

ელექტრონული საფულის ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის პოლიტიკა

1. ზოგადი დებულებები

1.1. წინამდებარე ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის პოლიტიკა (შემდგომში – „AML/CFT პოლიტიკა“) განსაზღვრავს შპს „მულტიპრაიმ“-ის მიერ ელექტრონული საფულის მომსახურების ფარგლებში ფულის გათეთრებისა და ტერორიზმის დაფინანსების პრევენციის, გამოვლენისა და აღკვეთის მიზნით განსახორციელებელ ღონისძიებებს.

1.2. პოლიტიკის მიზანია ელექტრონული საფულის გამოყენების გზით ფულის გათეთრების, ტერორიზმის დაფინანსების, სანქციების გვერდის ავლის, თაღლითობისა და სხვა უკანონო ფინანსური საქმიანობის რისკების მართვა.

1.3. კომპანია ელექტრონული საფულის მომსახურებას ახორციელებს მომხმარებლის სათანადო იდენტიფიკაციის, რისკზე დაფუძნებული მიდგომის, ტრანზაქციების მონიტორინგისა და შესაბამისი კონტროლის მექანიზმების გამოყენებით.

1.4. პოლიტიკა ვრცელდება კომპანიის ყველა შესაბამის თანამშრომელზე, მმართველი ორგანოს წევრებზე, კონტრაქტორებზე და იმ პირებზე, რომლებიც მონაწილეობენ ელექტრონული საფულის მომსახურების მიწოდებაში ან AML/CFT კონტროლში.

2. პოლიტიკის მიზნები

2.1. AML/CFT პოლიტიკის ძირითადი მიზნებია:

ა) ფულის გათეთრებისა და ტერორიზმის დაფინანსების რისკების გამოვლენა და მართვა;

ბ) მომხმარებლისა და ბენეფიციარი მესაკუთრის სათანადო იდენტიფიკაცია და ვერიფიკაცია;

გ) მომხმარებელთა რისკის შეფასება და რისკის შესაბამისი კონტროლის ღონისძიებების გამოყენება;

დ) საექვო და უჩვეულო ოპერაციების გამოვლენა და შესაბამისი რეაგირება;

ე) მაღალი რისკის მომხმარებლებისა და საქმიანობების გაძლიერებული მონიტორინგი;

ვ) სანქციებისა და შესაბამისი შემზღუდველი ღონისძიებების დაცვის უზრუნველყოფა;

ზ) ელექტრონული საფულისა და მასთან დაკავშირებული კრიპტოაქტივების გამოყენებით უკანონო ფინანსური საქმიანობის პრევენცია;

თ) შესაბამისი ჩანაწერებისა და დოკუმენტაციის შენახვა;

ი) კომპანიის AML/CFT ვალდებულებების შესრულების კონტროლი.

3. რისკზე დაფუძნებული მიდგომა

3.1. კომპანია AML/CFT კონტროლს ახორციელებს რისკზე დაფუძნებული მიდგომის საფუძველზე.

3.2. მომხმარებლის რისკის შეფასებისას კომპანია ითვალისწინებს, მათ შორის:

ა) მომხმარებლის ტიპსა და სამართლებრივ სტატუსს;

ბ) მოქალაქეობასა და რეზიდენტობას;

გ) საქმიანობას, სამუშაო ადგილსა და თანამდებობას;

დ) მომხმარებლის შემოსავლისა და ქონების წყაროს;

ე) სახსრების წყაროს;

ვ) ბენეფიციარ მესაკუთრეს;

ზ) PEP სტატუსს;

თ) სანქციებთან დაკავშირებულ რისკებს;

ი) გეოგრაფიულ ფაქტორებს;

კ) გამოყენებულ პროდუქტებსა და მომსახურებებს;

ლ) ტრანზაქციების მოცულობასა და სიხშირეს;

მ) ტრანზაქციების დანიშნულებასა და ეკონომიკურ შინაარსს;

ნ) გამოყენებულ გადახდის საშუალებებს;

ო) კრიპტოაქტივებთან დაკავშირებულ რისკებს;

პ) საფულის მისამართებთან და ტრანზაქციის ჯაჭვთან დაკავშირებულ რისკებს;

ჟ) მომხმარებლის ქცევის შესაბამისობას მის პროფილთან.

