AML/KYC POLICY / ПОЛИТИКА AML/KYC

English version

DCrypto AML/KYC Policy
Effective date: 2 April 2026

This AML/KYC Policy describes the main principles used by DCrypto LLC to identify users, assess risk, monitor activity and respond to suspicious, prohibited or restricted conduct.

1. Risk-based approach

1.1. DCrypto applies a risk-based approach. The level of review depends on the user profile, country, product, amount, transaction pattern, payment method, card route, wallet profile, blockchain exposure and other relevant factors.
1.2. Review may occur before onboarding, before a transaction, during a transaction, after a transaction, periodically, or at any other time considered reasonably necessary.

2. Identity verification

2.1. DCrypto may verify a user's identity using personal information, document review, facial comparison, liveness checks, residence checks and other appropriate methods.
2.2. Additional information may be requested where necessary, including source of funds, source of wealth, purpose of transaction, card ownership evidence, wallet control evidence and explanation of account activity.
2.3. If a user fails verification, provides incomplete information, provides misleading information or otherwise presents unacceptable risk, DCrypto may refuse service, delay a transaction, suspend the account or terminate the relationship.

3. Sanctions and restricted users

3.1. DCrypto screens users, counterparties, wallets, transactions and associated data against applicable sanctions, internal restrictions and other legal or operational prohibitions.
3.2. The Services are unavailable to citizens of the United States and to citizens or residents of Georgia.
3.3. DCrypto also restricts Services in relation to the jurisdictions listed in the User Agreement and may expand or revise those restrictions at its discretion.
3.4. Russia, Belarus and CIS users are not automatically rejected, but remain subject to full sanctions, AML and internal risk review.
3.5. Any attempt to conceal geography, beneficial ownership, nationality, residence or transaction purpose may lead to refusal, hold, closure or reporting.

4. Source of funds and purpose review

4.1. DCrypto may request evidence of the lawful origin of fiat funds and digital assets.
4.2. This may include bank statements, payroll records, tax records, contracts, invoices, sale documents, inheritance records, business records, screenshots, signed wallet messages, transaction explanations and other supporting documents.
4.3. DCrypto may request information concerning the purpose, economic rationale and expected frequency of transactions.

5. Blockchain and transaction monitoring

5.1. DCrypto may monitor wallet addresses, blockchain transactions, counterparties, transactional patterns, card routes, local payment routes and internal account activity.
5.2. DCrypto may use internal controls and external service providers for sanctions screening, transaction monitoring, fraud prevention and blockchain analytics.
5.3. Transactions connected to hacking, theft, ransomware, darknet activity, sanctioned exposure, obfuscation tools, fraud typologies or other prohibited activity may be rejected, held, escalated or reported.

6. Third-party funding and third-party payouts

6.1. Unless expressly approved, DCrypto does not permit third-party funding or payouts to third-party recipients.
6.2. Fiat payments, card payouts and digital asset transfers may be restricted to the verified user’s own payment instruments, cards, accounts and wallets.
6.3. DCrypto may request proof of ownership or control before processing or releasing a transaction.

7. Enhanced review

7.1. DCrypto may apply enhanced review where risk is elevated.
7.2. Enhanced review may apply in cases involving larger volumes, unusual patterns, complex routing, repeated failed verification, inconsistent user profile, adverse public information, higher-risk jurisdictions, opaque source of funds, wallet exposure concerns or partner requirements.

8. Refusal, hold and reporting

8.1. DCrypto may refuse onboarding, delay execution, place a transaction on hold, request additional documents, return funds where appropriate, suspend the account, terminate the relationship, or report the matter where required by law.
8.2. DCrypto is not required to disclose internal monitoring thresholds, red-flag logic, reporting decisions or details that could compromise compliance controls or investigations.

9. Record keeping

9.1. Financial transaction records, AML/KYC documents and related compliance records are retained for not less than five years, and longer where required by law or investigation.
9.2. Records may be shared with competent authorities, financial institutions and service providers where legally required or reasonably necessary.

10. Contact

10.1. Compliance-related requests may be sent to legal@dcrypto.io.

Русская версия

Политика AML/KYC DCrypto
Дата вступления в силу: 2 апреля 2026 года
Информационная версия. При расхождении действует английская версия.

Настоящая Политика описывает основные принципы, по которым DCrypto LLC устанавливает личность пользователя, оценивает риск, наблюдает за активностью и реагирует на подозрительное, запрещенное либо ограниченное поведение.

1. Риск-ориентированный подход

1.1. DCrypto применяет риск-ориентированный подход. Глубина проверки зависит от профиля пользователя, страны, продукта, суммы операции, характера операций, способа оплаты, карточного маршрута, профиля кошелька, блокчейн-экспозиции и иных факторов.
1.2. Проверка может проводиться до регистрации, до операции, во время операции, после операции, периодически либо в любой иной момент, когда это разумно необходимо.

