კლიენტების მომსახურების რეგლამენტის
დანართი № 12

საბროკერო კომპანია “რიონი კაპიტალის”

შეთანხმება

პროგრამული უზრუნველყოფის „პირადი კაბინეტის“ გამოყენებისა და კლიენტების დისტანციური მომსახურების შესახებ

თბილისი
2025

წინამდებარე შეთანხმება პროგრამული უზრუნველყოფის „პირადი კაბინეტის“ გამოყენებისა და კლიენტების დისტანციური მომსახურების შესახებ (შემდგომში „შეთანხმება“) წარმოადგენს საბროკერო კომპანია „რიონი კაპიტალის“ (შემდგომში “ბროკერი”, “კომპანია”) კლიენტების მომსახურების რეგლამენტის (შემდგომში „რეგლამენტი“) დანართს და მის განუყოფელ ნაწილს. შეთანხმება ითვლება კლიენტთან დადებულად საქართველოს სამოქალაქო კოდექსის 69–ე მუხლის მე– 3 ნაწილის შესაბამისად კლიენტის მიერ საბროკერო მომსახურების ხელშეკრულებაზე ხელმოწერის მომენტიდან. აღნიშნული შეთანხმების შესრულება სავალდებულოა როგორც ბროკერისთვის, ასევე კლიენტისთვის მხარეებს შორის ხელშეკრულების დადების მომენტიდან.

მუხლი 1. ტერმინთა განმარტება

1.1. პირადი კაბინეტი - პროგრამული უზრუნველყოფა (ვებ-სერვისი და/ან მობილური აპლიკაცია/ინტერფეისი), რომელსაც ბროკერი აწვდის კლიენტს დისტანციური ურთიერთქმედებისთვის, მათ შორის შეტყობინებების გაგზავნისთვის, მომსახურების შესახებ ინფორმაციისა და რისკების მართვის სისტემის პარამეტრების მისაღებად, აგრეთვე იმ ფუნქციების გამოყენებისთვის, რომლებიც გათვალისწინებულია ხელშეკრულებითა და რეგლამენტით.

1.2. შეტყობინება - ელექტრონული შეტყობინება, რომელსაც მხარეები აგზავნიან პირადი კაბინეტის მეშვეობით (აგრეთვე რეგლამენტით გათვალისწინებული სხვა არხების გამოყენებით), მათ შორის შეტყობინებები, მოთხოვნები, განცხადებები, დადასტურებები, აგრეთვე **დავალებები** (იმ შემთხვევაში, თუ მათი გამოყენება დაშვებულია პირადი კაბინეტის ფუნქციონალით და ხელშეკრულების/რეგლამენტის პირობებით).

1.3. ელექტრონული დოკუმენტი - ინფორმაცია, რომელიც დაფიქსირებულია ელექტრონულ ფორმაში და შეიცავს სავალდებულო რეკვიზიტებს, რაც შესაძლებელს ხდის მისი შინაარსის, ავტორისა და ფორმირების მომენტის ერთმნიშვნელოვნად იდენტიფიცირებას; დადგენილი ელექტრონული დადასტურების წესის დაცვის შემთხვევაში შეიძლება ჰქონდეს იურიდიული ძალა, რომელიც უტოლდება ქაღალდზე გაფორმებულ დოკუმენტს.

1.4. ელექტრონული ხელმოწერა - ინფორმაცია ელექტრონულ ფორმაში, რომელიც მიბმულია სხვა ელექტრონულ მონაცემებთან ან ლოგიკურად არის მათთან დაკავშირებული და გამოიყენება ხელმომწერის იდენტიფიკაციისა და ელექტრონული დოკუმენტის მთლიანობის დასადასტურებლად; გამოიყენება საქართველოს მოქმედი კანონმდებლობისა და ბროკერის დოკუმენტების მნიშვნელობით.

1.5. კლიენტის ID - უნიკალური ასო-ციფრული იდენტიფიკატორი, რომელიც ენიჭება კლიენტს რეგისტრაციისას და უცვლელია მხარეთა ურთიერთობის მთელი პერიოდის განმავლობაში.

1.6. რმს (რისკების მართვის სისტემა) / რმს-ის პარამეტრები / რისკის ჯგუფი - ბროკერის რისკების მართვის სისტემის ელემენტები; პარამეტრები და რისკის ჯგუფები გამოიყენება კლიენტის პორტფელზე, ქვეყნდება/აისახება ბროკერის არხებში (მათ შორის პირად კაბინეტში), ხოლო კლიენტი ვალდებულია აკონტროლოს მათი დაცვა.

1.7. სსს (საინფორმაციო სავაჭრო სისტემები) და მონაცემები პირად კაბინეტში - კლიენტი ინფორმირებულია, რომ სსს-ში (მათ შორის API-ს მეშვეობით) წარმოდგენილი მონაცემები შეიძლება განსხვავდებოდეს პირად კაბინეტში ასახული მონაცემებისგან; **პრიორიტეტი ენიჭება პირადი კაბინეტის მონაცემებს**, რადგან ისინი გათვლილია რმს-ის მეთოდოლოგიებით და გამოიყენება რისკის კონტროლის, მარჟინალური მოთხოვნებისა და იძულებითი პოზიციების დახურვის მიზნით.

1.8. სხვა ტერმინები გამოიყენება რეგლამენტისა და გლოსარით (რეგლამენტის დანართი №16) დადგენილი მნიშვნელობით.

