enhancing training, or implementing new controls.**

The draft of this protocol is typically provided as a template in a dedicated chapter (in this case, Chapter 16), making it easier for those responsible for audits to ensure consistency and compliance with the procedure.

Detection of Violations

Any employee or person within the company who identifies a violation of AML regulations or internal procedures shall report it immediately to the Authorised Person in charge of compliance oversight. This includes breaches that might have been caused by the individual making the discovery.

- **Immediate Reporting: The violation is required to be reported as soon as it is identified. The Authorised Person is responsible for evaluating the situation and determining the necessary course of action.**
- **Protection and Accountability: Whistleblowers who report violations shall be protected from retaliation, ensuring that employees are encouraged to speak up without fear of negative consequences.**

Assessment of the Violation and Further Action

Upon identifying a violation of the AML policies, it is necessary to assess the severity and impact of the breach. The process for this assessment includes:

- **Severity of the Violation: The level of severity refers to how serious the violation is in terms of its potential impact on the company's compliance with AML/CTF regulations and the risk it poses to the company's legal standing.**
    - **For example, a minor procedural lapse (such as a clerical error in documentation) may be categorized as a lower-severity violation, while signifimayt violations (such as intentional money laundering or failure to report suspicious activities) would be classified as high-severity.**
- **Potential Impact on AML Measures: The assessment is required to also include an evaluation of how the violation could undermine the effectiveness of the company's AML measures. If the breach compromises the integrity of the company's compliance system, more immediate corrective action will be needed.**
- **Personal Liability: Depending on the nature of the breach, personal liability may be incurred by those responsible, especially if the violation results from negligence, willful misconduct, or failure to follow procedures. The extent of liability will be governed by applicable labour law and internal company policies.**
- **Preventative Measures: To prevent a recurrence of similar violations, the Statutory Body is required to take appropriate measures, such as:**
    - **Retraining the responsible staff members**
    - **Revising internal procedures or policies**
    - **Implementing corrective actions based on the audit findings**

Consequences of Breaking the Rules

It is vital for all employees and stakeholders to understand that any violation of the AML rules and procedures could lead to serious consequences for both the individual involved and the company as a whole. The potential consequences include:

- ✓ **Legal and Regulatory Penalties: A breach of AML regulations could result in severe penalties, such as financial sanctions or even the revocation of the company's business license.**
- ✓ **Reputational Damage: Beyond legal consequences, violations may damage the company's reputation, affecting its relationships with customers, regulators, and other stakeholders.**
- ✓ **Disciplinary Action: Employees who are found responsible for violating AML procedures may face disciplinary actions, including termination, depending on the severity of the violation and the circumstances involved.**
- ✓ **Awareness of Risk: All employees and company stakeholders are made aware that violating the rules and procedures will most likely result in violating the provisions of the AML Act, which may trigger sanctions and regulatory scrutiny.**

The exercise of audit is a crucial part of Cloudpeak Systems s.r.o.'s internal control framework for ensuring AML compliance. Regular audits, effective detection of violations, and clear protocols for corrective action help maintain the integrity of the company's operations. A systematic approach to assessing breaches ensures that the company may address issues promptly and strengthen its AML practices. By making employees aware of the consequences of breaking the rules, the company fosters a culture of compliance and accountability, reducing the risks associated with financial crimes and regulatory non-compliance.

INTERNAL AUDIT PROTOCOL

This protocol serves as a comprehensive framework for auditing the compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies. The form provided below is required to be used to document and track the internal audit of the company's adherence to these policies and practices. It is intended to be used as a guide for auditing compliance and may be reproduced for this purpose as required.