2. Проверка личности

2.1. DCrypto вправе проверять личность пользователя с помощью персональных данных, проверки документа, сопоставления изображения лица, проверки присутствия, проверки места проживания и иных допустимых способов.
2.2. При необходимости могут запрашиваться дополнительные сведения, включая происхождение средств, происхождение благосостояния, цель операции, доказательства владения картой, подтверждение контроля над кошельком и объяснение активности по аккаунту.
2.3. Если пользователь не проходит проверку, дает неполные сведения, предоставляет вводящую в заблуждение информацию либо создает неприемлемый риск, DCrypto вправе отказать в сервисе, задержать операцию, ограничить аккаунт или прекратить отношения.

3. Санкции и ограничения

3.1. DCrypto проверяет пользователей, контрагентов, кошельки, операции и связанные данные по применимым санкциям, внутренним ограничениям и иным юридическим либо операционным запретам.
3.2. Сервис недоступен гражданам США, а также гражданам и резидентам Грузии.
3.3. DCrypto также ограничивает сервис в отношении юрисдикций, перечисленных в

Пользовательском соглашении, и вправе пересматривать этот перечень.
3.4. Пользователи из России, Беларуси и стран СНГ не отклоняются автоматически, но проходят полную санкционную, AML и внутреннюю проверку риска.
3.5. Любая попытка скрыть географию, бенефициара, гражданство, резидентство либо цель операции может повлечь отказ, удержание, закрытие аккаунта либо передачу сведений в установленном порядке.

4. Проверка происхождения средств и цели операции

4.1. DCrypto вправе запросить подтверждение законного происхождения фиатных средств и цифровых активов.
4.2. Это могут быть банковские выписки, документы о заработке, налоговые документы, договоры, счета, документы о продаже имущества, документы о наследовании, деловые документы, снимки экрана, подписанные сообщения кошелька, пояснения по транзакциям и иные подтверждения.
4.3. DCrypto вправе запросить сведения о цели, экономическом смысле и ожидаемой частоте операций.

5. Блокчейн и мониторинг операций

5.1. DCrypto вправе отслеживать адреса кошельков, блокчейн-операции, контрагентов, поведение операций, карточные маршруты, локальные платежные маршруты и активность по внутреннему аккаунту.
5.2. Для санкционного контроля, наблюдения за операциями, борьбы с мошенничеством и анализа блокчейна DCrypto может использовать внутренние правила и внешних поставщиков.
5.3. Операции, связанные со взломом, кражей, вымогательскими схемами, теневыми рынками, санкционной экспозицией, средствами сокрытия следа, схемами мошенничества или иной запрещенной активностью, могут быть отклонены, удержаны, переданы на углубленный разбор либо сообщены в установленном порядке.

6. Платежи и выплаты третьих лиц

6.1. Если иное прямо не одобрено, DCrypto не допускает финансирования от третьих лиц и выплаты в пользу третьих лиц.
6.2. Фиатные платежи, выплаты на карты и переводы цифровых активов могут быть ограничены собственными платежными инструментами, картами, счетами и кошельками верифицированного пользователя.
6.3. До проведения либо выдачи операции DCrypto вправе запросить доказательства владения или контроля.

7. Усиленная проверка

7.1. При повышенном риске DCrypto вправе применять усиленную проверку.
7.2. Такая проверка может использоваться при крупных объемах, необычном поведении, сложном маршруте, повторных неудачных верификациях, несоответствии профиля пользователя, негативной открытой информации, повышенном риске страны,

непрозрачном происхождении средств, вопросах к кошельку или по требованию партнера.

8. Отказ, удержание и сообщение

8.1. DCrypto вправе отказать в подключении клиента, задержать исполнение, удержать операцию, запросить дополнительные документы, вернуть средства в допустимых случаях, ограничить аккаунт, прекратить отношения или сообщить о ситуации, если того требует закон.
8.2. DCrypto не обязан раскрывать внутренние пороги мониторинга, логику красных флагов, основания для сообщения либо сведения, которые могут навредить контролю или расследованию.

9. Хранение записей

9.1. Сведения о финансовых операциях, документы AML/KYC и связанные комплаенс-записи хранятся не менее пяти лет, а при необходимости и дольше.
9.2. Эти материалы могут передаваться компетентным органам, финансовым организациям и поставщикам услуг, если это требуется законом либо разумно необходимо.

10. Контакт

10.1. Вопросы по комплаенсу можно направлять на legal@dcrypto.io.