1.9. სხვა ტერმინები

ტერმინები, რომლებიც პირდაპირ არ არის განსაზღვრული წინამდებარე შეთანხმებით, გამოიყენება იმ მნიშვნელობებით, რომლებიც დადგენილია:

- საბროკერო მომსახურების ხელშეკრულებით;
- „Rioni Capital“-ის კლიენტთა მომსახურების რეგლამენტით;
- ბროკერის სხვა შიდა დოკუმენტებით;
- საქართველოს მოქმედი კანონმდებლობით და საქართველოს ეროვნული ბანკის ნორმატიული აქტებით.

მუხლი 2. ზოგადი დებულებები

2.1. წინამდებარე შეთანხმება განსაზღვრავს:
- **a.** პირადი კაბინეტის წვდომისა და გამოყენების წესებს;
- **b.** მხარეთა დისტანციური ურთიერთქმედების პირობებს პირადი კაბინეტის მეშვეობით;
- **c.** შეტყობინებების ფორმირების/გაგზავნისა და (შესაბამისი ფუნქციონალის არსებობის შემთხვევაში) ელექტრონული დოკუმენტების გამოყენების წესს;
- **d.** უსაფრთხოების მოთხოვნებს, პასუხისმგებლობასა და შეზღუდვებს, რომლებიც დაკავშირებულია პირადი კაბინეტის გამოყენებასთან.

2.2. პირადი კაბინეტი წარმოადგენს კლიენტის დისტანციური მომსახურების ნაწილს და გამოიყენება საბროკერო მომსახურების ხელშეკრულებასთან, კლიენტთა მომსახურების რეგლამენტთან და მათ დანართებთან ერთად. წინამდებარე შეთანხმებით მხარეთა უფლებები და ვალდებულებები განიმარტება სისტემურად, ხელშეკრულებისა და რეგლამენტის კონტექსტში.

2.3. პირადი კაბინეტის გამოყენების უფლება კლიენტს მიენიჭება **უსასყიდლოდ**; პირადი კაბინეტით სარგებლობა შეუძლიათ როგორც ფიზიკურ, ისე იურიდიულ პირებს.

2.4. ბროკერს უფლება აქვს ნებისმიერ დროს გააუმჯობესოს, შეცვალოს, გააფართოოს ან შეზღუდოს პირადი კაბინეტის ფუნქციონალური შესაძლებლობები, აგრეთვე შეცვალოს მისი გამოყენების წესები.

2.5. ბროკერს უფლება აქვს შეაჩეროს, შეზღუდოს ან შეწყვიტოს კლიენტის წვდომა პირად კაბინეტზე იმ შემთხვევაში, თუ გამოვლინდება კლიენტის მიერ ხელშეკრულების, რეგლამენტის, წინამდებარე შეთანხმების ან საქართველოს კანონმდებლობისა და ეროვნული ბანკის ნორმატიული აქტების მოთხოვნების დარღვევა (უსაფრთხოებისა და კომპლაიანსის მოთხოვნებთან შეუსაბამო მიზეზების გამჟღავნების ვალდებულების გარეშე).

მუხლი 3. წვდომის, იდენტიფიკაციისა და ავთენტიფიკაციის პირობები

3.1. პირად კაბინეტზე წვდომა კლიენტს ენიჭება რეგისტრაციისა და იდენტიფიკაციის პროცედურების გავლის შემდეგ, რომლებიც გათვალისწინებულია ხელშეკრულებით, რეგლამენტითა და საქართველოს ეროვნული ბანკის მოქმედი მოთხოვნებით, მათ შორის კლიენტის მობილური ტელეფონის ნომრისა ან სხვა სახის საშუალებებით პიროვნების და მისი ნებაყოფლობის დადასტურებისთვის

3.2. კლიენტი ვალდებულია:
- **a.** უზრუნველყოს საკონტაქტო მონაცემების აქტუალურობა;
- **b.** დაიცვას წვდომის საშუალებების კონფიდენციალურობა;
- **c.** არ გადასცეს მესამე პირებს ლოგინები, პაროლები, დადასტურების კოდები და სხვა ავთენტიფიკაციის საშუალებები;
- **d.** დაუყოვნებლივ აცნობოს ბროკერს წვდომის შესაძლო ხელყოფის შესახებ.

3.3. კლიენტი თავად იღებს ყველა რისკს იმ შედეგებზე, თუ მის მობილურ ტელეფონზე ან SIM-ბარათზე წვდომა მიიღეს მესამე პირებმა.

3.4. ბროკერს უფლება აქვს გამოიყენოს კლიენტის ნებაყოფლობის დამატებითი გადამოწმების და/ან ქმედებების ავთენტურობის დადასტურების ზომები შეტყობინებებსა და ქმედებებზე, მათ შორის დადასტურება სატელეფონო ზარით, ელექტრონული ფოსტით და სხვა შიდა სისტემების მეშვეობით განხორციელებული გადამოწმების საშუალებებით.

