

ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის საჯარო პოლიტიკა

საჯარო მოკლე ვერსია

წინამდებარე დოკუმენტი წარმოადგენს შპს „სითი ფეის“ (შემდგომ - „კომპანია“), როგორც ვირტუალური აქტივის მომსახურების პროვაიდერის, ფულის გათეთრების, ტერორიზმის დაფინანსებისა და მასობრივი განადგურების იარაღის გავრცელების დაფინანსების პრევენციისა და აღკვეთის შიდა პოლიტიკის საჯარო მოკლე ვერსიას. მისი მიზანია კლიენტებსა და პარტნიორებს გააცნოს კომპანიის ძირითადი AML/CFT/PF პრინციპები და კონტროლის მიმართულებები.

1 მიზანი და მოქმედების სფერო

კომპანია ახორციელებს საქმიანობას საქართველოს მოქმედი AML/CFT კანონმდებლობის, საქართველოს ეროვნული ბანკისა და საქართველოს ფინანსური მონიტორინგის სამსახურის სავალდებულო მოთხოვნების შესაბამისად. პოლიტიკა ვრცელდება კომპანიის კლიენტებზე, მათ ბენეფიციარ მესაკუთრეებსა და წარმომადგენლებზე, პროდუქტებზე, მომსახურებებზე, ტრანზაქციებზე, მიწოდების არხებზე, თანამშრომლებსა და პარტნიორულ ურთიერთობებზე.

2 რისკზე დაფუძნებული მიდგომა

კომპანია განსაზღვრავს და აფასებს კლიენტთან, ბენეფიციარ მესაკუთრესთან, იურისდიქციასთან, საქმიანობასთან, პროდუქტთან, მომსახურებასთან, ტრანზაქციასთან, ტექნოლოგიასა და პარტნიორ პროვაიდერთან დაკავშირებულ ML/TF/PF და სანქციურ რისკებს. გამოვლენილი რისკების სამართავად გამოიყენება რისკის დონის შესაბამისი და პროპორციული ზომები.

კლიენტის რისკი ფასდება საქმიანი ურთიერთობის დამყარებამდე და გადაიხედება ურთიერთობის განმავლობაში, მათ შორის კლიენტის მონაცემების, საქმიანობის, ტრანზაქციული ქცევის ან სხვა მნიშვნელოვანი რისკ-ფაქტორის ცვლილებისას. ახალი პროდუქტის, მომსახურების, ტექნოლოგიის ან მიწოდების არხის დანერგვამდე კომპანია წინასწარ აფასებს შესაბამის რისკებს და განსაზღვრავს მათი შემცირების ზომებს.

3 კლიენტის შესწავლა

კანონმდებლობით გათვალისწინებულ შემთხვევებში კომპანია:

- ახდენს კლიენტის, მისი სახელით მოქმედი პირისა და ხელმძღვანელობითი ან წარმომადგენლობითი უფლებამოსილების მქონე პირის იდენტიფიკაციასა და ვერიფიკაციას;
- ადგენს იურიდიული პირის მფლობელობისა და კონტროლის სტრუქტურას და განსაზღვრავს მის საბოლოო ბენეფიციარ მესაკუთრეს;
- ადგენს საქმიანი ურთიერთობის მიზანსა და განზრახულ ხასიათს, მოსალოდნელი ოპერაციების პროფილს და, საჭიროების შემთხვევაში, ქონების, შემოსავლის, ფულადი სახსრების ან ვირტუალური აქტივის წარმომავლობას;
- ამოწმებს შესაბამის პირებს პოლიტიკურად აქტიური პირებისა და სანქციადაკისრებული პირების სიებში და აფასებს მათ რეპუტაციასთან დაკავშირებულ ინფორმაციას;

- ახორციელებს საქმიანი ურთიერთობისა და ტრანზაქციების მიმდინარე მონიტორინგს და უზრუნველყოფს მოპოვებული ინფორმაციისა და დოკუმენტების განახლებას.