Obliged Person:
(Please provide the full name of the individual or department being audited)

Date of Audit:
(Insert the date on which the audit was conducted)

Subject of the Audit:
The audit covers compliance with the obligations outlined in the System of Internal Policies and Procedures designed to prevent Money Laundering and Terrorist Financing. This includes adherence to the following:

- **The Money Laundering Risk Assessment and associated risk management processes.**
- **Compliance with Act No. 253/2008 Coll. on measures against the legalization of criminal proceeds and terrorist financing (as amended), and any other relevant sub-legal regulations.**
- **Act No. 69/2006 Coll. regarding the implementation of international sanctions (as amended).**
- **Other applicable laws, guidelines, and regulations, including those related to anti-money laundering (AML), counter-terrorist financing (CTF), and international sanctions.**

Person Who Carried Out the Audit:
(Full name and position of the individual conducting the audit)

Description of the Controlled Sample:
The sample being audited is required to be described here, including the scope, timeframe, and selection process. For example:

- **A random selection of transactions within the last quarter.**
- **A review of customer due diligence (CDD) records for specific high-risk accounts.**
- **Verification of the implementation of internal controls or any specific procedures deemed critical for AML/CTF compliance.**

Audit Procedure:

- **Details of the audit approach, including any checklists, tests, or other tools used to assess compliance.**
- **If applicable, describe any interviews, document reviews, or system checks carried out during the audit process.**

Result of the Audit:

- **Summarize the findings of the audit here. This is required to include:**
  - **Compliance status (e.g., fully compliant, partial compliance, non-compliant).**
  - **Any discrepancies or issues identified during the audit.**
  - **Effectiveness of internal controls in preventing money laundering or terrorist financing.**
  - **Recommendations for further actions, if necessary.**

Imposing Corrective Measures:

- **Based on the audit findings, list any corrective actions that shall be taken to address non-compliance or other issues. These measures is required to be specific and measurable, such as:**
  - **Updating or revising internal policies and procedures.**
  - **Providing additional training to staff on AML/CTF protocols.**
  - **Enhancing monitoring mechanisms or reviewing transaction patterns for suspicious activity.**
  - **Making changes to internal reporting procedures or escalating systems.**

Follow-up Actions:

- **Outline any follow-up actions required to ensure that corrective measures are implemented effectively. Include timelines for resolution and responsible parties.**

Signature of the Controller:
(Signature of the individual conducting the audit, followed by their printed name, title, and date of signature)

Management Review:

- **The audit results and corrective actions is required to be reviewed and signed off by senior management or the designated compliance officer to ensure proper oversight. This section is required to include a review date and any comments or approvals from the management.**

EMPLOYEE TRAINING PROTOCOL

pursuant to Section 23 of Act No. 253/2008 Coll. on certain measures against the legalisation of proceeds of crime and terrorist financing

Obliged person:	
Date of training:	
Content of the training:	• **introduction - legislation governing this area** • **definition of beneficial owner, politically exposed person and controlling person** • **identification procedure (first and subsequent updates of identification data)** • **customer due diligence procedure (initial before establishing a business relationship and ongoing CDD)** • **determining whether a customer is a politically exposed person and the procedures for doing so** • **verification of international sanctions, applicable sanctions lists, procedure for verification of international sanctions and procedure in case the Czech Republic applies international sanctions against the customer** • **prohibition to conduct business or establish a business relationship - situation and procedure, follow-up to the evaluation of suspicious activity** • **compiling and updating the risk profile, customer acceptability rules** • **risk assessment** • **the typology of suspicious activities and the list of characteristics of a suspicious activity and its assessment** • **other aspects of assessing suspicious activities** • **procedures in case of detection of suspicious activity** • **postponing the execution of the customer's order** • **information on the Authorised Person and Contact Person** • **duty of confidentiality** • **record-keeping obligation (time, method)** • **inspection and detection of breaches of obligations**

Name of the person:	**Signature:**

Name of the trainer who conducted the training:	**Signature:**

Document Name	**System of internal policies and rules of procedures to prevent money laundering & counter-terrorist financing procedures & anti-bribery policy**
Money Laundering Repoting Officer	**Hovsep Kocharyan**
Money Laundering Reporting Officer Signature:	
Authorised by Director	**Artur Tiunov**
Distribution Date	**17.03.2026**
Director Signature	

18. Annex 1 - List of Prohibited & Risk Level Countries

To evaluate a customer's risk profile from the perspective of money laundering and terrorist financing (ML/TF), Cloudpeak Systems s.r.o. applies a country/geo-risk methodology that combines:
- internal risk assessment;
- lists of high-risk third countries identified by the European Commission under Article 9 of Directive (EU) 2015/849 (as amended); and
- FATF public statements on "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring".