3.3. მომხმარებლის რისკის დონე შეიძლება განისაზღვროს როგორც დაბალი, საშუალო ან მაღალი, კომპანიის მიერ დამტკიცებული რისკის შეფასების მეთოდოლოგიის შესაბამისად.

4. მომხმარებლის იდენტიფიკაცია და ვერიფიკაცია

4.1. ელექტრონული საფულის გახსნამდე და მომსახურების შესაბამისი ეტაპიდან გამომდინარე კომპანია ახორციელებს მომხმარებლის იდენტიფიკაციასა და ვერიფიკაციას.

4.2. ფიზიკური პირის შემთხვევაში კომპანია აგროვებს და ამოწმებს, სულ მცირე, კანონმდებლობითა და კომპანიის პროცედურებით განსაზღვრულ საიდენტიფიკაციო ინფორმაციას.

4.3. იურიდიული პირის შემთხვევაში კომპანია ახორციელებს იურიდიული პირის, მისი წარმომადგენლისა და ბენეფიციარი მესაკუთრის იდენტიფიკაციასა და ვერიფიკაციას.

4.4. დისტანციური მომსახურების შემთხვევაში მომხმარებლის იდენტიფიკაცია და ვერიფიკაცია ხორციელდება კომპანიის მიერ დამტკიცებული ელექტრონული მეთოდების გამოყენებით.

4.5. მომხმარებლის იდენტიფიკაციისა და ვერიფიკაციის დასრულებამდე კომპანია უფლებამოსილია შეზღუდოს ან არ დაუშვას შესაბამისი მომსახურების გამოყენება.

5. ბენეფიციარი მესაკუთრის დადგენა

5.1. იურიდიული პირის ან სხვა სამართლებრივი ფორმის მომხმარებლის მომსახურების შემთხვევაში კომპანია ადგენს და ამოწმებს ბენეფიციარ მესაკუთრეს.

5.2. ბენეფიციარი მესაკუთრის იდენტიფიცირება ხორციელდება შესაბამისი ოფიციალური დოკუმენტების, რეესტრის მონაცემებისა და სხვა სანდო წყაროების გამოყენებით.

5.3. კომპანიისთვის მიუღებელია მომხმარებლის მომსახურება იმ შემთხვევაში, როდესაც ბენეფიციარი მესაკუთრის იდენტიფიცირება და შესაბამისი შემოწმება ვერ ხერხდება კანონმდებლობით გათვალისწინებული მოთხოვნების ფარგლებში.

6. მომხმარებლის რისკის შეფასება

6.1. კომპანია თითოეულ მომხმარებელს ანიჭებს შესაბამის რისკის კატეგორიას.

6.2. რისკის შეფასება ხორციელდება მომხმარებლის რეგისტრაციისას და პერიოდულად, ასევე იმ შემთხვევაში, როდესაც იცვლება მომხმარებლის პროფილი ან ვლინდება ახალი რისკის ფაქტორი.

6.3. რისკის შეფასებისას გამოიყენება:

- ა) მომხმარებლის რისკის ფაქტორები;
- ბ) გეოგრაფიული რისკები;
- გ) პროდუქტისა და მომსახურების რისკები;
- დ) ტრანზაქციის რისკები;
- ე) კრიპტოაქტივთან დაკავშირებული რისკები;
- ვ) სხვა შესაბამისი რისკის ფაქტორები.

6.4. მაღალი რისკის მომხმარებლების მიმართ კომპანია იყენებს გაძლიერებულ პრევენციულ ღონისძიებებს.

7. PEP-ის გამოვლენა და მართვა

7.1. კომპანია ახორციელებს მომხმარებლის, ბენეფიციარი მესაკუთრისა და შესაბამისი დაკავშირებული პირების PEP სტატუსის გამოვლენას.