3.5. კლიენტის დაცვისა და უსაფრთხოების მიზნით ბროკერი აწესებს და იყენებს, მათ შორის, შემდეგ ზომებს:

- **a.** ავთენტიფიკაციისა და/ან დადასტურების წარუმატებელი მცდელობების რაოდენობის ლიმიტს (არაუმეტეს 5-ისა), შემდგომი დროებითი ბლოკირების გამოყენებით;
- **b.** ბლოკირების/განბლოკვის წესებსა და წვდომის აღდგენის პროცედურებს რისკზე დაფუძნებული მიდგომის შესაბამისად;
- **c.** სესიის ავტომატურ ტაიმ-აუტს უმოქმედობის შემთხვევაში (როგორც წესი, არაუმეტეს 5 წუთისა; საჭიროების შემთხვევაში - არაუმეტეს 10 წუთისა გარკვეული კატეგორიის მომხმარებლებისთვის რისკზე დაფუძნებული მიდგომის შესაბამისად);
- **d.** სესიის დაცვის ზომებს უკანონო დაუფლებისა და მანიპულაციისგან, აგრეთვე ორფაქტორიანი ავთენტიფიკაციის (2FA) ფაქტორების დამოუკიდებლობის მოთხოვნას.

მუხლი 4. საინფორმაციო შეტყობინებები პირად კაბინეტში

4.1. საინფორმაციო შეტყობინებები, რომლებიც არ საჭიროებს კლიენტის დადასტურებას

4.1.1. ისეთ შეტყობინებებს, რომლებიც არ საჭიროებს კლიენტის დადასტურებას, მიეკუთვნება, მათ შორის:

- კლიენტის პორტფელში მიმდინარე მოვლენების შესახებ შეტყობინებები;
- რმს-ის პარამეტრების, მარჟინალური მოთხოვნების და რისკების შესახებ შეტყობინებები;
- რეგლამენტის, ტარიფების და მომსახურების პირობების ცვლილებების შესახებ შეტყობინებები;
- ტექნიკური და სერვისული ხასიათის შეტყობინებები.

4.1.2. აღნიშნულ შეტყობინებებს აქვთ მხოლოდ საინფორმაციო ხასიათი და არ საჭიროებენ კლიენტის ცალკეულ დადასტურებას, თუ შეტყობინების ტექსტში პირდაპირ სხვა რამ არ არის მითითებული.

4.2. შეტყობინებები, რომლებიც საჭიროებს გაცნობაზე დადასტურებას

4.2.1. ისეთ შეტყობინებებს, რომლებიც საჭიროებს კლიენტის მიერ გაცნობაზე დადასტურებას, მიეკუთვნება, მათ შორის:

- რისკების გამჟღავნება;
- მომსახურების პირობების არსებითი ცვლილებების შესახებ შეტყობინებები;
- ახალი შეზღუდვების, მოთხოვნების ან პროცედურების დანერგვის შესახებ შეტყობინებები.

4.2.2. გაცნობაზე დადასტურება ხორციელდება პირად კაბინეტში დადგენილი მექანიზმის მეშვეობით (SSO / ორფაქტორიანი ავთენტიფიკაცია (2FA) / სხვა მეთოდი) და ფიქსირდება ბროკერის ჟურნალებში.

მუხლი 5. იურიდიულად მნიშვნელოვანი ქმედებები და ელექტრონული დოკუმენტები პირად კაბინეტში

5.1. იურიდიული მნიშვნელობის ზოგადი პრინციპები

5.1.1. მხარეები აღიარებენ, რომ კლიენტის მიერ პირადი კაბინეტის გამოყენებით განხორციელებულ ქმედებებს, შეტყობინებებსა და ფორმირებულ ელექტრონულ დოკუმენტებს, რომლებიც დადგენილი წესით არის დადასტურებული, შეიძლება ჰქონდეს იურიდიული შედეგები, მათ შორის მხარეთა უფლებებისა და ვალდებულებების წარმოშობა, ცვლილება და შეწყვეტა, თუ ეს გათვალისწინებულია ხელშეკრულებით, რეგლამენტითა და საქართველოს მოქმედი კანონმდებლობით.

5.1.2. ელექტრონულ დოკუმენტებს, რომლებიც ფორმირებულია და დადასტურებულია პირადი კაბინეტის მეშვეობით წინამდებარე შეთანხმებით დადგენილი წესით, აქვთ იურიდიული ძალა, რომელიც უტოლდება საკუთარი ხელით ხელმოწერილ დოკუმენტებს, თუ სხვა რამ პირდაპირ არ არის დადგენილი კანონმდებლობის იმპერატიული ნორმებით.

5.1.3. კლიენტის ნებაყოფლობის დადასტურების მიზნით იურიდიულად მნიშვნელოვანი ქმედებების განხორციელებისას გამოიყენება ელექტრონული დადასტურების საშუალებები, მათ შორის ელექტრონული ხელმოწერა, SSO-ავთენტიფიკაცია, ორფაქტორიანი ავთენტიფიკაცია (2FA) და სხვა მეთოდები, რომლებიც ბროკერის მიერ არის მიჩნეული დასაშვებად რეგულატორის მოთხოვნებისა და რისკზე დაფუძნებული მიდგომის გათვალისწინებით.

5.1.4. ელექტრონული ხელმოწერის გამოყენების წესი, გამოყენებადი ელექტრონული ხელმოწერების სახეები, მხარეთა უფლებები და ვალდებულებები, აგრეთვე პირობები, რომელთა დაკმაყოფილებისას ელექტრონული ხელმოწერა უტოლდება საკუთარი ხელით ხელმოწერას, განისაზღვრება ელექტრონული ხელმოწერის გამოყენების შესახებ ცალკე შეთანხმებით, რომელიც წარმოადგენს ბროკერის ხელშეკრულებითი დოკუმენტაციის განუყოფელ ნაწილს.