Countries are categorised into three main groups:
- Prohibited – countries with which Cloudpeak Systems s.r.o. will not establish or will terminate business relationships, except in strictly limited circumstances approved by the Board and MLRO.
- High-Risk – countries where any nexus (customer domicile, place of business, main operating market, beneficial owner, key counterparties) leads to classification of the customer as high-risk and triggers Enhanced Due Diligence (EDD).
- Low-Risk – countries with strong AML/CFT frameworks and low systemic corruption risk.

The classification below is based on:
- the list of high-risk third countries identified by the European Commission (e.g. Commission Delegated Regulation (EU) 2016/1675, as updated);
- FATF public statements as of October 2025;
- the resolution of the Czech Parliament designating the current Russian regime as terrorist (Russia treated as high-risk third country under Section 9(1)(a)(3) of the AML Act); and
- Cloudpeak Systems s.r.o.'s internal risk assessment. Where:
- a country appears on the FATF "Call for Action" list, it shall, at a minimum, be classified as Prohibited; and
- a country appears on the FATF "Increased Monitoring" list, it shall, at a minimum, be classified as High-Risk.

The MLRO must review this Annex at least annually and after each FATF or European Commission update to ensure consistency with current external lists and internal risk appetite. Act No. 253/2008 Coll., which outlines measures against the laundering of proceeds of crime and terrorist financing, mandates the evaluation of customers associated with high-risk countries. These countries are identified by the European Commission (EC), the Financial Action Task Force (FATF), or other authoritative bodies.

When determining high-risk countries, the Company takes into account, in particular:

- the list of high-risk third countries identified by the European Commission under Article 9 of Directive (EU) 2015/849, as implemented and regularly updated by Commission Delegated Regulations (including Commission Delegated Regulation (EU) 2016/1675 and its subsequent amendments);

- the most recent FATF public statements on "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring", as published on the FATF website; and

- the resolution of the Chamber of Deputies of the Parliament of the Czech Republic of 15 November 2022 designating the current Russian regime as terrorist, as a result of which Russia is treated as a high-risk third country under Section 9(1)(a)(3) of the AML Act.The lists published by the EU and FATF play a vital role in evaluating customer risk, assessing transactions, and maintaining business relationships. If a customer's country of origin or associated activities are connected to any jurisdiction listed in these documents, heightened diligence is required. This may involve intensified monitoring, refusal to proceed with a transaction or establish a relationship, terminating existing relationships, or filing a report of suspicious activity.

