«Freedom Finance Global PLC» ЖК
Директорлар кеңесінің шешімімен
(2026 жылғы «23» шілдедегі хаттамасы)

бекітілген

2026 жылғы «23» шілдеден бастап
қолданысқа енгізілді

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Астана қ.

2026

МАЗМҰНЫ

1-тарау. ЖАЛПЫ ЕРЕЖЕЛЕР

1. «Freedom Finance Global PLC» жария компаниясының Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «Астана» халықаралық қаржы орталығының нормативтік құқықтық актілеріне, сондай-ақ Қазақстан Республикасының заңнамасына, қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеуді, бақылауды және қадағалауды жүзеге асыратын уәкілетті мемлекеттік органның нормативтік құқықтық актілеріне (бұдан әрі – қолданыстағы заңнама), Freedom Holding Corp. талаптарына және «Freedom Finance Global PLC» жария компаниясының (бұдан әрі – Компания) ішкі құжаттарына сәйкес әзірленді.
2. Осы Саясат ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) мақсаттарын, міндеттерін, негізгі қағидаттарын, АҚБЖ-ға қойылатын талаптарды, АҚБЖ-ның қолданылу аясын, сондай-ақ қауіпсіздікті қамтамасыз ету шараларын айқындайды.
3. Саясатта белгіленген талаптар меншік иесі және пайдаланушысы Компания болып табылатын барлық ақпараттық жүйелер мен құжаттарға қолданылады. Осы Саясат Компанияның барлық жұмыскерлеріне, оның ішінде еңбек және/немесе азаматтық-құқықтық шарттар негізінде тартылған жұмыскерлер мен персоналға, сондай-ақ келісімнің, шарттың негізінде Компанияның ақпараттық активтеріне қол жеткізетін немесе ақпарат алмасу процестеріне қатысатын үшінші тұлғаларға, Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, қолданылады.
4. Компанияның ақпараттық қауіпсіздігін (бұдан әрі – АҚ) қамтамасыз ету мәселелеріне Компанияның Бас атқарушы директоры жетекшілік етеді.
5. Компанияның ең маңызды активтерінің бірі оның қызметі үшін маңызы бар ақпарат, оның ішінде өзге тұлғалармен және жеке тұлғалармен өзара іс-қимыл барысында алынған ақпарат болып табылады.
6. Компаниядағы АҚ-ты қамтамасыз ету АҚБЖ-ны ұйымдастыруға, ақпараттық активтерді санаттауға, ақпараттық активтерге қолжетімділікті ұйымдастыруға, ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге, ақпаратты криптографиялық қорғау құралдарын қолдануға, үшінші тұлғалардың ақпараттық активтерге қол жеткізуі кезінде АҚ-ты қамтамасыз етуге, † жай-күйіне ішкі тексерулер жүргізуге, АҚБЖ процестеріне қойылатын талаптарды қамтиды және Компанияның коммерциялық қызметін табысты жүзеге асырудың қажетті шарты болып табылады. АҚ талаптарының бұзылуы қаржылық шығындар, құқықтық санкциялар, Компанияның іскерлік беделіне нұқсан келуі, оның ішінде клиенттер мен серіктестердің сенімінен айырылуы, сондай-ақ Компанияның бәсекеге қабілеттілігінің төмендеуі сияқты елеулі салдарға әкелуі мүмкін.
7. Компания ақпаратты қорғау мәселелеріне ерекше назар аударады, АҚБЖ-ны, АҚ қатерлерінен қорғаудың қолданылатын құралдары мен тәсілдерін тұрақты түрде жетілдіріп отырады, сондай-ақ Компания жұмыскерлерінің ақпаратты қорғау саласында үздіксіз хабардар болуын қамтамасыз етеді.