7.2. PEP-ის გამოვლენის შემთხვევაში კომპანია ახორციელებს კანონმდებლობითა და კომპანიის შიდა პროცედურებით გათვალისწინებულ დამატებით ღონისძიებებს.

7.3. შესაბამის შემთხვევებში კომპანია იღებს დამატებით ინფორმაციას მომხმარებლის ქონების, შემოსავლისა და სახსრების წარმომავლობის შესახებ.

7.4. PEP სტატუსის მქონე მომხმარებელი ექვემდებარება გაძლიერებულ მონიტორინგს კანონმდებლობით გათვალისწინებული მოთხოვნების შესაბამისად.

8. სანქციების სკრინინგი

8.1. კომპანია ახორციელებს მომხმარებლებისა და შესაბამის შემთხვევებში ტრანზაქციების მონაწილე პირების შემოწმებას მოქმედი სანქციებისა და შესაბამისი შემზღუდველი ღონისძიებების მიმართ.

8.2. სკრინინგი ხორციელდება მომხმარებლის რეგისტრაციისას და შემდგომ პერიოდულად, აგრეთვე კომპანიის მიერ განსაზღვრულ სხვა შემთხვევებში.

8.3. სანქციურ სიასთან შესაძლო დამთხვევის გამოვლენისას კომპანია ახორციელებს შესაბამის დამატებით შემოწმებას და იღებს კანონმდებლობითა და კომპანიის შიდა პროცედურებით განსაზღვრულ გადაწყვეტილებას.

8.4. შესაბამის შემთხვევაში ოპერაცია შეიძლება შეჩერდეს, შეიზღუდოს ან უარყოფილ იქნეს.

9. სახსრებისა და ქონების წარმომავლობის დადგენა

9.1. კომპანიის მიერ განსაზღვრულ შემთხვევებში მომხმარებლისგან მიიღება ინფორმაცია სახსრების წყაროსა და/ან ქონების წარმომავლობის შესახებ.

9.2. აღნიშნული ინფორმაცია შეიძლება მოიცავდეს:

- ა) დასაქმებიდან მიღებულ შემოსავალს;
- ბ) ბიზნესსაქმიანობიდან მიღებულ შემოსავალს;
- გ) ინვესტიციებიდან მიღებულ შემოსავალს;
- დ) ქონების რეალიზაციიდან მიღებულ თანხას;
- ე) მემკვიდრეობას;
- ვ) სხვა კანონიერ წყაროს.

9.3. საჭიროების შემთხვევაში კომპანია უფლებამოსილია მოითხოვოს აღნიშნული ინფორმაციის დამადასტურებელი დოკუმენტები.

10. ელექტრონული საფულის ტრანზაქციების მონიტორინგი

10.1. კომპანია ახორციელებს ელექტრონული საფულის მეშვეობით განხორციელებული ოპერაციების მუდმივ ან პერიოდულ მონიტორინგს, შესაბამისი რისკის გათვალისწინებით.

10.2. მონიტორინგი მოიცავს:

- ა) ტრანზაქციის თანხას;
- ბ) ტრანზაქციის სიხშირეს;
- გ) ოპერაციების ერთმანეთთან დაკავშირებულობას;
- დ) მომხმარებლის ჩვეულებრივ ქცევასთან შესაბამისობას;
- ე) თანხების მოძრაობის მიმართულებას;
- ვ) ოპერაციის გეოგრაფიულ მიმართულებას;

ზ) უჩვეულო ან საეჭვო ქცევის გამოვლენას.

10.3. კომპანია იყენებს ავტომატიზებულ და/ან არავტომატიზებულ კონტროლის მექანიზმებს.

10.4. გამოვლენილი საეჭვო ან უჩვეულო ოპერაცია ექვემდებარება დამატებით ანალიზს.

11. კრიპტოაქტივებთან დაკავშირებული კონტროლი

11.1. ელექტრონული საფულის კრიპტოაქტივებთან დაკავშირებული ფუნქციონალის გამოყენებისას კომპანია ითვალისწინებს კრიპტოაქტივებისათვის დამახასიათებელ დამატებით AML/CFT რისკებს.