5.2. იურიდიულად მნიშვნელოვანი ქმედებების სახეები

5.2.1. პირადი კაბინეტის მეშვეობით კლიენტის მიერ განხორციელებულ იურიდიულად მნიშვნელოვან ქმედებებს მიეკუთვნება, მათ შორის (შესაბამისი ფუნქციონალის არსებობის შემთხვევაში):

- **a.** ხელშეკრულებების, შეთანხმებების, დანართების, შეტყობინებებისა და ინფორმაციის გამჟღავნების დოკუმენტების აქცეპტი;
- **b.** კლიენტის განცხადებებისა და შეტყობინებების წარდგენა;
- **c.** თანხმობებისა და უარების, აგრეთვე სხვა ნებაყოფლობითი გამოვლინებების დადასტურება;
- **d.** დავალებების წარდგენა (სავაჭრო და/ან არასავაჭრო), თუ ეს გათვალისწინებულია ხელშეკრულებითა და რეგლამენტით;
- **e.** სხვა ქმედებები, რომლებიც პირადი კაბინეტის ინტერფეისში პირდაპირ არის მითითებული როგორც დადასტურებას დაქვემდებარებული და იურიდიული შედეგების გამომწვევი.

5.2.2. შეტყობინებებისა და ელექტრონული დოკუმენტების კონკრეტული ჩამონათვალი, რომლებიც იურიდიულად მნიშვნელოვანად ითვლება, განისაზღვრება წინამდებარე შეთანხმების დანართი №1-ით და შეიძლება შეიცვალოს ბროკერის მიერ პირადი კაბინეტის ფუნქციონალის განვითარების პროცესში.

5.3. იურიდიულად მნიშვნელოვანი ქმედების განხორციელების წესი

5.3.1. პირადი კაბინეტის მეშვეობით იურიდიულად მნიშვნელოვანი ქმედების განხორციელება მოიცავს შემდეგ ეტაპებს:

- **a.** ქმედების ინიცირება კლიენტის მიერ პირადი კაბინეტის ინტერფეისში;
- **b.** მონაცემებისა და წვდომის უფლებების ავტომატური ვალიდაცია;

c. კლიენტის ნებაყოფლობის დადასტურება დადგენილი ელექტრონული დადასტურების საშუალებით;

d. ქმედების რეგისტრაცია ბროკერის სისტემებში უნიკალური იდენტიფიკატორის მინიჭებით;

e. ქმედების სტატუსის ჩვენება კლიენტისთვის.

5.3.2. კლიენტის ნებაყოფლობის დადასტურება ხორციელდება იმ მეთოდის გამოყენებით, რომელიც ბროკერის მიერ არის განსაზღვრული შესაბამისი ქმედების სახისთვის, რისკის დონის, რმს-ის მოთხოვნებისა და მოქმედი ნორმატიული აქტების გათვალისწინებით.

5.3.3. იურიდიულად მნიშვნელოვანი ქმედება ჩაითვლება კლიენტის მიერ განხორციელებულად იმ მომენტიდან, როდესაც წარმატებით დასრულდება დადასტურების ეტაპი და ქმედება დარეგისტრირდება პირად კაბინეტში, თუ სხვა რამ პირდაპირ არ არის დადგენილი ხელშეკრულებით ან რეგლამენტით.

5.4. ჟურნალიზაცია და მტკიცებულებითი ძალა

5.4.1. ბროკერი უზრუნველყოფს კლიენტის იურიდიულად მნიშვნელოვანი ქმედებების ფიქსაციას მოვლენათა ჟურნალებში (audit trail), მათ შორის:

- კლიენტის იდენტიფიკატორი;
- ქმედების თარიღი და დრო;
- ქმედების ან დოკუმენტის სახე;
- დადასტურების მეთოდი;
- ქმედების შედეგი.

5.4.2. მოვლენათა ჟურნალები და პირადი კაბინეტის სისტემური ჩანაწერები წარმოადგენს ქმედებების ფაქტისა და შინაარსის მტკიცებულებას და შეიძლება გამოყენებულ იქნეს ბროკერისა და კლიენტის მიერ დავების გადაწყვეტისას, პერსონალური მონაცემების დაცვის შესახებ კანონმდებლობის მოთხოვნების დაცვის პირობით.

5.5. განსაკუთრებული წესები რისკთან დაკავშირებული ქმედებებისთვის

5.5.1. კლიენტი ადასტურებს, რომ რისკების მართვის სისტემის პარამეტრები, მათ შორის მარჟინალური მოთხოვნები და პოზიციების იძულებითი დახურვის პირობები, ასახულია პირად კაბინეტში და კლიენტი ვალდებულია დამოუკიდებლად აკონტროლოს მათი დაცვა.

5.5.2. ღია პოზიციების იძულებითი დახურვის პირობების დადგომისას ბროკერი მოქმედებს კლიენტის პირობითი დავალების საფუძველზე, რომელიც მოცემულია ხელშეკრულებაში და/ან მის დანართებში, კლიენტის დამატებითი დადასტურების მიღების გარეშე.

5.6. ინფორმაციის კლიენტამდე მიყვანის მომენტი

შეტყობინებები და ელექტრონული დოკუმენტები, რომლებიც განთავსებულია პირად კაბინეტში, ჩაითვლება კლიენტისათვის მიწოდებულად მათი პირად კაბინეტში განთავსების მომენტიდან, კლიენტის მიერ პირად კაბინეტში ფაქტობრივი შესვლის მიუხედავად, თუ სხვა რამ არ არის გათვალისწინებული ხელშეკრულებით ან კანონმდებლობის იმპერატიული ნორმებით.