ქართული ვერსია

DCrypto-ის AML/KYC პოლიტიკა
ძალაში შესვლის თარიღი: 2026 წლის 2 აპრილი
საცნობარო თარგმანი. შეუსაბამობის შემთხვევაში უპირატესობა ენიჭება ინგლისურ ვერსიას.

ეს პოლიტიკა აღწერს ძირითად წესებს, რომლითაც DCrypto LLC ადგენს მომხმარებლის ვინაობას, აფასებს რისკს, აკვირდება აქტივობას და რეაგირებს საეჭვო, აკრძალულ ან შეზღუდულ ქცევაზე.

1. რისკზე დაფუძნებული მიდგომა

1.1. DCrypto იყენებს რისკზე დაფუძნებულ მიდგომას. შემოწმების სიღრმე დამოკიდებულია მომხმარებლის პროფილზე, ქვეყანაზე, პროდუქტზე, თანხის ოდენობაზე, ოპერაციების ხასიათზე, გადახდის მეთოდზე, საბარათე მარშრუტზე, საფულის პროფილსა და სხვა გარემოებებზე.
1.2. შემოწმება შეიძლება ჩატარდეს რეგისტრაციამდე, ოპერაციამდე, ოპერაციის დროს, ოპერაციის შემდეგ, პერიოდულად ან ნებისმიერ სხვა გონივრულად საჭირო დროს.

2. პირის იდენტიფიკაცია

2.1. DCrypto უფლებამოსილია მომხმარებლის ვინაობა გადაამოწმოს პერსონალური მონაცემებით, დოკუმენტის შემოწმებით, სახის შედარებით, სიცოცხლის დადასტურებით, საცხოვრებლის შემოწმებით და სხვა დასაშვები მეთოდებით.
2.2. საჭიროების შემთხვევაში შეიძლება მოითხოვოს დამატებითი ინფორმაცია, მათ შორის თანხის წარმომავლობა, ქონებრივი მდგომარეობის წარმომავლობა, ოპერაციის მიზანი, ბარათის ფლობის მტკიცებულება, საფულის კონტროლის დადასტურება და ანგარიშის აქტივობის ახსნა.
2.3. თუ მომხმარებელი ვერ გაივლის შემოწმებას, წარადგენს არასრულ ან შეცდომაში შემყვან ინფორმაციას ან ქმნის მიუღებელ რისკს, DCrypto უფლებამოსილია უარი თქვას მომსახურებაზე, დააყოვნოს ოპერაცია, შეზღუდოს ანგარიში ან შეწყვიტოს ურთიერთობა.

3. სანქციები და შეზღუდვები

3.1. DCrypto ამოწმებს მომხმარებლებს, კონტრაგენტებს, საფულეებს, ოპერაციებსა და მათთან დაკავშირებულ მონაცემებს მოქმედი სანქციების, შიდა შეზღუდვებისა და სხვა სამართლებრივი ან საოპერაციო აკრძალვების მიხედვით.
3.2. მომსახურება მიუწვდომელია აშშ-ის მოქალაქეებისთვის, ასევე საქართველოს მოქალაქეებისა და რეზიდენტებისთვის.
3.3. DCrypto ასევე ზღუდავს მომსახურებას იმ იურისდიქციებთან მიმართებით, რომლებიც ჩამოთვლილია მომხმარებლის შეთანხმებაში, და უფლებამოსილია ეს ჩამონათვალი გადაახედოს.
3.4. რუსეთის, ბელარუსისა და დსთ-ის ქვეყნების მომხმარებლები ავტომატურად არ იბლოკებიან, თუმცა ექვემდებარებიან სრულ სანქციურ, AML და შიდა რისკის შემოწმებას.
3.5. გეოგრაფიის, ბენეფიციარის, მოქალაქეობის, რეზიდენტობის ან ოპერაციის მიზნის დამალვის ნებისმიერი მცდელობა შეიძლება გამოიწვიოს უარი, შეჩერება, ანგარიშის დახურვა ან ინფორმაციის გადაცემა დადგენილი წესით.

4. თანხის წარმომავლობა და ოპერაციის მიზანი

4.1. DCrypto უფლებამოსილია მოითხოვოს ფიატური თანხისა და ციფრული აქტივების კანონიერი წარმომავლობის დამადასტურებელი მასალა.
4.2. ასეთ მასალად შეიძლება მოთხოვნილი იყოს საბანკო ამონაწერი, შემოსავლის დამადასტურებელი დოკუმენტი, საგადასახადო დოკუმენტი, ხელშეკრულება, ინვოისი, ქონების გაყიდვის საბუთი, მემკვიდრეობის დოკუმენტი, ბიზნეს-დოკუმენტი, ეკრანის ანაბეჭდი, საფულით ხელმოწერილი შეტყობინება, ოპერაციის ახსნა და სხვა მტკიცებულება.
4.3. DCrypto უფლებამოსილია მოითხოვოს ოპერაციის მიზნის, ეკონომიკური შინაარსისა და მოსალოდნელი სიხშირის განმარტება.