11.2. კომპანიის კონტროლის მექანიზმები შეიძლება მოიცავდეს:

ა) კრიპტოაქტივის საფულის მისამართების შემოწმებას;

ბ) ტრანზაქციის ისტორიის ანალიზს;

გ) blockchain analytics-ის გამოყენებას;

დ) მაღალი რისკის მისამართების გამოვლენას;

ე) darknet-თან, ransomware-თან, თაღლითობასთან, სანქცირებულ პირებთან ან სხვა უკანონო საქმიანობასთან დაკავშირებული რისკების გამოვლენას;

ვ) ტრანზაქციის წყაროსა და მიმართულების დამატებით შესწავლას;

ზ) შესაბამის შემთხვევებში ტრანზაქციის შეჩერებას ან დამატებითი ინფორმაციის მოთხოვნას.

11.3. კრიპტოაქტივებთან დაკავშირებული მაღალი რისკის გამოვლენის შემთხვევაში კომპანია ახორციელებს გაძლიერებულ შემოწმებასა და მონიტორინგს.

12. უჩვეულო და საეჭვო ოპერაციების გამოვლენა

12.1. კომპანია განსაზღვრავს ტრანზაქციებისა და ქცევის შესაბამის ინდიკატორებს, რომელთა არსებობის შემთხვევაში ოპერაცია შეიძლება დაექვემდებაროს დამატებით შემოწმებას.

12.2. ასეთ შემთხვევებს შეიძლება მიეკუთვნებოდეს:

ა) მომხმარებლის პროფილთან შეუსაბამო ტრანზაქციები;

- ბ) უჩვეულოდ მაღალი მოცულობის ოპერაციები;
 - გ) ხშირი და ერთმანეთთან დაკავშირებული ოპერაციები;
 - დ) თანხების სწრაფი შეტანა და გატანა;
 - ე) მომხმარებლის მიერ ანგარიშის გამოყენება გაურკვეველი ეკონომიკური მიზნის მქონე ოპერაციებისთვის;
 - ვ) მაღალი რისკის იურისდიქციებთან დაკავშირებული ოპერაციები;
 - ზ) კრიპტოაქტივის მაღალი რისკის საფულებთან დაკავშირებული ოპერაციები;
 - თ) მომხმარებლის მიერ მოთხოვნილი ინფორმაციის ან დოკუმენტაციის წარუდგენლობა;
 - ი) მომხმარებლის მიერ იდენტიფიკაციისა და შემოწმების პროცესის თავიდან აცილების მცდელობა.
-

13. საექვო გარიგების შესახებ ანგარიშგება

13.1. თუ კომპანიის მიერ განხორციელებული ანალიზის შედეგად არსებობს შესაბამისი საფუძველი, რომ ოპერაცია ან საქმიანობა შეიძლება დაკავშირებული იყოს ფულის გათეთრებასთან, ტერორიზმის დაფინანსებასთან ან სხვა შესაბამის უკანონო საქმიანობასთან, კომპანია მოქმედებს მოქმედი კანონმდებლობის შესაბამისად.

13.2. საექვო გარიგების შესახებ შესაბამისი ინფორმაციის წარდგენა ხორციელდება კანონმდებლობით დადგენილი წესითა და ვადებში.

13.3. მომხმარებელს არ მიეწოდება ინფორმაცია იმ შემთხვევაზე, როდესაც ასეთი გამჟღავნება აკრძალულია კანონმდებლობით.

14. გაძლიერებული შემოწმება

14.1. მაღალი რისკის მომხმარებლის, ოპერაციის, გეოგრაფიის ან სხვა მაღალი რისკის ფაქტორის გამოვლენის შემთხვევაში კომპანია ახორციელებს გაძლიერებულ პრევენციულ ღონისძიებებს.