4 გაძლიერებული ღონისძიებები და პოლიტიკურად აქტიური პირები

მომეტებული რისკის შემთხვევაში კომპანია იყენებს გაძლიერებულ პრევენციულ ღონისძიებებს. ასეთი ღონისძიებები შეიძლება მოიცავდეს დამატებითი ინფორმაციისა და დოკუმენტების მოპოვებას, ქონებისა და შემოსავლის ან ფულადი სახსრებისა და ვირტუალური აქტივის წარმომავლობის დადგენას, უფლებამოსილი ხელმძღვანელი პირის თანხმობას, გაძლიერებულ მონიტორინგსა და სხვა რისკის თანაზომიერ ზომებს.

პოლიტიკურად აქტიური პირების, მათი ოჯახის წევრებისა და მათთან ასოცირებული პირების მიმართ გამოიყენება კანონმდებლობით განსაზღვრული გაძლიერებული კონტროლი. საჯარო ან პოლიტიკური ფუნქციის დასრულების შემდეგ შესაბამისი ზომები ნარჩუნდება იმდენ ხანს, რამდენ ხანსაც არსებობს ამ სტატუსთან დაკავშირებული განგრძობითი რისკი.

5 სანქციებთან შესაბამისობა

კომპანია კლიენტებს, მათ წარმომადგენლებს, ხელმძღვანელობითი უფლებამოსილების მქონე პირებსა და ბენეფიციარ მესაკუთრეებს ამოწმებს მოქმედი სანქციური რეჟიმების ფარგლებში, მათ შორის გაეროს უშიშროების საბჭოს, აშშ-ის, ევროკავშირისა და გაერთიანებული სამეფოს შესაბამის სიებში. სკრინინგი ტარდება საქმიანი ურთიერთობის დამყარებამდე და ურთიერთობის განმავლობაში.

შესაძლო დამთხვევა ექვემდებარება ინდივიდუალურ განხილვას. დადასტურებული დამთხვევის ან სანქციების გვერდის ავლის რისკის გამოვლენისას კომპანია იღებს შესაბამისი სანქციური რეჟიმითა და კანონმდებლობით მოთხოვნილ ზომებს, მათ შორის, საჭიროების შემთხვევაში, ტრანზაქციის ან მომსახურების შეზღუდვას, შეჩერებას, აქტივის გაყინვას, ურთიერთობის არდამყარებას ან შეწყვეტას და კომპეტენტური ორგანოსთვის ინფორმაციის წარდგენას.

6 ვირტუალური აქტივების კონტროლი

კომპანია შესაბამისი ბლოკჩეინ-ანალიტიკური საშუალებებით ამოწმებს ვირტუალური აქტივის მისამართებსა და ტრანზაქციებს და აფასებს მათ წყაროს, დანიშნულებას, დაკავშირებულ საფუძვლებსა და მაღალი რისკის კატეგორიებთან შესაძლო კავშირს. ტექნიკური რისკის შეფასება არ ანაცვლებს ტრანზაქციის ეკონომიკური მიზნის, წარმომავლობისა და მონაწილე მხარეების შინაარსობრივ შესწავლას. ახალი რისკის ინფორმაციის მიღებისას შეიძლება განხორციელდეს ხელახალი შემოწმება.

7 მიმდინარე მონიტორინგი და ანგარიშგება

კომპანია მუდმივად აკვირდება კლიენტის საქმიანობასა და ტრანზაქციებს და შეისწავლის რთულ, უჩვეულოდ დიდ, დანაწევრებულ, ეკონომიკური ან კანონიერი მიზნის არმქონე ან კლიენტის პროფილთან შეუსაბამო ოპერაციებს. საფუძვლიანი ეჭვის არსებობისას AML ოფიცერი დამოუკიდებლად იღებს გადაწყვეტილებას საქართველოს ფინანსური მონიტორინგის სამსახურისთვის ანგარიშგების წარდგენის შესახებ, კანონით განსაზღვრული წესითა და ვადით.