2-тарау. МАҚСАТТАРЫ, МІНДЕТТЕРІ, НЕГІЗГІ ҚАҒИДАТТАРЫ МЕН ТАЛАПТАРЫ

8. Компанияда АҚ-ты қамтамасыз ету Компанияның ақпараттық активтеріне төнетін әртүрлі қауіп-қатерлерге байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет. Осы мақсатта Компания ақпараттың мынадай негізгі қасиеттерін қамтамасыз етеді:
   1) **қолжетімділік** – тиісті өкілеттіктері бар субъектілердің ақпаратқа уақтылы әрі кедергісіз қол жеткізу мүмкіндігін сипаттайтын қасиет;
   2) **құпиялылық** – ақпаратқа қол жеткізуге құқығы бар тұлғалар шеңберін шектеу қажеттілігін

білдіретін және жүйенің (ортаның) аталған ақпаратты оған қол жеткізуге өкілеттігі жоқ тұлғалардан құпия сақтай алу қабілетімен қамтамасыз етілетін қасиет;

3) **тұтастық** – ақпараттың бұрмаланбаған түрде (оның белгілі бір тіркелген күйіне қатысты өзгеріссіз) болуын білдіретін қасиет.

9. АҚБЖ негізгі мақсаты – ақпараттың өмірлік циклінің барлық кезеңдерінде оның құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету, сондай-ақ Компанияның ақпараттық активтерінің ақпараттық қауіпсіздігін қамтамасыз етуге байланысты тәуекелдер тұрақты түрде бақыланатын және жол берілетін деңгейде сақталатын жағдайларды Компанияда тұрақты негізде қамтамасыз ету.

10. Аталған мақсатқа қол жеткізу:

1) Компанияның ақпараттық активтерін барлық қауіп-қатер түрлерінен (сыртқы және ішкі, қасақана және абайсызда туындайтын) қорғауға;

2) Компанияның бизнес-процестерінің үздіксіз жұмыс істеуін қамтамасыз ету үшін АҚ инциденттері салдарынан туындауы мүмкін әлеуетті және қаржылық залалды барынша азайтуға мүмкіндік береді.

11. Жоғарыда көрсетілген мақсатқа мынадай міндеттерді шешу арқылы қол жеткізіледі:

1) АҚБЖ-ның жұмыс істеуін қамтамасыз ету және оны тұрақты түрде дамыту, оның қатысушыларын және олардың жауапкершілік аймақтарын айқындау;

2) қолданыстағы заңнаманың талаптарына сәйкес келетін АҚ-ты қамтамасыз ету бойынша құжатталған рәсімдердің болуы;

3) АҚ тәуекелдерін басқару мақсатында, оның ішінде АҚ тәуекелдерін бағалау және оларды барынша азайтуды қоса алғанда, Компанияның ақпараттық активтерінің өмірлік циклінің барлық кезеңдерінде ақпараттық активтерге байланысты қауіп-қатерлер мен осалдықтарды тұрақты түрде айқындау, талдау және олардың алдын алу;

4) Компанияның ақпараттық активтерінің сынилық санатын айқындау және тиісті қорғау деңгейін қамтамасыз ету мақсатында оларды түгендеу және санаттау;

5) Компанияның ақпараттық активтеріне қол жеткізуді басқару, сонымен қоса ең аз артықшылықтар қағидатын, аутентификацияның қажетті деңгейін және есептік жазбаларды бақылауды жүзеге асыру;

6) желілік инфрақұрылымды қорғауды, АЖ/БЖ осалдықтары мен жаңартуларын басқаруды қоса алғанда, ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету;

7) ақпаратты криптографиялық қорғау құралдарын пайдалану, деректерді берудің қорғалған арналарын қолдану;

8) үшінші тұлғалардың Компанияның ақпараттық активтеріне қол жеткізуі кезінде АҚ-ты қамтамасыз ету;

9) АҚ-ты қамтамасыз ету жөніндегі қызметке, сондай-ақ шабуылдарға қарсы іс-қимыл жасау және АҚ инциденттерінің алдын алу жөніндегі іс-шараларға мониторинг жүргізу;

10) АҚ инциденттерін басқару және мониторинг жүргізу, оның ішінде АҚ оқиғалары мен инциденттеріне ден қою, оларды айқындау, тіркеу, туындау себептерін талдау, инциденттерді тергеп-тексеру, сондай-ақ АҚ инциденттері туралы ақпаратты жинау, шоғырландыру және сақтау бойынша процестерді қамтиды;

11) АҚБЖ-ның жай-күйін Компанияның АҚ-ты қамтамасыз ету жөніндегі ішкі құжаттарына және қолданыстағы заңнаманың нормативтік құқықтық актілеріне сәйкестігі тұрғысынан тұрақты түрде ішкі тексерулер жүргізу;

12) Компания жұмыскерлерінің АҚ-ты қамтамасыз ету рәсімдері бойынша хабардарлық деңгейін арттыру және ол бойынша тұрақты оқытуды жүргізу.