14.2. გაძლიერებული ღონისძიებები შეიძლება მოიცავდეს:

- ა) დამატებითი ინფორმაციის მოთხოვნას;
- ბ) სახსრების წყაროს დადგენას;

- გ) ქონების წარმომავლობის დადგენას;
 - დ) ოპერაციის ეკონომიკური მიზნის დადგენას;
 - ე) დამატებით დოკუმენტურ შემოწმებას;
 - ვ) ტრანზაქციების გაძლიერებულ მონიტორინგს;
 - ზ) მომხმარებლის მონაცემების უფრო ხშირ განახლებას;
 - თ) ხელმძღვანელობის შესაბამისი დონის თანხმობის მოთხოვნას, როდესაც ამას კომპანიის პროცედურა ითვალისწინებს.
-

15. მომხმარებლის მონაცემების განახლება

- 15.1. კომპანია პერიოდულად აახლებს მომხმარებლის საიდენტიფიკაციო და რისკის შეფასებისთვის საჭირო ინფორმაციას.
 - 15.2. მონაცემების განახლების სიხშირე განისაზღვრება მომხმარებლის რისკის დონისა და შესაბამისი სამართლებრივი მოთხოვნების გათვალისწინებით.
 - 15.3. მომხმარებლის მნიშვნელოვანი ცვლილების გამოვლენის შემთხვევაში კომპანია უფლებამოსილია მოითხოვოს დამატებითი ინფორმაცია ან დოკუმენტაცია.
-

16. მომსახურების შეზღუდვა და შეწყვეტა

- 16.1. კომპანია უფლებამოსილია შეზღუდოს ან შეწყვიტოს მომხმარებლის მომსახურება კანონმდებლობით, ხელშეკრულებით ან კომპანიის შიდა წესებით გათვალისწინებულ შემთხვევებში.
- 16.2. მომსახურების შეზღუდვის ან შეწყვეტის საფუძველი შეიძლება გახდეს, მათ შორის:
 - ა) მომხმარებლის იდენტიფიკაციის ან ვერიფიკაციის შეუძლებლობა;
 - ბ) აუცილებელი ინფორმაციის ან დოკუმენტაციის წარუდგენლობა;
 - გ) მაღალი AML/CFT რისკის გამოვლენა;
 - დ) სანქციურ სიასთან დადასტურებული შესაბამისობა;
 - ე) საექვო საქმიანობის გამოვლენა;
 - ვ) კომპანიის მოთხოვნების სისტემატური დარღვევა;

ზ) კანონმდებლობით გათვალისწინებული სხვა საფუძველი.

17. თანამშრომელთა პასუხისმგებლობა და სწავლება

17.1. კომპანიის თანამშრომლები, რომელთა ფუნქციები დაკავშირებულია AML/CFT პროცესებთან, ვალდებული არიან დაიცვან წინამდებარე პოლიტიკა და შესაბამისი შიდა პროცედურები.

17.2. კომპანია უზრუნველყოფს შესაბამისი თანამშრომლების AML/CFT მიმართულებით პერიოდულ სწავლებასა და ცნობიერების ამაღლებას.

17.3. თანამშრომლები ვალდებული არიან დაუყოვნებლივ მიაწოდონ ინფორმაცია შესაბამის პასუხისმგებელ პირს მათთვის ცნობილი საეჭვო ან უჩვეულო ქცევის/ოპერაციის შესახებ.

18. AML/CFT პასუხისმგებელი პირი

18.1. კომპანია განსაზღვრავს AML/CFT მიმართულებაზე პასუხისმგებელ შესაბამის პირს.

18.2. AML/CFT პასუხისმგებელი პირის ძირითადი ფუნქციებია:

- ა) AML/CFT პოლიტიკისა და პროცედურების შესრულების ზედამხედველობა;
 - ბ) მომხმარებელთა რისკის შეფასების კონტროლი;
 - გ) საეჭვო და უჩვეულო ოპერაციების განხილვა;
 - დ) შესაბამისი ანგარიშგების უზრუნველყოფა;
 - ე) სანქციების სკრინინგისა და სხვა კონტროლის მექანიზმების ზედამხედველობა;
 - ვ) AML/CFT რისკების შესახებ მენეჯმენტისთვის შესაბამისი ინფორმაციის მიწოდება;
 - ზ) თანამშრომელთა სწავლების ორგანიზებაში მონაწილეობა;
 - თ) AML/CFT სისტემებისა და კონტროლის მექანიზმების პერიოდული შეფასება.
-

19. AML/CFT სისტემები და ტექნოლოგიური კონტროლი

19.1. კომპანია იყენებს შესაბამის ტექნიკურ და ორგანიზაციულ მექანიზმებს მომხმარებელთა და ტრანზაქციების მონიტორინგისთვის.