საეჭვოობის განხილვასთან, ანგარიშგებასთან ან კომპეტენტური ორგანოს მითითებასთან დაკავშირებული ინფორმაცია კონფიდენციალურია და კლიენტისთვის ან სხვა არაუფლებამოსილი პირისთვის არ გამჟღავნდება.

8 პარტნიორების შეფასება

კომერციულ ბანკთან, საგადახდო მომსახურების პროვაიდერთან, სხვა ვირტუალური აქტივის მომსახურების პროვაიდერთან ან სხვა პარტნიორ ფინანსურ ინსტიტუტთან ურთიერთობის დამყარებამდე კომპანია აფასებს მის ავტორიზაციას, ზედამხედველობას, რეპუტაციას, მფლობელობასა და მართვას, სანქციურ სტატუსსა და AML/CFT კონტროლის სისტემას. კომპანია არ ამყარებს ან წყვეტს ურთიერთობას, თუ გამოვლენილი რისკის სათანადოდ მართვა შეუძლებელია ან ურთიერთობა აკრძალულია კანონმდებლობით.

9 მონაცემთა შენახვის მართვა და კონტროლი

კლიენტის შესწავლის, ტრანზაქციებისა და ანგარიშგების შესახებ ინფორმაცია და დოკუმენტები ინახება შესაბამისი ურთიერთობის ან ოპერაციის დასრულებიდან არანაკლებ ხუთი წლის განმავლობაში, ხოლო კანონმდებლობით გათვალისწინებულ შემთხვევაში - კანონით ნებადართული დამატებითი ვადით. ინფორმაცია დაცულია კონფიდენციალურობისა და წვდომის კონტროლის შესაბამისი ზომებით.

კომპანიის ხელმძღვანელობა უზრუნველყოფს შესაბამისობის კონტროლის სისტემისთვის საჭირო რესურსებსა და ზედამხედველობას. AML ოფიცერი მართავს და აკონტროლებს სისტემის ფუნქციონირებას, თანამშრომლები გადიან როლზე მორგებულ სწავლებას, ხოლო კონტროლის ეფექტიანობა მოწმდება დამოუკიდებელი აუდიტით და საჭიროების შემთხვევაში ექვემდებარება განახლებას.

10 კლიენტის ვალდებულებები და კომპანიის უფლებამოსილება

კლიენტი ვალდებულია კომპანიას მიაწოდოს სრული, ზუსტი და განახლებული ინფორმაცია და დოკუმენტები, დროულად აცნობოს მნიშვნელოვანი ცვლილების შესახებ და მოთხოვნის შემთხვევაში განმარტოს ტრანზაქციის მიზანი და წარმომავლობა. თუ კომპანია ვერ ასრულებს კანონით გათვალისწინებულ პრევენციულ ღონისძიებებს ან გამოვლენილი რისკის მართვა შეუძლებელია, კომპანია უფლებამოსილია, მოქმედი კანონმდებლობისა და შიდა კონტროლის ფარგლებში, მოითხოვოს დამატებითი ინფორმაცია, არ დაამყაროს ან შეწყვიტოს საქმიანი ურთიერთობა და შეზღუდოს ან შეაჩეროს მომსახურება ან ტრანზაქცია.

Public Anti Money Laundering and Counter Terrorist Financing Policy

Concise public version

This document is a concise public version of the internal policy of CityPay LLC (the Company), a virtual asset service provider, for preventing and combating money laundering, terrorist financing and proliferation financing. Its purpose is to inform customers and partners about the Company's core AML/CFT/PF principles and control areas.

1 Purpose and scope

The Company conducts its activities in accordance with applicable Georgian AML/CFT legislation and the binding requirements of the National Bank of Georgia and the Financial Monitoring Service of Georgia. This policy applies to the Company's customers, their beneficial owners and representatives, products, services, transactions, delivery channels, employees and business relationships with partners.

2 Risk based approach

The Company identifies and assesses ML/TF/PF and sanctions risks associated with customers, beneficial owners, jurisdictions, business activities, products, services, transactions, technology and partner providers. Measures that are proportionate to the identified level of risk are applied to manage those risks.