მუხლი 6. დისტანციური ელექტრონული ურთიერთქმედება, მონაცემთა პრიორიტეტი და ინფორმაციული უსაფრთხოება

6.1. შეტყობინებების გაცვლის წესი პირადი კაბინეტის მეშვეობით

6.1.1. პირადი კაბინეტის მეშვეობით გაგზავნილი შეტყობინებები ჩაითვლება კლიენტისათვის მიწოდებულად მათი პირადი კაბინეტის ინტერფეისში განთავსების/გამოსახვის მომენტიდან (თუ კონკრეტული შეტყობინებებისათვის სხვა რამ პირდაპირ არ არის დადგენილი ხელშეკრულებით/რეგლამენტით).

6.1.2. ბროკერს შეუძლია გამოიყენოს პირადი კაბინეტი, როგორც პრიორიტეტული არხი კლიენტის ინფორმირებისთვის შემდეგის შესახებ:

- ტარიფების/მომსახურების პარამეტრების ცვლილებები და ასეთი ცვლილებების სტატუსი;
- რისკების მართვის სისტემის მოვლენები (მარჟინალური მოთხოვნები, რისკის პარამეტრები, იძულებითი დახურვა და სხვა);
- მომსახურებასთან დაკავშირებული სხვა ინფორმაცია.

6.1.3. ბროკერს უფლება აქვს გაუგზავნოს კლიენტს შეტყობინებები ასევე ჩატის, ელექტრონული ფოსტისა და რეგლამენტით გათვალისწინებული სხვა არხების მეშვეობით; კონკრეტული არხი შეიძლება განისაზღვროს შეტყობინების კრიტიკულობისა და ტექნიკური ხელმისაწვდომობის მიხედვით.

6.2. ინფორმაციული შეუსაბამობები და მონაცემთა პრიორიტეტი

6.2.1. კლიენტი ადასტურებს, რომ ინფორმირებულია ინფორმაციულ ტექნიკური უზრუნველყოფის მონაცემებსა (მათ შორის API-ის გამოყენებით) და პირადი კაბინეტის მონაცემებს შორის შესაძლო შეუსაბამობების შესახებ.

6.2.2. მხარეები შეთანხმდნენ, რომ პრიორიტეტი ენიჭება პირად კაბინეტში გამოქვეყნებულ მონაცემებს, ვინაიდან ისინი გამოითვლება რისკების მართვის სისტემის მეთოდოლოგიების შესაბამისად და გამოიყენება რისკის კონტროლისთვის, მარჟინალური მოთხოვნების წარდგენისთვის და პოზიციების იძულებითი დახურვისთვის.

6.2.3. კლიენტი იღებს ასეთ შეუსაბამობებთან დაკავშირებულ რისკს და ვალდებულია, შეუსაბამობის შემთხვევაში, იხელმძღვანელოს პირადი კაბინეტის მონაცემებით.

6.3. ინფორმაციული უსაფრთხოების ინციდენტები, წვდომის ხელყოფა და ქმედებების წესი

6.3.1. ინფორმაციული უსაფრთხოების ინციდენტად მიიჩნევა მოვლენა (ან მოვლენათა ერთობლიობა), რომელმაც გამოიწვია ან შეიძლება გამოიწვიოს:

- პირად კაბინეტზე უნებართვო წვდომა;
- მონაცემების გაჟონვა/დამახინჯება/განადგურება;
- სერვისის ხელმისაწვდომობის დარღვევა;
- თაღლითური ოპერაციები ან ასეთი ოპერაციების მცდელობები.

6.3.2. ხელყოფის ნიშნებად მიიჩნევა, მათ შორის:

- უნებართვო შესვლები/შესვლის მცდელობები;
- საკონტაქტო მონაცემების მოულოდნელი ცვლილებები;
- შეტყობინებები ქმედებების შესახებ, რომლებიც კლიენტს არ განუხორციელებია;
- ფიშინგზე/მავნე პროგრამულ უზრუნველყოფაზე ეჭვი კლიენტის მოწყობილობაზე.

6.3.3. კლიენტი ვალდებულია დაუყოვნებლივ აცნობოს ბროკერს ხელმისაწვდომი საკომუნიკაციო არხების მეშვეობით, თუ:

- კლიენტმა დაკარგა კონტროლი ტელეფონის ნომერზე/SIM-ბარათზე;
- არსებობს პაროლის/დადასტურების კოდების ხელყოფის ეჭვი;
- კლიენტმა აღმოაჩინა ოპერაციები ან ქმედებები, რომლებიც თავად არ განუხორციელებია.

6.3.4. კლიენტი იღებს ყველა რისკსა და შედეგს იმ შემთხვევაში, თუ მის მობილურ ტელეფონზე ან SIM-ბარათზე წვდომა მიიღეს მესამე პირებმა.

6.3.5. კონტროლის აღდგენამდე კლიენტი ვალდებულია შეწყვიტოს პირადი კაბინეტის გამოყენება პოტენციურად ხელყოფილი მოწყობილობებიდან, შეცვალოს პაროლი/საიდუმლო მონაცემები (თუ უსაფრთხო არხი ხელმისაწვდომია) და მიჰყვეს ბროკერის ინსტრუქციებს წვდომის აღდგენის მიზნით.