Risk Level	Countries/Regions
Prohibited	**Abkhazia, Afghanistan, American Samoa, Akrotiri and Dhekelia, Antarctica, Artsakh, Barbados, Botswana, Burkina Faso, Burundi, Cambodia, Cameroon, Central African Republic, Cuba, Democratic Republic of Congo, Crimea Region (Ukraine), Eastern Ukraine, Ethiopia, Haiti, Hawaii, Heard Island and McDonald Islands, Fiji, Guam, Iran, Iraq, Kosovo, Lebanon, Libya, Luhansk People's Republic, Mali, Mozambique, Myanmar, Nicaragua, Nigeria, North Korea, Pakistan, Palau, Palestinian Territories, Samoa, Senegal, Somalia, South Ossetia, South Sudan, Sudan, Syria, Transnistria, Trinidad and Tobago, US Minor Outlying Islands, US Virgin Islands, United States, Uganda, Venezuela, Western Sahara, Yemen, Zimbabwe, Belarus, Russia.**
High-Risk	**Åland Islands, Albania, Algeria, Angola, Anguilla, Antigua and Barbuda, Argentina, Armenia, Aruba, Azerbaijan, Bahamas, Bahrain, Bangladesh, Belize, Benin, Bermuda, Bhutan, Bolivia, Bosnia and Herzegovina, Brazil, British Indian Ocean Territory, Brunei, Bulgaria, Canada, Canary Islands, Cape Verde, Cayman Islands, Cyprus, Chad, Chile, China, Colombia, Comoros, Costa Rica, Croatia, Curaçao, Djibouti, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Eswatini, Falkland Islands, Faroe Islands, Gabon, Gambia, Georgia, Ghana, Greenland, Grenada, Guatemala, Guinea, Guinea-Bissau, Guyana, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Israel, Ivory Coast, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kiribati, Kuwait, Kyrgyzstan, Laos, Lesotho, Liberia, Liechtenstein, Madagascar, Malawi, Malaysia, Maldives, Malta, Marshall Islands, Mauritania, Mauritius, Mexico, Moldova, Monaco, Mongolia, Montenegro, Morocco, Namibia, Nepal, New Caledonia, New Zealand, Niger, North Macedonia, Oman, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Qatar, Rwanda, Saudi Arabia, Seychelles, Sierra Leone, Solomon Islands, South Africa, Sri Lanka, Suriname, Tajikistan, Tanzania, Thailand, Timor-Leste, Togo, Tonga, Tunisia, Turkey, Turkmenistan, Tuvalu, Ukraine, United Arab Emirates, Uruguay.**
Low-Risk	**Australia, Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom of Great Britain and Northern Ireland.**

19. Annex 2 - The Current List of Jurisdictions with Strategic Deficiencies

This Annex refers to jurisdictions with significant gaps in their anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) frameworks, as identified by the Financial Action Task Force (FATF). Such countries are subject to either:

- a call for action ("high-risk jurisdictions"), or
- increased monitoring ("grey-list jurisdictions").

Cloudpeak Systems s.r.o. does not hard-code specific FATF lists in this Manual. Instead, the Company always refers to the most recent FATF public statements available on the FATF website and updates its internal country-risk classification and controls accordingly.

As of the latest FATF public statements, the structure of jurisdictions with strategic deficiencies is as follows:

1.High-Risk Jurisdictions Subject to a Call for Action ("FATF black list") These are jurisdictions for which the FATF calls on all members and all jurisdictions to apply enhanced due diligence measures, and in the most serious cases, counter-measures, to protect the international financial system from the risks of money laundering, terrorist financing and proliferation financing.

Cloudpeak Systems s.r.o.:
- normally does not enter into or maintain business relationships with customers having any nexus (residence, incorporation, business operations, ownership, transactional flows) to such jurisdictions; and
- where an existing nexus is identified, applies the most stringent restrictions, including immediate review of the relationship by senior management, suspension of transactions, and, where appropriate, termination of the relationship and filing of a suspicious activity report.

The current list of high-risk jurisdictions is available in the FATF statement "High-Risk Jurisdictions subject to a Call for Action", published on the FATF website.

2. Jurisdictions Under Increased Monitoring ("FATF grey list")
These are jurisdictions that are actively working with the FATF to address strategic deficiencies in their AML/CFT/CPF regimes within agreed timeframes and are therefore subject to increased monitoring.

Cloudpeak Systems s.r.o.:
- treats any customer with a nexus to such jurisdictions as high-risk in its internal risk-assessment methodology;
- always applies Enhanced Due Diligence (EDD), including a deeper understanding of the customer's business model, ownership structure, and source of funds/wealth; and
- performs more frequent and more granular ongoing monitoring of transactions and customer behaviour.The current list of jurisdictions under increased monitoring is available in the FATF

statement "Jurisdictions under Increased Monitoring", published on the FATF website.