19.2. შესაბამისი სისტემები შეიძლება მოიცავდეს:

- ა) KYC სისტემას;
- ბ) სანქციების სკრინინგის სისტემას;
- გ) PEP სკრინინგის სისტემას;
- დ) ტრანზაქციების მონიტორინგის სისტემას;
- ე) blockchain analytics სისტემას;
- ვ) საექსპორტო ოპერაციების alert-ების მართვის მექანიზმს.

19.3. ავტომატიზებული სისტემის მიერ გენერირებული alert ექვემდებარება შესაბამის შეფასებას და საჭიროების შემთხვევაში დამატებით ანალიზს.

20. მესამე პირებთან დაკავშირებული რისკები

20.1. იმ შემთხვევაში, როდესაც ელექტრონული საფულის მომსახურებაში მონაწილეობენ მესამე პირები, კომპანია აფასებს მათთან დაკავშირებულ AML/CFT რისკებს.

20.2. შესაბამის შემთხვევებში მესამე პირის შერჩევისას კომპანია ითვალისწინებს:

- ა) მომსახურების ხასიათს;
- ბ) მესამე პირის რეპუტაციას;
- გ) რეგულირების სტატუსს;
- დ) AML/CFT კონტროლის მექანიზმებს;
- ე) მონაცემთა და ინფორმაციის დაცვის შესაძლებლობებს;
- ვ) სხვა შესაბამის რისკის ფაქტორებს.

20.3. მესამე პირის ჩართულობა არ ათავისუფლებს კომპანიას მისთვის კანონმდებლობით დაკისრებული AML/CFT ვალდებულებების შესრულებისგან.

21. ჩანაწერების შენახვა

21.1. კომპანია უზრუნველყოფს AML/CFT მიზნებისთვის საჭირო ინფორმაციისა და დოკუმენტაციის სათანადო აღრიცხვასა და შენახვას.

21.2. ჩანაწერები შეიძლება მოიცავდეს:

- ა) მომხმარებლის საიდენტიფიკაციო მონაცემებს;
- ბ) KYC/CDD დოკუმენტაციას;
- გ) რისკის შეფასების შედეგებს;
- დ) ტრანზაქციების შესახებ ინფორმაციას;
- ე) საექვო/უჩვეულო ოპერაციების განხილვის მასალებს;
- ვ) სანქციებისა და PEP სკრინინგის შედეგებს;
- ზ) გადაწყვეტილებებსა და შესაბამის შიდა ჩანაწერებს.

21.3. მონაცემებისა და ჩანაწერების შენახვის ვადა განისაზღვრება მოქმედი კანონმდებლობისა და კომპანიის შიდა წესების შესაბამისად.

22. კონფიდენციალურობა და ინფორმაციის გამჟღავნების აკრძალვა

22.1. AML/CFT პროცესების ფარგლებში მიღებული ინფორმაცია წარმოადგენს კონფიდენციალურ ინფორმაციას და მისი გამოყენება დასაშვებია მხოლოდ შესაბამისი უფლებამოსილების ფარგლებში.

22.2. კომპანია და მისი თანამშრომლები არ ახდენენ მომხმარებლისთვის იმ ინფორმაციის გამჟღავნებას, რომლის გამჟღავნებაც კანონმდებლობით აკრძალულია.

22.3. AML/CFT ინფორმაციაზე წვდომა აქვს მხოლოდ შესაბამისი უფლებამოსილების მქონე პირებს.

23. შიდა კონტროლი და პოლიტიკის შეფასება

23.1. კომპანია პერიოდულად აფასებს AML/CFT კონტროლის მექანიზმების ეფექტიანობას.