6.3.6. ბროკერს უფლება აქვს დაუყოვნებლივ:

- შეზღუდოს პირად კაბინეტზე წვდომა;
- მოითხოვოს შეტყობინებების/ქმედებების ავთენტურობის დამატებითი გადამოწმება (მათ შორის ტელეფონით/ელექტრონული ფოსტით დადასტურება და კლიენტის მონაცემებთან შიდა სისტემებში არსებული პარამეტრების შედარება).

6.3.7. ბროკერს უფლება აქვს დროებით შეაჩეროს კლიენტის ცალკეული დავალებების/ქმედებების დამუშავება უსაფრთხოების და/ან კომპლაიანსის შემოწმებების დასრულებამდე.

6.3.8. ინციდენტის გამოსაკვლევად გამოიყენება მომხმარებელთა ქმედებების ჟურნალები, API-ის გამოძახებების ჟურნალები და ბროკერის სხვა სისტემური ჩანაწერები კანონმდებლობის მოთხოვნების დაცვის პირობით.

6.3.9. ბროკერი ატყობინებს კლიენტს მიმართვის/ინციდენტის სტატუსის შესახებ პირადი კაბინეტის და/ან რეგლამენტით გათვალისწინებული სხვა საკომუნიკაციო არხების მეშვეობით იმ მოცულობით, რომელიც დასაშვებია უსაფრთხოების პოლიტიკებითა და AML/კომპლაიანსის მოთხოვნებით.

6.3.10. წვდომის აღდგენა ხორციელდება ბროკერის მიერ დადგენილი პროცედურის შესაბამისად (წინამდებარე შეთანხმების დანართი №3): კლიენტის იდენტიფიკაცია, ტელეფონის ნომერზე/ანგარიშზე უფლებების დადასტურება, რისკის წყაროს დამატებითი შემოწმება (საჭიროების შემთხვევაში), საიდუმლო მონაცემების შეცვლა, აქტიური სესიების განულება.

6.3.11. კლიენტი აცნობიერებს და ეთანხმება, რომ ბროკერი არ არის ვალდებული დეტალურად გაამჟღავნოს ავტორიზაციის/SSO/2FA სისტემების არქიტექტურა, დაცვის მეთოდები და შიდა რეაგირების პროცედურები, თუ ასეთი გამჟღავნება ქმნის დამატებით უსაფრთხოების რისკებს.

მუხლი 7. კლიენტის ვალდებულებები პირადი კაბინეტის გამოყენებისას

7.1. კლიენტი ვალდებულია ყოველდღიურად აკონტროლოს რისკების მართვის სისტემის პარამეტრები პირად კაბინეტში, დროულად მოახდინოს რეაგირება მარჟინალურ მოთხოვნებზე, უზრუნველყოს უზრუნველყოფის შენარჩუნება და გაითვალისწინოს საბაზრო რისკები რეგლამენტისა და ხელშეკრულებით დადგენილი მოცულობით.

7.2. კლიენტი ვალდებულია დაიცვას ინფორმაციული უსაფრთხოების მოთხოვნები, მათ შორის:

- გამოიყენოს ოპერაციული სისტემების, ბრაუზერებისა და აპლიკაციების აქტუალური ვერსიები;
- არ გამოიყენოს ხელყოფილი მოწყობილობები;
- დაუყოვნებლივ აცნობოს ბროკერს ხელყოფის ეჭვის არსებობის შემთხვევაში.

7.3. კლიენტი აცნობიერებს და ეთანხმება, რომ პირად კაბინეტზე წვდომა მობილური აპლიკაციების და/ან მესამე პირების პროგრამული საშუალებების მეშვეობით ხორციელდება კლიენტის

რისკით; ბროკერი არ აგებს პასუხს ასეთი აპლიკაციების/საშუალებების გამართულობაზე ბროკერის კონტროლის ზონის ფარგლებს გარეთ.

მუხლი 8. ბროკერის ვალდებულებები: უსაფრთხოება, ჟურნალიზაცია, მონაცემთა შენახვა

8.1. ბროკერი იყენებს ორგანიზაციულ და ტექნიკურ დაცვის ზომებს, რომლებიც შეესაბამება საქმიანობის რისკ-პროფილსა და რისკების მართვის სისტემის შიდა დოკუმენტებს, მათ შორის:
- მონაცემთა დაშიფვრა „გადაცემისას“ (TLS 1.2+) და „შენახვისას“;
- უფლებამოსილი პირების წვდომის გამიჯვნა მონაცემებსა და დოკუმენტებზე დონეების მიხედვით;
- მნიშვნელოვანი ქმედებებისა და მოვლენების სრული ჟურნალიზაცია (audit trail) - შესვლები/გასვლები, კლიენტის მონაცემების ცვლილებები, back-office/risk/trading ქმედებები, კონფიგურაციების ცვლილებები და სხვა - დროის, მომხმარებლის/სისტემის, შედეგისა და ტექნიკური პარამეტრების ფიქსაციით; ამასთან, ჟურნალი არ ექვემდებარება განვლილი თარიღით ცვლილებას.

8.2. ბროკერი უზრუნველყოფს სისტემებს შორის მონაცემთა შედარებას (reconciliation) და შეუსაბამობების გამოძიებას იმ კონტურებში, რომლებიც უკავშირდება პირად კაბინეტსა და back-office/რისკ-კონტურებს.