3. Interaction with EU High-Risk Third Countries and National Measures
In addition to FATF lists:
- the Company aligns its country-risk framework with the list of high-risk third countries identified by the European Commission under Article 9 of Directive (EU) 2015/849 and its implementing Delegated Regulations (including Commission Delegated Regulation (EU) 2016/1675 and its subsequent amendments); and
- the Company applies any additional national measures adopted by the Czech Republic, including the treatment of Russia as a high-risk third country pursuant to Section 9(1)(a)(3) of the AML Act, following the resolution of the Chamber of Deputies of 15 November 2022 designating the current Russian regime as terrorist.

4. Operational Use The MLRO is responsible for:
- ensuring that the latest FATF and EU lists are reflected in the Company's screening systems and country-risk ratings;
- documenting any changes to internal country categorisation and communicating them to relevant teams (KYC/onboarding, Risk, Operations, Product); and
- ensuring that the Company's internal methodology and controls remain aligned with the most recent FATF public statements and EU law. For day-to-day operations, staff shall always refer to the latest versions of:
- FATF "High-Risk Jurisdictions subject to a Call for Action;
- FATF "Jurisdictions under Increased Monitoring"; and
- the European Commission list of high-risk third countries.

20. Annex 3 – FATF's Forty [40] Recommendations (AML)

The FATF Forty Recommendations constitute the globally recognised standard for anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF). Cloudpeak Systems s.r.o. designs and maintains its AML/CFT/CPF framework in line with these recommendations, in particular with respect to the risk-based approach to ML/TF risk management (Recommendation 1), national and institutional risk assessment and coordination (Recommendations 1–2), customer due diligence and beneficial-ownership transparency (Recommendations 10, 24 and 25), record-keeping (Recommendation 11), reporting of suspicious transactions (Recommendation 20), internal controls, foreign branches and subsidiaries (Recommendation 18), and the regulation and supervision of virtual asset service providers (VASPs) and other DNFBPs (Recommendation 15 and the relevant Interpretive Notes).

Cloudpeak Systems s.r.o. periodically compares its policies and procedures with the current FATF standards and the relevant FATF Guidance for a risk-based approach to virtual assets and VASPs.

The full, up-to-date text of the FATF Recommendations is available at: https://www.fatf-gafi.org/en/topics/fatf-recommendations.html.

1. High-Risk Jurisdictions subject to a Call for Action ("Black List")

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation financing (ML/TF/PF). For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence (EDD) and, in the most serious cases, counter-measures to protect the international financial system.

As of October 2025, the following jurisdictions are subject to a FATF Call for Action ("black list"):

- Democratic People's Republic of Korea (DPRK)

- Iran

- Myanmar

For these jurisdictions Cloudpeak Systems s.r.o. will, as a minimum:

-prohibit onboarding of new customers domiciled in, or ultimately owned/controlled from, these jurisdictions;

- apply the highest level of EDD and continuous monitoring to any existing relationships with any nexus to these jurisdictions;

- consider the application of additional risk-mitigation measures, including the refusal or termination of business relationships, where legally permitted.

2. Jurisdictions under Increased Monitoring ("Grey List")

Jurisdictions under increased monitoring are actively working with FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation financing. This list is commonly referred to as the "grey list". FATF does not call for automatic de-risking, but for a risk-based approach and appropriate EDD. As of October 2025, the following jurisdictions are subject to increased monitoring:

- Algeria

- Angola

- Bulgaria

- Burkina Faso

- Cameroon

- Côte d'Ivoire

- Croatia

-Democratic Republic of the Congo

- Haiti

- Kenya

- Lao PDR

- Lebanon

- Mali

- Monaco

- Mozambique

- Namibia

- Nepal

- Nigeria

- South Africa

- South Sudan

- Syria

- Tanzania

- Venezuela

- Vietnam

- Yemen

For customers or transactions with a nexus to "grey list" jurisdictions, Cloudpeak Systems s.r.o. will:

- treat such customers as at least "high risk" in the internal risk-rating methodology, unless there are strong mitigating factors;

- apply EDD measures, including obtaining detailed information on source of funds and source of wealth, purpose and nature of the business relationship, and transaction patterns;

- increase the frequency and depth of ongoing monitoring, including periodic KYC file refresh and adverse-media screening.