12. Компанияның АҚБЖ-сын құру және оның жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылуға тиіс:

1) **қауіпсіз архитектура** – бизнес-процестерді жобалау және ақпараттық жүйелерді құру кезінде АҚ аспектілері ескерілетінін білдіреді;

2) **тиісті деңгейдегі уәждеме мен тартылу** – басшылар мен жұмыскерлердің өз әрекеттерінің маңыздылығын түсіне отырып және белгіленген қағидаттар мен талаптардың сақталуына жауапкершілік ала отырып, АҚ мақсаттарына қол жеткізуге белсенді қатысатынын білдіреді. Бұл хабардарлықты, Ақпараттық қауіпсіздік саясатына бейілділікті және ақпараттық активтермен жұмыс істеу кезінде проактивті мінез-құлықты қолдауға бағытталған ішкі және сыртқы ынталандыруларды қамтиды;

3) **кешенділік** – АҚБЖ АҚ-ты қамтамасыз ету үшін қажетті барлық элементтерді: құжаттама жиынтығын (саясаттар мен рәсімдер), АҚ процестерін, АҚБЖ-ның ұйымдық құрылымын, АҚ мәдениетін, білікті персоналды, инфрақұрылым мен қолданбаларды қамтитынын білдіреді;

4) **артықшылықтарды барынша шектеу** – Компанияның пайдаланушылары мен жүйелеріне өз міндеттерін орындау үшін қажетті ең аз қол жеткізу құқықтары ғана берілуге тиіс екенін білдіреді. Бұл ықтимал осалдықтар мен теріс пайдалануларды шектеуге мүмкіндік береді;

5) **көпдеңгейлі қорғау** – АҚ бақылау шараларын іске асыру кезінде бірнеше қорғау деңгейі қалыптастырылатынын білдіреді;

6) **оқыту және хабардарлық** – Компанияның барлық жұмыскерлері АҚ тәуекелдері мен қауіп-қатерлері туралы хабардар болуын және қорғау шараларын сақтаудың маңыздылығын түсінуін білдіреді;

7) **ашықтық** – Компанияның ақпаратты қорғауға байланысты барлық әрекеттері мен процестері аудит ізін жүргізу үшін журналдарда тіркелуге, түсінікті әрі құжатталған болуға тиіс екенін білдіреді. Бұл қауіпсіздік шараларының орындалуын бақылауға мүмкіндік береді және пайдаланушылар мен реттеуші органдар тарапынан сенімді қамтамасыз етеді;

8) **міндеттерді бөлу** – ешбір пайдаланушыға ақпараттық жүйеге немесе сыни маңызды бизнес-процестерге өз бетінше нұқсан келтіруге мүмкіндік беретін жеткілікті құқықтар берілмеуге тиіс екенін білдіреді;

9) **АҚ бойынша заңнама талаптарын сақтау** – АҚ саласындағы заңнама талаптарын сақтамауға жол берілмейтінін білдіреді. Барлық сәйкессіздіктер жойылуға тиіс немесе, кем дегенде, оларды жою тиісті іс-шаралар жоспарларында жоспарлануға тиіс;

10) **тәуекелді басқару** – ақпараттық жүйелер мен деректер үшін тәуекелдерді жүйелі түрде бағалауға, сондай-ақ тиісті қауіпсіздік шараларының көмегімен осы тәуекелдерді барынша азайту жөнінде шешімдер қабылдауға бағытталған;

11) **тиімділік және бақылау** – олардың бағаланатын тәуекелдерге сәйкестігін, іске асырылуының толықтығы мен сапасын бақылауға бағытталған. Қабылданған шаралардың тиімділігі қойылған мақсаттар мен қол жеткізілген нәтижелерге қол жеткізу деңгейі негізінде бағалануға тиіс.

13. Компания ақпараттық жүйелерде жасалатын, сақталатын және өңделетін ақпаратқа пайдаланушылардың қол жеткізуін басқару тәртібін айқындайды, сондай-ақ ақпаратқа және оған қол жеткізуге мониторинг жүргізу құқығын өзіне қалдырады. Ақпаратқа қол жеткізу жұмыскерлерге өздеріне жүктелген лауазымдық міндеттерін орындау үшін қажетті көлемде ғана беріледі.