მუხლი 9. პასუხისმგებლობის შეზღუდვები და გარანტიებზე უარი

9.1. ბროკერი არ აგებს პასუხს პირადი კაბინეტის გამოყენების დაგვიანებაზე, შეფერხებებზე ან შეუძლებლობაზე, რომლებიც პირდაპირ ან ირიბად წარმოიშვა მესამე პირების ქმედებების/უმოქმედობის და/ან სატრანსპორტო-საინფორმაციო არხების გაუმართაობის შედეგად ბროკერის კონტროლის ზონის ფარგლებს გარეთ.

9.2. ბროკერი არ აგებს პასუხს პირდაპირ ან ირიბ ზარალზე, რომელიც წარმოიშვა პირადი კაბინეტის გამოყენების ან მისი გამოყენების შეუძლებლობის შედეგად, მათ შორის მონაცემთა შეცდომების/გაუმართაობის/წაშლის/წვდომის დაკარგვის/მესამე პირების მიერ უნებართვო წვდომის შემთხვევებში, თუ სხვა რამ არ გამომდინარეობს მოქმედი სამართლის იმპერატიული ნორმებიდან.

9.3. ბროკერს უფლება აქვს (თუმცა არ არის ვალდებული) გაუგზავნოს კლიენტს რისკებთან დაკავშირებული შეტყობინებები; შეტყობინების არარსებობა არ ათავისუფლებს კლიენტს რისკის კონტროლისა და უზრუნველყოფის შენარჩუნების ვალდებულებისგან.

მუხლი 10. დასკვნითი დებულებები

10.1. წინამდებარე შეთანხმება ძალაში შედის კლიენტის მიერ მასზე მიერთების მომენტიდან (აქცეპტი პირად კაბინეტში/ხელმოწერა/დადგენილი წესით დადასტურება) და მოქმედებს ხელშეკრულების ვადის განმავლობაში, თუ იგი ადრე არ შეწყდა ხელშეკრულებით, რეგლამენტით ან კანონით გათვალისწინებული საფუძვლებით.

10.2. ბროკერს უფლება აქვს შეიტანოს ცვლილებები წინამდებარე შეთანხმებაში (მათ შორის პირადი კაბინეტის ფუნქციონალის, საქართველოს ეროვნული ბანკის მოთხოვნების და/ან უსაფრთხოების ზომების ცვლილების გამო). შეთანხმების მოქმედი რედაქცია კლიენტს

მიეწოდება პირადი კაბინეტის და/ან რეგლამენტით გათვალისწინებული სხვა არხების მეშვეობით.

10.3. იმ ნაწილში, რომელიც არ არის მოწესრიგებული წინამდებარე შეთანხმებით, მხარეები ხელმძღვანელობენ ხელშეკრულებით, რეგლამენტითა და საქართველოს მოქმედი კანონმდებლობით.

10.4. წინამდებარე შეთანხმებასთან დაკავშირებული დავები და უთანხმოებები ექვემდებარება გადაწყვეტას ხელშეკრულებით/რეგლამენტით და საქართველოს მოქმედი კანონმდებლობით დადგენილი წესით.

11. დანართები

პროგრამული უზრუნველყოფის „პირადი კაბინეტის“ გამოყენებისა და კლიენტების დისტანციური მომსახურების შესახებ **შეთანხმების**

დანართი № 1

წინამდებარე დანართი განსაზღვრავს შეტყობინებებისა და ელექტრონული დოკუმენტების ჩამონათვალს, რომლებიც შეიძლება ფორმირდებოდეს, იგზავნებოდეს და დასტურებოდეს კლიენტისა და ბროკერის მიერ პირადი კაბინეტის გამოყენებით.

ხელმისაწვდომი შეტყობინებებისა და ელექტრონული დოკუმენტების კონკრეტული შემადგენლობა დამოკიდებულია:

- კლიენტის სტატუსზე (ფიზიკური პირი / იურიდიული პირი);
- პირადი კაბინეტის მიერთებული ფუნქციონალის მოცულობაზე;
- საქართველოს მოქმედი კანონმდებლობისა და საქართველოს ეროვნული ბანკის ნორმატიული აქტების მოთხოვნებზე;
- ბროკერის შიდა პროცედურებზე (მათ შორის რისკების მართვის სისტემა და AML/CTF).

აღნიშნული შეტყობინებებისა და ელექტრონული დოკუმენტების ფორმირება და დადასტურება ხორციელდება მხოლოდ ხელშეკრულების, რეგლამენტისა და წინამდებარე შეთანხმების ფარგლებში.