3. Ongoing Maintenance

The MLRO is responsible for:
- monitoring FATF publications and promptly identifying any additions/removals from the “black” and “grey” lists;
- ensuring that this Annex, the internal country-risk matrix and the list of prohibited / high-risk countries (Annex 1) are aligned with the latest FATF statements, EU and national (Czech) regulatory requirements;
- ensuring that relevant changes are communicated to all impacted teams (e.g. Onboarding, Operations, Risk, Product) and reflected in screening tools and rule-based transaction-monitoring scenarios.

21. Annex 4 – FATF's Nine [9] Special Recommendations (CTF)

These are specific recommendations aimed at combating terrorist financing, and are integral for ensuring that businesses do not inadvertently facilitate terrorist activities.

Key FATF Recommendations (CTF)

Recommendation	Description
1. Criminalizing Terrorist Financing	**Terrorist financing should be criminalized under national law.**
5. International Cooperation	**Nations should cooperate on investigations of terrorist financing.**
8. Freezing Terrorist Assets	**Financial institutions must freeze assets linked to terrorists.**

22. Annex 5 – Sanctions Lists

This annex includes relevant sanction lists imposed by international bodies like the United Nations (UN), the European Union (EU), and the US (OFAC) to restrict dealings with individuals, entities, and countries involved in financial crimes or terrorism.

Sanctions Overview:

Sanctions are legal measures used by international communities to stop financial crime and terrorism. They are designed to modify the behavior of targeted countries, regimes, or individuals, especially when diplomatic means have failed. These measures typically include economic, trade, and financial service restrictions, as well as travel bans.

UN Sanctions:

The United Nations Security Council maintains a list of individuals and organizations subject to financial sanctions due to their involvement with ISIL (Da'esh), Al-Qaeda, and the Taliban. All UN member states are legally required to freeze the assets and economic resources of individuals and entities listed in this list and to report any matches to relevant authorities. The UN also has additional sanction lists that cover other jurisdictions, entities, and individuals involved in broader terrorist activity under UNSR 1373.
UN Consolidated Sanctions List:
UN SC Consolidated List

EU Sanctions:

The European Union imposes sanctions as part of its Common Foreign and Security Policy (CFSP), which is based on the objectives set out in the Treaty of the European Union. These sanctions may be based on UN Security Council measures or may be autonomous, depending on the specific EU foreign policy aims. It is important to note that EU autonomous sanctions maynot be imposed on individuals or entities unless there is a foreign policy dimension.
EU Sanctions Regimes:
SanctionsMap
This site also includes information on UN sanctions regimes.

OFAC Sanctions:

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury enforces economic and trade sanctions that align with US foreign policy and national security goals. These sanctions target foreign countries, regimes, terrorists, international drug traffickers, entities involved in the proliferation of weapons of mass destruction, and other national security threats. While US sanctions typically apply to US citizens and companies, the use of US dollars in international transactions connects non-US entities to OFAC regulations. OFAC publishes a list of "Specially Designated Nationals" (SDNs), whose assets are blocked, and US persons are generally prohibited from doing business with them.
OFAC SDN List:
OFAC Sanctions List Search

UK Sanctions:

The UK imposes sanctions on individuals, companies, and countries that appear on its sanctions list. Transactions with such entities are prohibited.
UK Sanctions List:
Office of Financial Sanctions Implementation

Other Sanction Sources:

- ✓ **EU Sanctions Map: Provides an up-to-date map of countries under EU sanctions.**
- ✓ **OFAC Search Database: Used to identify SDNs and blocked persons.**
- ✓ **Ministry of Foreign Affairs of the Czech Republic: Official data on sanctions against various entities and countries.**
- ✓ **Consolidated EU Financial Sanctions List: Contains individuals, groups, and entities subject to financial sanctions within the EU.**
- ✓ **OpenSanctions: A repository for open-source sanction data, useful for due diligence.**
- ✓ **Sanction List Search - OFAC, UN, EU, HMT: Provides access to a range of international sanctions lists.**
- ✓ **UK Financial Sanctions - Office of Financial Sanctions Implementation (OFSI): The UK's official portal for financial sanctions implementation.**
- ✓ **EU Sanctions Login: Login portal for EU sanctions data files.**
- ✓ **UN Sanctions Search: Allows searches of the UN sanctions list.**
- ✓ **US Consolidated Sanctions List Data Files: Consolidated US sanctions data, available for download.**
- ✓ **UK Sanctions List: Consolidated UK sanctions data**

Please note that not all sanctions lists have been saved or retained. All sanction lists need to be preserved for proper monitoring and compliance.