5. ბლოკჩეინი და ოპერაციების მონიტორინგი

5.1. DCrypto უფლებამოსილია დააკვირდეს საფულის მისამართებს, ბლოკჩეინის ოპერაციებს, კონტრაგენტებს, ოპერაციულ ქცევას, საბარათე მარშრუტებს, ადგილობრივ გადახდის მარშრუტებსა და შიდა ანგარიშის აქტივობას.
5.2. სანქციების შემოწმების, ოპერაციების მონიტორინგის, თაღლითობის პრევენციისა და ბლოკჩეინის ანალიზისათვის DCrypto შეიძლება იყენებდეს როგორც შიდა წესებს, ისე გარე მომწოდებლებს.
5.3. ოპერაციები, რომლებიც უკავშირდება გატეხვას, ქურდობას, გამოსასყიდის სქემებს,

ჩრდილოვან ბაზრებს, სანქციურ რისკს, კვალის დამალვის საშუალებებს, თაღლითობის ტიპოლოგიებს ან სხვა აკრძალულ ქმედებას, შეიძლება იყოს უარყოფილი, შეჩერებული, გადაცემული გაძლიერებულ განხილვაზე ან, საჭიროების შემთხვევაში, შეტყობინებული.

6. მესამე პირის დაფინანსება და მესამე პირზე ჩარიცხვა

6.1. თუ პირდაპირი ნებართვა არ არსებობს, DCrypto არ უშვებს მესამე პირის მიერ დაფინანსებას და მესამე პირის სასარგებლოდ ჩარიცხვას.
6.2. ფიატური გადახდები, ბარათზე ჩარიცხვები და ციფრული აქტივების გადარიცხვები შეიძლება შეიზღუდოს მხოლოდ ვერიფიცირებული მომხმარებლის საკუთარ გადახდის ინსტრუმენტებზე, ბარათებზე, ანგარიშებსა და საფულეებზე.
6.3. ოპერაციის დამუშავებამდე ან თანხის გაცემამდე DCrypto უფლებამოსილია მოითხოვოს ფლობის ან კონტროლის დადასტურება.

7. გაძლიერებული შემოწმება

7.1. მომატებული რისკის შემთხვევაში DCrypto უფლებამოსილია გამოიყენოს გაძლიერებული შემოწმება.
7.2. ეს შეიძლება შეეხოს დიდ მოცულობას, უჩვეულო ქცევას, რთულ მარშრუტს, მრავალჯერად წარუმატებელ ვერიფიკაციას, მომხმარებლის პროფილთან შეუსაბამობას, უარყოფით საჯარო ცნობებს, მაღალი რისკის ქვეყანას, გაუმჭვირვალე თანხის წარმომავლობას, საფულესთან დაკავშირებულ კითხვებს ან პარტნიორის მოთხოვნას.

8. უარი, შეჩერება და შეტყობინება

8.1. DCrypto უფლებამოსილია უარი თქვას კლიენტის მიღებაზე, დააყოვნოს შესრულება, შეაჩეროს ოპერაცია, მოითხოვოს დამატებითი დოკუმენტები, კანონით დასაშვებ შემთხვევაში დააბრუნოს თანხა, შეზღუდოს ანგარიში, შეწყვიტოს ურთიერთობა ან მოახდინოს შეტყობინება, თუ ამას კანონი მოითხოვს.
8.2. DCrypto არ არის ვალდებული გაამჟღავნოს შიდა მონიტორინგის ზღვარი, წითელი ნიშნების ლოგიკა, შეტყობინების საფუძველი ან სხვა ინფორმაცია, რომელიც შეიძლება დააზიანოს შესაბამისობის კონტროლი ან გამოძიება.

9. ჩანაწერების შენახვა

9.1. ფინანსური ოპერაციების ჩანაწერები, AML/KYC დოკუმენტები და შესაბამისობის მასალები ინახება არანაკლებ ხუთი წლის განმავლობაში და, საჭიროების შემთხვევაში, უფრო დიდხანს.
9.2. ეს მასალები შეიძლება გაეზიაროს უფლებამოსილ ორგანოებს, ფინანსურ დაწესებულებებსა და მომსახურების მომწოდებლებს, თუ ამას კანონი მოითხოვს ან ეს გონივრულად აუცილებელია.

10. საკონტაქტო მისამართი

10.1. შესაბამისობასთან დაკავშირებული საკითხები უნდა გაიგზავნოს მისამართზე legal@dcrypto.io.