პირად კაბინეტში ფორმირებადი შეტყობინებებისა და ელექტრონული დოკუმენტების ჩამონათვალი და მათი იურიდიული მნიშვნელობა

№№	დასახელება	იურიდიულად მნიშვნელოვანი ქმედება	დადასტურების მეთოდი
1.	პირად კაბინეტში შესვლა	დიახ	ორფაქტორიანი ავთენტიფიკაცია (2FA)
2.	დავალება საკონტაქტო მონაცემების შეცვლაზე	დიახ	ორფაქტორიანი ავთენტიფიკაცია (2FA)
3.	დავალება საიდენტიფიკაციო დოკუმენტის (პასპორტის) შეცვლაზე	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
4.	ანკეტური მონაცემების შეცვლა	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
5.	განცხადება ტარიფული გეგმის შეცვლაზე	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
6.	დავალება ფულადი სახსრების გატანაზე	დიახ	ორფაქტორიანი ავთენტიფიკაცია (2FA)
7.	დავალება ფასიანი ქაღალდების გატანაზე	დიახ	ორფაქტორიანი ავთენტიფიკაცია (2FA)
8.	დავალება გარიგებაზე	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
9.	განცხადება კლიენტის კატეგორიის შეცვლაზე	დიახ	ორფაქტორიანი ავთენტიფიკაცია (2FA)
10.	განცხადება ფასიანი ქაღალდების სესხის პროგრამასთან მიერთების შესახებ	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
11.	განცხადება მარჟინალური გარიგებების დაშვების შესახებ	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
12.	განცხადება „Short“ გარიგებების დაშვების შესახებ	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)
13.	დავალება პორტფელის რისკის დონის შეცვლაზე	დიახ	ავთენტიფიკაცია პირად კაბინეტში (SSO)

პროგრამული უზრუნველყოფის „პირადი კაბინეტის“ გამოყენებისა და
კლიენტების დისტანციური მომსახურების შესახებ **შეთანხმების**

დანართი № 2

კლიენტის მოწყობილობებისა და პროგრამული უზრუნველყოფის მინიმალური მოთხოვნები

1. ზოგადი მოთხოვნები

1.1. კლიენტი ვალდებულია გამოიყენოს პირადი კაბინეტი მხოლოდ იმ მოწყობილობებიდან, რომლებიც:

- იმყოფება მის კონტროლქვეშ;
- დაცულია უნებართვო წვდომისგან;
- არ შეიცავს მავნე პროგრამულ უზრუნველყოფას.

1.2. კლიენტი დამოუკიდებლად აგებს პასუხს:

- გამოყენებული მოწყობილობის უსაფრთხოებაზე;
- ოპერაციული სისტემისა და ბრაუზერის აქტუალობაზე;
- უსაფრთხოების განახლებების დაყენებაზე.

2. შეზღუდვები და გაფრთხილებები

2.1. ბროკერი არ იძლევა პირადი კაბინეტის გამართული მუშაობის გარანტიას შემდეგ შემთხვევებში:

- მოძველებული ბრაუზერებისა და ოპერაციული სისტემების გამოყენებისას;
- მოდიფიცირებული ან გატეხილი მოწყობილობების გამოყენებისას;
- მესამე მხარის განახლებების გამოყენებისას, რომლებიც გავლენას ახდენენ უსაფრთხოებაზე.

2.2. საჯარო ან არასაიმედო ქსელების (public Wi-Fi) გამოყენება კლიენტის მიერ ხორციელდება საკუთარი რისკით.

პროგრამული უზრუნველყოფის „პირადი კაბინეტის“ გამოყენებისა და
კლიენტების დისტანციური მომსახურების შესახებ **შეთანხმების**

დანართი № 3

პირად კაბინეტზე წვდომის ბლოკირების, აღდგენის და შეწყვეტის წესი

3. წვდომის ბლოკირების საფუძვლები

1.3. ბროკერს უფლება აქვს დროებით ან მუდმივად შეზღუდოს კლიენტის წვდომა პირად კაბინეტზე შემდეგ შემთხვევებში:

- წვდომის ხელყოფის ნიშნების გამოვლენა;
- ავთენტიფიკაციის წარუმატებელი მცდელობების დასაშვები რაოდენობის გადაჭარბება;
- კლიენტის მიერ ხელშეკრულების, რეგლამენტის ან წინამდებარე შეთანხმების პირობების დარღვევა;
- რეგულატორის ან კომპეტენტური ორგანოების მოთხოვნა;
- რისკების მარღვის სისტემის ან AML/CTF-ის ფარგლებში მომატებული რისკის გამოვლენა.

4. დროებითი ბლოკირების წესი

2.3. დროებითი ბლოკირება შეიძლება გამოყენებულ იქნას ავტომატურად ან არაავტომატურად.

2.4. კლიენტი ბლოკირების შესახებ ინფორმირდება ხელმისაწვდომი საკომუნიკაციო არხების მეშვეობით, თუ ასეთი შეტყობინება არ ეწინააღმდეგება უსაფრთხოებისა და კომპლაიანსის მოთხოვნებს.

5. წვდომის აღდგენა

3.1. წვდომის აღდგენა ხორციელდება შემდეგის შემდეგ:

- კლიენტის იდენტიფიკაცია;
- საკონტაქტო მონაცემებზე კონტროლის დადასტურება;
- რისკზე დაფუძნებული მიდგომის შესაბამისად დამატებითი შემოწმებების ჩატარება.

3.2. ბროკერს უფლება აქვს:

- მოითხოვოს დამატებითი დოკუმენტები;
- შეცვალოს ავთენტიფიკაციის მეთოდები;
- გაანულოს აქტიური სესიები.

6. წვდომის შეწყვეტა

4.1. პირად კაბინეტზე წვდომა წყდება ხელშეკრულების შეწყვეტის შემთხვევაში, აგრეთვე სხვა შემთხვევებში, რომლებიც გათვალისწინებულია რეგლამენტითა და კანონმდებლობით.

4.2. წვდომის შეწყვეტა არ ათავისუფლებს მხარეებს მანამდე წარმოშობილი ვალდებულებების შესრულებისგან.