Customer risk is assessed before a business relationship is established and is reviewed throughout the relationship, including when customer information, activity, transactional behaviour or another material risk factor changes. Before introducing a new product, service, technology or delivery channel, the Company assesses the relevant risks and defines appropriate mitigating measures.

3 Customer due diligence

Where required by law, the Company:

- identifies and verifies the customer, any person acting on the customer's behalf and persons authorised to manage or represent a legal entity;
- understands the ownership and control structure of a legal entity and identifies its ultimate beneficial owner;
- establishes the purpose and intended nature of the business relationship, the expected transaction profile and, where required, the source of wealth, income, funds or virtual assets;
- screens relevant persons against politically exposed person and sanctions lists and assesses relevant reputational information;
- conducts ongoing monitoring of the business relationship and transactions and keeps the information and documents obtained up to date.

4 Enhanced measures and politically exposed persons

Where higher risk is identified, the Company applies enhanced due diligence measures. These measures may include obtaining additional information and documents, establishing the source of wealth and income or the source of funds and virtual assets, obtaining approval from an authorised member of management, enhanced monitoring and other measures proportionate to the risk.

Politically exposed persons, their family members and known close associates are subject to the enhanced controls required by law. After a public or political function ends, appropriate measures remain in place for as long as a continuing risk associated with that status exists.

5 Sanctions compliance

The Company screens customers, their representatives, persons authorised to manage them and beneficial owners under applicable sanctions regimes, including the relevant lists of the United Nations Security Council, the United States, the European Union and the United Kingdom. Screening is performed before a business relationship is established and throughout the relationship.

A potential match is reviewed individually. If a match is confirmed or a risk of sanctions evasion is identified, the Company applies the measures required by the relevant sanctions regime and applicable law, including, where necessary, restricting or suspending a transaction or service, freezing assets, declining or terminating a relationship and reporting to a competent authority.

6 Virtual asset controls

The Company uses appropriate blockchain analytics to screen virtual asset addresses and transactions and assesses their source, destination, associated wallets and possible links to high-risk categories. A technical risk assessment does not replace the substantive assessment of the economic purpose and origin of a transaction or the parties involved. Addresses and transactions may be rescreened when new risk information becomes available.

7 Ongoing monitoring and reporting

The Company continuously monitors customer activity and transactions and reviews complex, unusually large, structured, apparently unjustified or profile-inconsistent activity. Where reasonable suspicion exists, the AML Officer independently decides whether to submit a report to the Financial Monitoring Service of Georgia in the manner and within the timeframe prescribed by law.

Information relating to the review or reporting of suspicious activity or to an instruction from a competent authority is confidential and is not disclosed to the customer or any other unauthorised person.

8 Assessment of partners

Before establishing a relationship with a bank, payment service provider, another virtual asset service provider or another partner financial institution, the Company assesses its authorisation, supervision, reputation, ownership and management, sanctions status and AML/CFT control framework. The Company does not establish or terminates a relationship where the identified risk cannot be managed appropriately or where the relationship is prohibited by law.

9 Record keeping governance and controls

Customer due diligence, transaction and reporting information and documents are retained for at least five years after the relevant relationship or transaction ends and, where provided by law, for an

additional period permitted by law. Information is protected through appropriate confidentiality and access controls.

The Company's management provides the resources and oversight required for the compliance control system. The AML Officer manages and monitors the operation of the framework, relevant employees receive role-appropriate training, and the effectiveness of the controls is reviewed through independent audit and updated where necessary.

10 Customer obligations and Company authority

Customers must provide complete, accurate and up-to-date information and documents, promptly notify the Company of material changes and, when requested, explain the purpose and origin of a transaction. If the Company cannot complete the preventive measures required by law or cannot appropriately manage an identified risk, it may, within the limits of applicable law and its internal control framework, request additional information, decline or terminate a business relationship, or restrict or suspend a service or transaction.