23.2. შეფასების ფარგლებში შეიძლება შემოწმდეს:

- ა) KYC/CDD პროცესები;
- ბ) მომხმარებელთა რისკის შეფასება;
- გ) ტრანზაქციების მონიტორინგი;
- დ) სანქციების სკრინინგი;
- ე) PEP-ის გამოვლენის პროცესი;

- ვ) საექსპოზიციო ოპერაციების განხილვა;
- ზ) ანგარიშგების პროცესი;
- თ) თანამშრომელთა ცოდნა და ტრენინგები;
- ი) ტექნიკური სისტემების მუშაობა.

23.3. გამოვლენილი ნაკლოვანებების შემთხვევაში კომპანია ადგენს შესაბამისი გამოსწორების ღონისძიებებს და აკონტროლებს მათ შესრულებას.

24. AML/CFT რისკის შეფასება ელექტრონული საფულის მომსახურებისთვის

24.1. კომპანია პერიოდულად ახორციელებს ელექტრონული საფულის მომსახურებასთან დაკავშირებული AML/CFT რისკების შეფასებას.

24.2. რისკის შეფასებისას გათვალისწინებული უნდა იქნეს:

- ა) მომხმარებელთა ტიპები;
- ბ) მომხმარებელთა გეოგრაფია;
- გ) მომსახურების დისტანციური ხასიათი;
- დ) ელექტრონული საფულის ფუნქციონალი;
- ე) თანხების შეტანისა და გატანის შესაძლებლობა;
- ვ) გადარიცხვები;
- ზ) კრიპტოაქტივების კონვერტაცია;
- თ) კრიპტოაქტივების შემოტანა და გატანა;
- ი) მესამე პირებთან ურთიერთობა;
- კ) ტექნოლოგიური და კიბერუსაფრთხოების რისკები;
- ლ) ახალი პროდუქტებისა და ტექნოლოგიების დანერგვასთან დაკავშირებული რისკები.

25. ახალი პროდუქტებისა და მომსახურებების AML/CFT შეფასება

25.1. ახალი პროდუქტის, მომსახურების, ტექნოლოგიის ან მნიშვნელოვანი ფუნქციონალის დანერგვამდე კომპანია აფასებს შესაბამის AML/CFT რისკებს.

25.2. რისკის შეფასების შედეგად განისაზღვრება საჭირო დამატებითი კონტროლის ღონისძიებები.

25.3. ახალი მომსახურების დანერგვა არ უნდა განხორციელდეს იმ შემთხვევაში, როდესაც შესაბამისი AML/CFT რისკების მართვის მექანიზმები სათანადოდ არ არის განსაზღვრული.

26. პოლიტიკის გადახედვა

26.1. წინამდებარე პოლიტიკა პერიოდულად გადაიხედება კანონმდებლობის, მარეგულირებელი მოთხოვნების, კომპანიის საქმიანობის, მომსახურებებისა და გამოვლენილი რისკების ცვლილების შესაბამისად.

26.2. პოლიტიკაში ცვლილებები მტკიცდება კომპანიის უფლებამოსილი ორგანოს/პირის მიერ.

26.3. პოლიტიკის ახალი რედაქცია ძალაში შედის დამტკიცების შემდეგ, მასში მითითებული თარიღიდან.

27. დასკვნითი დებულებები

27.1. კომპანია უზრუნველყოფს წინამდებარე AML/CFT პოლიტიკის მოთხოვნების შესრულებას ელექტრონული საფულის მომსახურების ყველა შესაბამის ეტაპზე.

27.2. პოლიტიკაში მოუგვარებელი საკითხები რეგულირდება საქართველოს მოქმედი კანონმდებლობისა და შესაბამისი მარეგულირებელი მოთხოვნების შესაბამისად.

27.3. წინამდებარე პოლიტიკის მოთხოვნების შესრულება სავალდებულოა კომპანიის შესაბამისი თანამშრომლებისა და უფლებამოსილი პირებისთვის.