Overall, the provided internal policies and procedures of the company regarding anti-money laundering (AML) and counter-terrorist financing (CTF) have a clearly defined structure and control system aimed at ensuring compliance with legal requirements. In addition to the regular auditing and monitoring of the implementation of regulatory procedures, key elements include the identification of risks associated with high-risk clients, as well as the integration of international sanctions lists and lists of countries recognized as high-risk for money laundering and terrorism financing. An important aspect is the use of individual risk assessments, which allows for taking into account the specific nature of each client and adequately assessing their risk level.

The policies also emphasize the importance of employee training and ensuring proper documentation regarding the sources of funds and other aspects that contribute to improving efficiency and transparency in the fight against financial crimes. Given the complexity and variety of international regulations, the company ensures the fulfillment of all obligations regarding client verification and financial transactions through the use of sanctions lists and relevant international standards.

Thus, the company has a comprehensive policy that covers not only internal control procedures but also continuous adaptation to international changes in the AML/CTF field, ensuring its compliance with modern security requirements and the prevention of financial crimes.

23. Annex 6 – Source of Wealth/Funds

The Company prohibits online gaming or depositing funds for online gaming purposes unless the participant has: Registered with the company via the registration page on the respective domain operating under the gaming license, created an account, and confirmed their acceptance of the terms and conditions.

A list of examples of relevant information and/or supporting documentation required to verify the Source of Wealth and Funds:

Source of funds/wealth	Information / Documents that may be required
Employment Income	➢ Nature of employer's business ➢ Name and address of the employer ➢ Annual salary and bonuses for the last couple of years ➢ Last month/recent pay slip ➢ Confirmation from the employer of annual salary ➢ Latest accounts or tax declaration if self employed
Savings / deposits	➢ Bank statement and enquiry of the source of wealth
Property Sale	➢ Details of the property sold (i.e. address, date of sale, sale value of property sold, parties involved) ➢ Copy of contract of sale ➢ Title deed from land registry
Sale of shares or other investment	➢ Copy of contract ➢ Sale value of shares sold and how they were sold (i.e. name of stock exchange) ➢ Statement of account from agent ➢ Transaction receipt/confirmation ➢ Shareholder's certificate ➢ Date of sale
Loan	➢ Loan agreement ➢ Amount, date and purpose of loan ➢ Name and address of Lender ➢ Details of any security
Company Sale	➢ Copy of the contract of sale ➢ Internet research of Company Registry ➢ Name and Address of Company ➢ Total sales price ➢ Clients' share participation ➢ Nature of business ➢ Date of sale and receipt of funds ➢ Media coverage

Company Profits / Dividends	➢ Copy of latest audited financial statements ➢ Copy of latest management accounts ➢ Board of Directors approval ➢ Dividend distribution ➢ Tax declaration form
Inheritance	➢ Name of deceased ➢ Date of death ➢ Relationship to client ➢ Date received ➢ Total amount ➢ Solicitor's details ➢ Tax clearance documents
Gift	➢ Date received ➢ Total amount ➢ Relationship to client ➢ Letter from donor explaining the reason for the gift and the source of donor's wealth ➢ Certified identification documents of donor ➢ Donor's source of wealth
Maturity/surrender of life policy	➢ Amount received ➢ Policy provider ➢ Policy number/reference ➢ Date of surrender
Other income sources	➢ Nature of income, amount, date received and from who ➢ Appropriate supporting documentation