



**«Қазақстан Республикасы Ұлттық Банкінің Ұлттық төлем корпорациясы»
акционерлік қоғамы**

«ҰТК» АҚ Директорлар кеңесінің
«___» _____ 20___ ж.
(№___ хаттама)
шешімімен бекітілген

Күшіне енген күні
«___» _____ 20___ ж.

**«Қазақстан Республикасы Ұлттық Банкінің Ұлттық төлем корпорациясы»
акционерлік қоғамындағы Ақпараттық қауіпсіздік саясаты**

Тірк. № _____

Алматы қ.

Мазмұны

1 - тарау. Жалпы ережелер	3
2 - тарау. Мақсаттары мен міндеттері.....	3
3 - тарау. АҚБЖ-нің негізгі ережелері.....	4
4 - тарау. Басқару моделі	6
5 - тарау. Жауапкершілік және бақылау	6
6 - тарау. Қорытынды ережелер	7

1 тарау. Жалпы ережелер

1. «Қазақстан Республикасы Ұлттық Банкінің Ұлттық төлем корпорациясы» акционерлік қоғамының (бұдан әрі – Саясат) Ақпараттық қауіпсіздік саясаты Қазақстан Республикасы Ұлттық Банкінің «Ұлттық төлем корпорациясы» акционерлік қоғамында (бұдан әрі – Қоғам) ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттарын көрсететін негізгі құжат болып табылады.

2. Саясат мынадай талаптарға сәйкес әзірленді:

- 1) Қазақстан Республикасының Цифрлық кодексіне;
- 2) «Қазақстан Республикасының Ұлттық Банкі туралы» Қазақстан Республикасының Заңына;
- 3) «Қазақстан Республикасындағы банктер және банк қызметі туралы» Қазақстан Республикасының Заңына;
- 4) «Төлемдер және төлем жүйелері туралы» Қазақстан Республикасының Заңына;
- 5) «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңына;
- 6) ақпараттық қауіпсіздік мәселелерін реттейтін Қазақстан Республикасы Ұлттық Банкінің және Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігінің құқықтық актілеріне;
- 7) Қазақстан Республикасының ҚР СТ ISO/IEC 27001 ұлттық стандартына.

3. Қоғамның басқару органы қолданыстағы және ықтимал ақпараттық қауіпсіздік қатерлері, сондай-ақ Қазақстан Республикасының заңнамасы мен технологиялық ортаның өзгеруі жағдайында ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі – АҚБЖ) құрудың, дамытудың және тұрақты жетілдірудің маңыздылығы мен қажеттілігін түсінеді.

4. Қоғам өз қызметінің қолданылатын заңнамалық және реттеушілік талаптарға, сондай-ақ ақпараттық қауіпсіздік саласындағы халықаралық және мемлекеттік стандарттарға сәйкестігін қамтамасыз етеді.

5. Қолданылатын заңнамалық және реттеушілік талаптарға, сондай-ақ ақпараттық қауіпсіздік саласындағы халықаралық және мемлекеттік стандарттарға сәйкестікті қамтамасыз ету мақсатында Қоғам осындай талаптар мен стандарттардағы өзгерістерге уақтылы мониторинг жүргізуді, сондай-ақ АҚБЖ-нің ішкі нормативтік құжаттарын көрсетілген өзгерістерге сәйкес өзектендіруді қамтамасыз етеді.

2-тарау. Мақсаттары мен міндеттері

6. Саясаттың мақсаты Қоғамның активтерін қорғауды ұйымдастыруға бағытталған Қоғамдағы ақпараттық қауіпсіздікті қамтамасыз етудің бірыңғай тәсілін айқындау болып табылады.

7. Саясаттың мақсатына қол жеткізу үшін негізгі міндеттер мыналар болып табылады:

- 1) сақталатын, берілетін және өңделетін ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету, сондай-ақ үшінші

тұлғалардың ақпаратын қорғау;

2) ақпараттық қауіпсіздік қатерлерін анықтау, алдын алу және бейтараптандыру, сондай-ақ олардың туындау себептері мен жағдайларын айқындау;

3) ақпараттық қауіпсіздік қатерлерінің іске асырылуының салдарын барынша азайту және оқшаулау, сондай-ақ олардың қайталануына жол бермеу мақсатында ақпараттық қауіпсіздік оқиғаларына талдау жүргізу;

4) Қоғам қызметінің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы қолданылатын заңнамалық, реттеушілік талаптарға, халықаралық және ұлттық стандарттарға сәйкестігін қамтамасыз ету, сондай-ақ Қоғамның ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ішкі нормативтік құжаттарын тұрақты түрде өзектендіру;

5) Қоғам қызметкерлерінің ақпараттық қауіпсіздік саласындағы хабардарлық деңгейін арттыру және активтермен қауіпсіз жұмыс істеу мәдениетін қалыптастыру;

6) активтерді қорғау үшін қолданылатын ұйымдастырушылық және техникалық шаралардың тиімділігі мен жеткіліктілігін бақылау.

8. Саясатты іске асырудың және Қоғамдағы ақпараттық қауіпсіздік талаптарын сақтаудың негізгі бағыттары:

1) активтерді қорғаудың ұйымдастырушылық және техникалық шараларын іске асыру;

2) заңнамалық және реттеушілік талаптарды, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық және халықаралық стандарттардың қолданылатын талаптарын сақтау;

3) ақпараттық қауіпсіздікті қамтамасыз етудің әртүрлі аспектілерін реттейтін ішкі нормативтік құжаттарды әзірлеу және сақтау, оның ішінде, бірақ олармен шектелмей, аутентификацияны басқару және қол жеткізу құқықтарын ажырату, пайдаланушылардың есептік жазбаларын басқару, ақпараттық активтерді басқару және оларды жіктеу, ақпаратты өңдеу, сақтау және беру кезінде қорғау, ақпаратты қорғаудың криптографиялық құралдарын басқару, желілік инфрақұрылым мен ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету, осалдықтарды басқару және қорғалу деңгейін талдау, ақпараттық қауіпсіздік оқиғаларының мониторингі және ақпараттық қауіпсіздік оқиғаларына ден қою, бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу кезінде қауіпсіздікті қамтамасыз ету, ақпараттық жүйелердегі өзгерістерді басқару, ақпараттың резервтік көшірмесін жасау және қалпына келтіру, жеткізушілермен және үшінші тараптармен өзара іс-қимыл кезінде қауіпсіздікті қамтамасыз ету, сондай-ақ ақпараттық-коммуникациялық инфрақұрылым объектілерінің физикалық қауіпсіздігін қамтамасыз ету процестері.

3-тарау. АҚБЖ-нің негізгі ережелері

9. Осы Саясаттың мақсатына қол жеткізу үшін Қоғам Қоғамның активтерінің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған, тәуекелге бағдарланған тәсілді қолдану негізінде АҚБЖ-нің жұмыс істеуін және оны тұрақты жетілдіруді қамтамасыз етеді.

10. АҚБЖ-нің жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылады:

1) заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-қимыл Қазақстан Республикасының заңнамасына сәйкес жүзеге асырылады, бұл ретте Қоғамның активтеріне теріс әсер етуді анықтау, алдын алу, оқшаулау және жолын кесудің заңнамада рұқсат етілген әдістері қолданылады;

2) кешенділік – активтердің өмірлік циклінің барлық кезеңдерінде, сондай-ақ активтердің жұмыс істеуінің барлық режимдерінде олардың қауіпсіздігін қамтамасыз ету;

3) дербес жауапкершілік – Басқарма мүшелері, құрылымдық бөлімшелердің басшылары және Қоғамның қызметкерлері ақпараттық қауіпсіздік талаптарынан хабардар болуға және активтерді қорғаудың белгіленген шараларын сақтауға дербес жауапты болуға тиіс;

4) өзара іс-қимыл және үйлестіру – ақпараттық қауіпсіздік шаралары Қоғамның құрылымдық бөлімшелерінің өзара іс-қимылы, қойылған мақсаттарға қол жеткізу үшін олардың қызметін үйлестіру, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша мемлекеттік органдармен, кәсіби қоғамдастықтармен және өзге де ұйымдармен өзара іс-қимыл жасау негізінде жүзеге асырылады.

11. Қоғамда АҚБЖ-нің жұмыс істеуі мынадай талаптарды сақтау арқылы қамтамасыз етіледі:

1) АҚБЖ қолданылу саласын айқындау және қолдау;

2) ақпараттық қауіпсіздік тәуекелдерін тұрақты негізде, сондай-ақ Қоғам қызметіндегі елеулі өзгерістер кезінде сәйкестендіру, талдау, бағалау және өңдеу;

3) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы қызметкерлердің рөлдерін, жауапкершілігі мен өкілеттіктерін айқындау;

4) ақпараттық қауіпсіздік саласындағы ішкі нормативтік құжаттарды әзірлеу, бекіту және өзектендіру;

5) қызметкерлердің ақпараттық қауіпсіздік мәселелері бойынша хабардар болуын қамтамасыз ету;

6) АҚБЖ жұмысының тиімділігіне мониторинг жүргізу, оны талдау және бағалау;

7) Қазақстан Республикасының заңнамасы мен Қоғамның ішкі нормативтік құжаттарының талаптарына сәйкестікті қамтамасыз ету;

8) мониторинг, тексерулер және оқиғаларды талдау нәтижелері негізінде АҚБЖ-ні үздіксіз жетілдіру;

9) АҚБЖ-нің жұмыс істеуіне ішкі тексерулер жүргізу;

10) АҚБЖ-нің жеткіліктілігін, нәтижелілігін және Қоғам қызметінің мақсаттарына сәйкестігін бағалау, сондай-ақ оны жетілдіру жөнінде шешімдер қабылдау мақсатында Қоғам басшылығы тарапынан АҚБЖ-нің жұмыс істеуіне талдау жүргізу.

12. АҚБЖ-нің қолданылу саласы Қоғамның барлық құрылымдық бөлімшелері мен қызметкерлеріне, үшінші тұлғалармен өзара іс-қимыл

процестерін қоса алғанда, бизнес-процестерге, сондай-ақ Қоғам қызметінде пайдаланылатын активтерге қолданылады.

13. Қоғамның ақпараттық қауіпсіздік бөлімшесінің қызметкерлері ақпараттық қауіпсіздік саласында тұрақты оқудан және біліктілігін арттырудан өтеді.

4-тарау. Басқару моделі

14.Қоғамдағы АҚБЖ-нің жұмыс істеуі жауапкершілікті бөлуді, бақылау функцияларының тәуелсіздігін және ақпараттық қауіпсіздік талаптарының сақталуын үздіксіз бақылауды қамтамасыз ететін «үш қорғау желісі» моделі негізінде ішкі бақылау жүйесі шеңберінде жүзеге асырылады.

15.«Үш қорғау желісі» моделіне қатысушылардың рөлдерін, жауапкершілігін, өкілеттіктері мен функцияларын бөлу, сондай-ақ олардың өзара іс-қимыл жасау және бақылау функцияларын жүзеге асыру тәртібі Қоғамның ішкі нормативтік құжаттарымен айқындалады.

5-тарау. Жауапкершілік және бақылау

16.Қоғам Басқармасының Төрағасы АҚБЖ-нің жұмыс істеуін және жетілдірілуін қамтамасыз етуге жалпы жауапты болады, осы Саясаттың мақсаттарына қол жеткізілуін бақылайды және ақпараттық қауіпсіздік талаптарын іске асыру үшін қажетті ресурстардың бөлінуін қамтамасыз етеді.

17. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті ұйымдастыру және үйлестіру, ақпаратты қорғаудың ұйымдастырушылық және техникалық шараларына қойылатын талаптарды айқындау, ақпараттық қауіпсіздік процестерін әдіснамалық сүйемелдеу, ақпараттық қауіпсіздік тәуекелдерін басқаруға қатысу, сондай-ақ ақпараттық қауіпсіздік саласындағы талаптардың сақталуын бақылау Қоғамның ақпараттық қауіпсіздік бөлімшесімен жүзеге асырылады.

18.Ақпараттық қауіпсіздік бөлімшесінің басшысы АҚБЖ-нің жұмыс істеуін ұйымдастыруға, ақпараттық қауіпсіздікті қамтамасыз ету процестерін үйлестіруге, сондай-ақ ақпараттық қауіпсіздік бөлімшесінің құзыреті шегінде Қоғамда ақпараттық қауіпсіздік талаптарының сақталуын бақылау мен мониторингін жүзеге асыруға жауапты болады.

19.Құрылымдық бөлімшелердің басшылары мен Қоғамның қызметкерлері өздерінің функционалдық міндеттері шегінде ақпараттық қауіпсіздік талаптарын сақтауға, ақпаратты қорғаудың белгіленген шараларын орындауға және Қоғам активтерінің қауіпсіз пайдаланылуын қамтамасыз етуге жауапты болады.

20.Ішкі аудит бөлімшесі АҚБЖ-нің, ішкі бақылау жүйесінің және ақпараттық қауіпсіздік тәуекелдерін басқару процестерінің жұмыс істеу тиімділігіне тәуелсіз бағалау жүргізеді.

21. Қоғамның ақпараттандыру объектілері мен ақпаратына қол жеткізе алатын үшінші тараптардың өкілдері жасалған шарттардың талаптарына сәйкес ақпараттық қауіпсіздік талаптарын сақтауға міндетті.

22.Қоғамның барлық қызметкерлері АҚБЖ-нің ішкі құжаттарында белгіленген ақпараттық қауіпсіздік талаптарын сақтамағаны үшін дербес жауапты болады және анықталған барлық бұзушылықтар мен ақпараттық

қауіпсіздік оқиғалары туралы ақпараттық қауіпсіздік бөлімшесіне дереу хабарлауға міндетті.

23. Қызметкерлердің лауазымдық нұсқаулықтары мен үшінші тұлғалармен жасалатын шарттарда Қоғамның ақпараттық қауіпсіздігін қамтамасыз ету және сақтау жөніндегі талаптар қамтылуға тиіс. Қоғамның ішкі құжаттарында, егер олармен реттелетін процестер ақпаратты өңдеуге, сақтауға немесе беруге байланысты болса, ақпараттық қауіпсіздік талаптары қамтылады.

6-тарау. Қорытынды ережелер

24. Саясат кемінде 3 жылда бір рет, сондай-ақ мынадай жағдайларда қайта қаралуға жатады:

- 1) Қоғам қызметіндегі елеулі өзгерістер;
- 2) Қазақстан Республикасының заңнамасындағы өзгерістер;
- 3) Қоғам қызметі саласында реттеуді және (немесе) қадағалауды жүзеге асыратын мемлекеттік органдар талаптарының өзгеруі;
- 4) АҚБЖ-нің жұмыс істеуіне әсер ететін өзге де мән-жайлар.

25. Ақпараттық қауіпсіздік бөлімшесі осы Саясатты Қоғамның барлық қызметкерлерінің назарына жеткізуді қамтамасыз етеді.

26. Саясат жалпыға қолжетімді құжат болып табылады және Қоғамның ресми интернет-ресурсында орналастырылады.