14. Осы Саясатқа, оған қатысты құжаттарға, ақпараттық жүйелерге және тұтастай алғанда АҚ жүйесіне, сондай-ақ қауіп-қатерлерді айқындау және талдау, шабуылдарға қарсы іс-қимыл жасау және АҚ инциденттерін тергеп-тексеру жөніндегі іс-шараларға талдау мен бағалау кем дегенде жыл сайын мынадай іс-шаралардың нәтижелері негізінде жүргізіледі:

    1) АҚБЖ-ның жай-күйін талдау;

    2) АҚ жай-күйіне ағымдағы тексерулер жүргізу;

    3) АҚ департаменті немесе білікті сыртқы аудиторлар жүргізетін ақпараттық жүйелерде осалдықтардың болуына сканерлеу жүргізу және енуге тестілеу өткізу;

    4) анықталған инциденттер және АҚ талаптарының бұзылуы;

    5) аудиторлық тексерулер жүргізу кезінде АҚ жай-күйін тексеру;

    6) АҚ жүйесіне қатысты өзге де аудиттер мен тексерулер.

15. Қолданыстағы жүйелерді тексеруді талап ететін аудит жөніндегі іс-шаралар бизнес-процестердің үзілу тәуекелін барынша азайтатындай етіп жоспарлануға және келісілуге тиіс.

16. АҚ-ты қамтамасыз ету жөніндегі қызметке мониторинг жүргізу барысында алынған АҚ инциденттері туралы ақпарат шоғырландырылуға, жүйелендірілуге және сақталуға тиіс.

17. АҚ инцидентін өңдеу нәтижелері бойынша АҚ инцидентінің туындау себептеріне, оның туындау тетігі мен салдарына жан-жақты талдау жүргізіледі.

3-тарау. ҚОЛДАНЫЛУ АЯСЫ

18. Компанияда АҚ-ты қамтамасыз етудің негізгі объектілері ретінде мыналар танылады:

    1) қолданыстағы заңнамаға және Компанияның ішкі нормативтік құжаттарына сәйкес Компанияның коммерциялық құпиясына жатқызылған мәліметтерді, сондай-ақ Компанияның қалыпты жұмыс істеуін қамтамасыз ету үшін қажетті өзге де кез келген ақпаратты қамтитын ақпараттық активтер (бұдан әрі – қорғалатын ақпарат);

    2) қорғалатын ақпаратты өңдеу, беру және сақтау жүзеге асырылатын ақпараттандыру құралдары мен жүйелері (есептеу техникасы құралдары, ақпараттық-есептеу кешендері, желілер, жүйелер);

    3) қорғалатын ақпаратты өңдеу жүзеге асырылатын Компанияның автоматтандырылған ақпараттық жүйесінің бағдарламалық құралдары (операциялық жүйелер, дерекқорларды басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық жасақтама);

    4) ақпараттық активтерді басқаруға және пайдалануға байланысты Компанияның процестері;

    5) қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

    6) Компания жұмыскерлерінің жұмыс үй-жайлары мен кабинеттері, сондай-ақ жабық келіссөздер мен кеңестер өткізуге арналған Компанияның үй-жайлары;

    7) қорғалатын ақпаратқа қол жеткізу құқығы бар Компанияның жұмыскерлері;

8) ашық ақпаратты өңдейтін, бірақ қорғалатын ақпарат өңделетін үй-жайларда орналасқан техникалық құралдар мен жүйелер.

19. Қорғалуға жататын ақпарат:

1) қағаз тасымалдағыштарда орналастырылуы мүмкін;

2) электрондық түрде болуы мүмкін (есептеу техникасы құралдарының көмегімен өңделуі, берілуі және сақталуы, сондай-ақ техникалық құралдардың көмегімен жазылуы және қайта жаңғыртылуы мүмкін);

3) байланыс арналары (оның ішінде телефон байланысы, факсимильдік байланыс, электрондық пошта, хабар алмасу жүйелері және өзге де телекоммуникациялық сервистер) арқылы электр сигналдары түрінде берілуі мүмкін..

4-тарау. ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ШАРАЛАРЫ

20. Компанияның АҚ-ын қамтамасыз етудің негізгі шаралары мыналар болып табылады:

1) әкімшілік-құқықтық және ұйымдастырушылық шаралар;

2) техникалық қауіпсіздік шаралары;

3) бағдарламалық-техникалық шаралар.

21. Әкімшілік-құқықтық және ұйымдастырушылық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

1) қолданыстағы заңнама мен Компанияның ішкі құжаттары талаптарының сақталуын бақылау;

2) АҚ-ты қамтамасыз етуге қойылатын талаптарды әзірлеу және енгізу, сондай-ақ АҚ-ты қамтамасыз ету мәселелері бойынша процестерге әдіснамалық қолдау көрсету (қағидалар, рәсімдер);

3) бизнес-процестердің осы Саясатта белгіленген талаптарға сәйкестігін бақылау;

4) Компания жұмыскерлерін ақпараттық жүйелермен жұмыс істеу және АҚ талаптары бойынша хабардар ету және оқыту;

5) АҚ инциденттеріне ден қою, оларды оқшаулау және олардың салдарын барынша азайту;

6) АҚ тәуекелдерін талдау және барынша азайту;

7) төтенше жағдайлар туындаған кезде орындалатын іс-қимылдарды айқындау;

8) Компанияның ішкі құжаттарының талаптарына сәйкес Компания жұмыскерлерін жұмысқа қабылдау және жұмыстан босату кезінде АҚ-ты қамтамасыз ету жөніндегі тиісті шараларды жүзеге асыру.

22. Техникалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

1) өткізу және объектішілік режимдерді ұйымдастыру;

2) қорғалатын объектілердің қауіпсіздік периметрін ұйымдастыру;

3) қорғалатын объектілерде бейнебақылауды және өрт қауіпсіздігін ұйымдастыру;

4) Компания жұмыскерлерінің қолжетімділігі шектеулі үй-жайларға кіруін бақылау.

23. Бағдарламалық-техникалық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):

1) лицензиялық бағдарламалық жасақтаманы және ақпаратты қорғаудың сертификатталған құралдарын пайдалану;
2) ақпараттық активтердің қауіпсіздік жаңартуларын уақтылы орнату;
3) кешенді антивирустық қорғауды қолдану;
4) ақпараттық жүйелерге кіріктірілген АҚ құралдарын пайдалану;
5) ақпараттық активтерді пайдаланушыларды сәйкестендіру және аутентификациялау тетіктерін, оның ішінде құпия сөз саясатты тиісті деңгейде баптау;
6) қауіпсіздік баптауларының өзгерістерін және жүйелік әрі конфигурациялық файлдардың тұтастығын бақылау, сондай-ақ ақпараттық активтердегі аудит ізі журналдарының өзгермейтіндігін қамтамасыз ету;
7) ақпараттың резервтік көшірмесін тұрақты түрде жасауды және деректерді қауіпсіз қалпына келтіруді қамтамасыз ету;
8) пайдаланушылардың есептік жазбаларын, қол жеткізу құқықтарын және олардың іс-әрекеттерін, оның ішінде артықшылықты пайдаланушылардың іс-әрекеттерін басқару және бақылау;
9) ақпаратты криптографиялық қорғау жүйелерін қолдану;
10) аппараттық құралдардың іркіліссіз жұмысын қамтамасыз ету;
11) ақпараттық жүйенің сыни элементтерінің жай-күйіне мониторинг жүргізу.

5-тарау. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

24. Осы Саясаттың талаптарын тиісінше орындамағаны және/немесе бұзғаны үшін жауапкершілік Компания жұмыскерлеріне өздеріне жүктелген функционалдық міндеттері шегінде жүктеледі.
25. Саясатты қайта қарау Компанияның қауіпсіздігіне қауіп төнген жағдайда, қолданыстағы заңнамаға және Компанияның ішкі процестеріне өзгерістер енгізілген кезде, ішкі нормативтік құжаттарда белгіленген тәртіппен жүзеге асырылады.
26. Осы Саясатпен реттелмеген мәселелер қолданыстағы заңнамаға, Компанияның ішкі құжаттарына, сондай-ақ Компания органдары мен лауазымды тұлғаларының өз құзыреті шегінде белгіленген тәртіппен қабылдаған шешімдеріне сәйкес шешіледі.