Հաստատված է
«ԷՓՐԻՔՈԹ ԿԱՊԻՏԱԼ»
փակ բաժնետիրական ընկերության
Գործադիր տնօրենի
10.03.2026թ.-ի թիվ ԷԿ ՀՊ 10/03/2026-1 որոշմամբ
Գործադիր տնօրեն՝ Վաչիկ Գևորգյան

«ԷՓՐԻՔՈԹ ԿԱՊԻՏԱԼ» ՓԱԿ ԲԱԺՆԵՏԻՐԱԿԱՆ ԸՆԿԵՐՈՒԹՅԱՆ

ՀԱՄԱԿԱՐԳԻ ԱՆՎՏԱՆԳ ՕԳՏԱԳՈՐԾՄԱՆ ԿԱՆՈՆՆԵՐ

ԵՐԵՎԱՆ 2026թ.

1. Ընդհանուր դրույթներ

1.1 Նպատակը և կարգավորման առարկան

«Էփրիքոթ Կապիտալ» ՓԲԸ-ի (այսուհետ՝ Ընկերություն) Համակարգի անվտանգ օգտագործման կանոնները (այսուհետ՝ Կանոններ) սահմանում են Ընկերության կողմից մատուցվող ծառայությունների շրջանակում կիրառվող ծրագրային ապահովումների և տեղեկատվական համակարգերի անվտանգ օգտագործման պահանջները: Կանոնների նպատակն է նվազագույնի հասցնել տեղեկատվական անվտանգության պատահարների բացասական ազդեցությունը, Ընկերության տեղեկատվական համակարգերում չարտոնված մուտքի ռիսկերը, ինչպես նաև ապահովել ոչ հրապարակային տվյալների պատշաճ պաշտպանությունը:

1.2. Սահմանումներ և մեկնաբանում

1.2.1 Սույն Քաղաքականության մեջ օգտագործվող հիմնական հասկացություններն են.

- **«Հաճախորդ»**՝ այն անձը (այդ թվում վերջինիս ներկայացուցիչը), որն օգտվում է Ընկերության կողմից մատուցվող ներդրումային ծառայություններից և/կամ ոչ հիմնական ծառայություններից և/կամ կրիպտոակտիվներով մատուցվող ծառայություններից.
- **«Համակարգ»**՝ Համապատասխան ինտերֆեյսով էլեկտրոնային (ցանցային, ինտերնետ) գործիք հանդիսացող հեռախոսային հավելված կամ «Առևտրային հարթակ Beta)» մոդուլ (հղումը տրված է www.apricotcapital.am կայքում) որին հասանելիություն ունենալով Հաճախորդները կարող են փոխանցել գործարքների կնքման Պատվերներն ի կատարումն, Հաճախորդին ներկայացնել Պատվերների, կատարված գործարքների վերաբերյալ և այլ տեղեկություններ.
- **«Տեղեկատվական անվտանգության պատահար»**՝ միջադեպ, որը փաստացի վտանգում է կամ հավանական է, որ կվտանգի Համակարգի կամ Համակարգի կողմից մշակվող, պահվող կամ փոխանցվող տեղեկատվության ամբողջականությունը, հասանելիությունը կամ գաղտնիությունը կամ հանդիսանում է անվտանգության կանոնների, ընթացակարգերի և քաղաքականության խախտում կամ տվյալների ամբողջականության խափանմանն ուղղված սպառնալիք:

1.2.2. Սույն Կանոններում չսահմանված հասկացությունները օգտագործվում են ՀՀ օրենսդրությամբ, այդ թվում՝ «Արժեթղթերի շուկայի մասին» ՀՀ օրենքի, ինչպես նաև Ընկերության Բրոքերային (դիլերային) և պահառության ծառայությունների մատուցման ընդհանուր պայմաններում և Կրիպտոակտիվներով ծառայությունների մատուցման ընդհանուր պայմաններում կիրառվող իմաստով:

1.2.3. Կանոնների առանձին կետերի անվանումներն ունեն կողմնորոշիչ նշանակություն և չեն ազդում դրանց բովանդակության մեկնաբանման վրա:

2. Համակարգի անվտանգ օգտագործման պահանջներ

2. 1. Ընդհանուր օգտագործում

2.1.1 Հաճախորդը պարտավոր է օգտագործել Համակարգը միայն Ընկերության սահմանած կանոնների համաձայն:

2.1.2 Հաճախորդը պետք է ապահովի, որ Համակարգի հասանելիությունը սահմանափակվի միայն դրա համար լիազորված անձանց համար և կանխի դրա չթույլատրված/չարտոնված օգտագործումը:

2.2. Անվտանգություն

2.2.1 Հաճախորդը պատասխանատու է բոլոր տվյալների, ներառյալ՝ օգտանունների, գաղտնաբառերի, PIN-կոդերի, անվտանգության տոկենների և այլ նույնականացման տեղեկատվության գաղտնիությունը պահելու համար:

2.2.2 Համակարգերից օգտվելիս Հաճախորդը չպետք է հրապարակի կամ որևէ այլ կերպ հասանելի դարձնի իր գաղտնաբառերը կամ այլ նույնականացման տվյալները որևէ երրորդ անձի (համապատասխան իրավասություն չունեցող անձի), ներառյալ ընտանիքի անդամներ, ընկերներ կամ գործընկերներ:

2.2.3 Հաճախորդը պարտավորվում է ձեռնարկել բոլոր անհրաժեշտ միջոցները, այդ թվում Համակարգ մուտքից հետո (այդ թվում Համակարգ առաջին մուտքից հետո) փոխել Ընկերության կողմից տրամադրված գաղտնաբառը, և իրականացնել պատշաճ վերահսկողություն, որպեսզի բացառվի Հաճախորդի իրավասու էլեկտրոնային հասցեներին կամ այլ կապի միջոցներին /հաղորդակցման եղանակներին/ և/կամ Համակարգին համապատասխան իրավասություն չունեցող անձանց կողմից մուտքը և/կամ նրանց հասանելիությունը:

2.2.4 Հաճախորդը պետք է անմիջապես տեղեկացնի Ընկերությանը ցանկացած կասկածելի վտանգի, գաղտնաբառի կորուստի կամ գողության մասին:

2.2.5 Հաճախորդը պարտավոր է Համակարգ մուտք գործել և Համակարգից օգտվել բացառապես այն սարքերից, որոնք պաշտպանված են հակավիրուսային ծրագրերով:

2.2.6 Հաճախորդը պետք է խուսափի հասարակ կամ անապահով ցանցերից Համակարգի օգտագործման ժամանակ, բացառությամբ լրացուցիչ անվտանգության միջոցների կիրառման (օրինակ՝ VPN):

2.2.7 Հաճախորդը չպետք է փորձի շրջանցել Համակարգի անվտանգության ֆունկցիաները կամ օգտագործել Համակարգը չարամիտ, անօրինական նպատակներով:

2.3. Հսկողություն և հաղորդում

2.3.1 Հաճախորդը պարտավոր է Ընկերությանն անհապաղ հաղորդել Համակարգում ցանկացած կասկածելի գործարքի կամ Համակարգի չարտոնված մուտքի.

հասանելիության, ամբողջականության, գաղտնիության խախտման դեպքերի կամ որևէ այլ տեսակի խնդիրների մասին:

2.3.2 Հաճախորդը պարտավոր է Համակարգի օգտագործման համար գաղտնաբառի կորստի և (կամ) ցանկացած ձևով երրորդ անձանց այն հասանելի դառնալու դեպքում Ընկերությանն ուղարկել համապատասխան ծանուցում:

3. Այլ դրույթներ

Կանոններում բոլոր այլ կետերը, որտեղ հղում է տրված կրիպտոակտիվներով ծառայությունների մատուցմանը կամ Կրիպտոակտիվներով ծառայությունների մատուցման ընդհանուր պայմաններին, միայն այդ մասով ուժի մեջ են մտնում «Կրիպտոակտիվների մասին» ՀՀ օրենքի համաձայն ՀՀ կենտրոնական բանկի կողմից Ընկերությանը կրիպտոակտիվներով ծառայությունների մատուցման հայցվող թույլտվություն տալու պահից: