Тіркеу № 19
«01» 02 2024 ж.

«БЖЗҚ» АҚ Директорлар кеңесінің
2024 ж. «26» 01 № 2
хаттамасымен бекітілді

«БЖЗҚ» АҚ ақпараттық қауіпсіздік саясаты

«БЖЗҚ» АҚ Директорлар кеңесінің хаттамасымен бекітілген өзгерістер мен толықтырулар:

№	Өзгерістер, толықтырулар енгізілді	Бекітілген күні	Хаттама №	Тіркеу №
1	Хаттама	«___» _____ 20__ ж.	№____	№___
2	Хаттама	«___» _____ 20__ ж.	№ ____	№ ____
3	Хаттама	«___» _____ 20__ ж.	№ ____	№ ____
4	Хаттама	«___» _____ 20__ ж.	№ ____	№ ____

«БЖЗҚ» АҚ Директорлар кеңесінің 202__ ж. «___» _____ № ___хаттамасымен күшін жойды деп танылды

1-тарау. Жалпы ережелер

1. Осы «БЖЗҚ» АҚ ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) ақпаратты қорғау жөніндегі негізгі қағидаттарды, бағыттар мен талаптарды айқындайды, ақпараттық қауіпсіздік ркжимін қамтамасыз ету үшін негіз болып табылады, «БЖЗҚ» АҚ (бұдан әрі – Қор) тиісті ішкі құжаттарын әзірлеу кезінде нұсқаулық қызметін атқарады.

2. Саясаттың нормативтік-құқықтық негізін ақпараттық жүйелерді пайдалану және ақпараттық қауіпсіздік мәселелері жөніндегі Қазақстан Республикасы заңнамасының ережелері, сондай-ақ ақпараттық қауіпсіздікті басқару халықаралық стандарттарының талаптары құрайды.

3. Саясат ережелері Қордың барлық қызметкерлері, тағылымгерлер, тәжірибеден өтушілер үшін орындауға міндетті болып табылады, сондай-ақ міндетті зейнетақы жарналары (МЗЖ) салымшыларының, жұмыс берушінің міндетті зейнетақы жарналары (ЖМЗЖ), міндетті кәсіптік зейнетақы жарналары (МКЗЖ), ерікті зейнетақы жарналары (ЕЗЖ) аударылған жеке тұлғалардың, зейнетақы төлемдерін алушылардың, нысаналы талаптарды алушылардың және Қордың ақпараттық жүйелері мен құжаттарына Қор мен оның қызметіне тікелей өзара байланысы бар бөлігінде қол жеткізе алатын, басқа да үшінші тұлғалардың назарына жеткізілуі тиіс.

4. Осы Саясаттың талаптары Қорға тиесілі және ол пайдаланушы болып табылатын барлық ақпараттық жүйелер мен құжаттарға қолданылады. Ақпараттық қауіпсіздікті қамтамасыз ету – Қор қызметін табысты жүзеге асырудың қажетті шарты. Ақпарат Қордың ең маңызды активтерінің бірі болып табылады.

5. Осы Саясаттағы Қордың ақпараттық қауіпсіздігі электрондық ақпараттық ресурстарды, коммерциялық және (немесе) заңмен қорғалатын басқа да құпияларға жататын ақпаратты (конфеденциалды ақпарат), ақпараттық жүйелер мен ақпараттық инфрақұрылымды, Қорға материалдық зиян, беделіне нұқсан келтіруі мүмкін, сыртқы және ішкі қатерлерден қорғау жағдайын білдіреді.

6. Ақпараттық қауіпсіздік саясаты дербес деректерді, МКЗЖ салымшылары, ЖМЗЖ, МКЗЖ, ЕЗЖ аударылған жеке тұлғалар, зейнетақы төлемдерін алушылар, сондай-ақ нысаналы талаптарға қатысушылар, нысаналы талаптарды алушылар және басқа да мүдделі тараптар туралы ақпаратты қорғауға бағытталған.

7. Осы Саясатта келесідей терминдер, анықтамалар және қысқартулар пайдаланылады:

1) АЖ ресурстарының әкімшілері – ақпараттық жүйелерді басқаруды жүзеге асыратын Қордың Цифрландыру департаменті мен Инфрақұрылымды дамыту және қолдау департаментінің қызметкерлері;

2) мүдделі тараптар – тауарларды/жұмыстарды/көрсетілетін қызметтерді жеткізушілер, зейнетақы активтері мен (немесе) меншікті активтерді басқаратын басқарушы компаниялар, сыртқы ақпараттық деректерді жеткізушілер және Қор өз функциялары мен міндеттерін іске асыру кезінде өзара іс-әрекеттер жүргізетін басқа да іскерлік контрагенттер;

3) АҚ – ақпараттық қауіпсіздік;

4) АҚ тосын оқиғасы - ақпараттық ресурстың жұмыс істеуінің бұзылуына немесе ақпарат қауіпсіздігіне қатер төнуіне немесе ақпаратты қорғау талаптарының бұзылуына әкеп соққан (әкелуі мүмкін) ақпараттық қауіпсіздіктің күтпеген немесе жағымсыз оқиғасы (оқиғалар тобы);

5) АЖ – ақпараттық жүйе;

6) АТ-инфрақұрылымы – бұл Қордың ақпараттық өзара іс-әрекет құралдарының жұмыс істеуін және дамуын қамтамасыз ететін, өзара байланысты ақпараттық жүйелер мен сервистер кешені;

7) кибершабуыл – шабуылдаушының ақпараттың үш қасиетінің бірін – қолжетімділікті, тұтастықты немесе құпиялылықты бұзуға бағытталған қасақана әрекеттерінің жиынтығы;

8) корпоративтік деректерді компроматтау (бұзу) – қорғалатын ақпаратқа рұқсатсыз кіру (қол жеткізу) фактісі, сондай-ақ осындай кірудің орын алуы мүмкін екендігіне күдіктену;

9) ЖАҚО – жедел ақпараттық қауіпсіздік орталығы, нақты уақыт режимінде желілік белсенділік пен оқиғаларды орталықтандырылған жинау арқылы ақпараттық инфрақұрылым мен АТ-инфрақұрылымындағы ақпараттық қауіпсіздіктің жағдайы туралы ақпарат алуға, ұйым үшін қауіп төндіретін ықтимал қауіпті және күдікті белсенділіктер туралы толық ақпарат алуға, кешенді талдау жүргізуге және 24/7/365 режимінде АТ инфрақұрылымындағы инциденттерді анықтауға мүмкіндік беретін кешенді шешім.

2-тарау. Талаптарға сәйкестігі

8. Осы Саясат және жалпы алғанда АҚ жүйесі келесідей нормативтік құқықтық актілерге және халықаралық стандарттарға негізделеді (осы бөлімде жалпы Қордың АҚ жүйесін құру процесіне тікелей ықпал ететін негізгі нормативтік актілер көрсетілген; сонымен қатар, АҚ-ны мемлекеттік деңгейде дамытудың стратегиялық аспектілерін сипаттайтын немесе жекелеген қосымшаларды/көрсетілетін қызметтерді ақпараттық қорғау жөніндегі қағидаларды регламенттейтін бірқатар құжаттар бар):

1) Қазақстан Республикасының 2023 жылғы 20 сәуірдегі № 224-VII Әлеуметтік кодексі;

2) «Қазақстан Республикасының кейбір заңнамалық актілеріне Қазақстан Республикасының Ұлттық қорынан балаларға арналған қаражатты есептеу, төлеу және пайдалану мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» Қазақстан Республикасының 2023 жылғы 16 қарашадағы № 40-VIII ҚРЗ заңы;

3) «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 21.05.2013 № 94-V Заңы;

4) Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы (бұдан әрі – Бірыңғай талаптар);

5) Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2023 жылғы 7 маусымдағы № 40 қаулысымен бекітілген Бірыңғай жинақтаушы зейнетақы қорына және ерікті жинақтаушы зейнетақы қорларына арналған тәуекелдерді басқару мен ішкі бақылау жүйесін қалыптастыру қағидалары;

6) Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2023 жылғы 26 маусымдағы № 60 қаулысымен бекітілген зейнетақы активтері мен жинақтарын есепке алуға арналған автоматтандырылған ақпараттық жүйелерге қойылатын талаптар;

7) ISO/IEC 27001:2005 «Ақпараттық технологиялар - Қауіпсіздікті қамтамасыз ету әдістері - Ақпараттық қауіпсіздікті басқару жүйелері - Талаптар» халықаралық стандарты (ҚР СТ ИСО/МЭК 27001-2015);

8) ISO/IEC 20000-1: 2018 «Ақпараттық технологиялар - Қызметтерді басқару - 1-бөлім: Қызметтерді басқару жүйесіне қойылатын талаптар» халықаралық стандарты.

9. Қорда Қазақстан Республикасының зияткерлік меншік құқығын, дербес деректерді қорғау жөніндегі нормативтік құқықтық актілерінің талаптары және криптографиялық құралдарды пайдалану жөніндегі шектеулер сақталады.

10. ISO/IEC 27001 және ISO/IEC 20000-1:2018 халықаралық стандартының барлық талаптары мен ережелері, Қордың тиісті ішкі нормативтік құжаттарымен айқындалатын, оларды қолдану саласында орындау үшін міндетті болып табылады.

11. АҚ құралдары мен әдістерін әзірлеу және қолдану кезінде Қордың үшінші тұлғалармен шарттық міндеттемелерінің талаптары ескеріледі.

12. Осы Саясаттың, Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының және ISO/IEC 27001 және ISO/IEC 20000-1: 2018 халықаралық стандарттарының ережелері, осы стандарттардың талаптарын іске асыруға тартылған Қор қызметкерлерінің лауазымдық нұсқаулықтарында және берілген құжаттар мен стандарттардың күші қолданылатын жүйелерге қызмет көрсетуге және пайдалануға тартылған бөгде ұйымдармен және жеке тұлғалармен жасалатын шарттарда қамтылған.

13. Қазақстан Республикасының нормативтік құқықтық актілерінің немесе халықаралық стандарттардың талаптары болған кезде Қор контрагенттердің (тауарлар мен көрсетілетін қызметтерді берушілердің) белгілі бір талаптарға сәйкестігін тексереді.

14. Саясат негізінде Қорда АҚ-ны қамтамасыз етудің нақты ережелері мен әдістерін регламенттейтін төмен тұрған деңгейдегі ішкі нормативтік құжаттар, стандарттардың қолданылуы саласындағы жеке саясат және т.б. бекітіледі. Аталған құжаттар саясат талаптарын толықтыра және кеңейте алады, бірақ оларға қайшы келе алмайды.

3-тарау. АҚ құрудың мақсаттары, міндеттері және негізге алынатын қағидаттары

15. АҚ негізгі мақсаты Қордың АЖ, конфеденциалды ақпаратты, коммерциялық және дербес деректерді ақпаратқа, оны тасымалдағыштарға, өңдеу және жіберу процестеріне кездейсоқ немесе қасақана әсер ету арқылы ықтимал залал келтіруден қорғау, сондай-ақ тәуекелдер деңгейін барынша азайту болып табылады. Бұл мақсатқа жету үшін, Саясаттың барлық ережелері ақпараттық қауіпсіздікке қатер төндіретін оқиғалардың алдын алу немесе олардың салдарын барынша азайту арқылы, осы оқиғалардан келетін залалды азайтуға бағытталған.

16. Қойылған мақсатқа қол жеткізу мына міндеттерді орындаумен қамтамасыз етіледі:

1) қолжетімділік – тиісті өкілеттігі бар субъектілердің ақпаратқа дер кезінде кедергісіз қол жеткізу мүмкіндігімен сипатталатын қасиет;

2) конфеденциалдылық – бұл ақпаратқа рұқсаты бар субъектілер шеңберіне шектеулер енгізу қажеттілігін көрсететін және жүйенің (ортаның) осы ақпаратты оған қол жеткізуге құқығы жоқ субъектілерден құпия сақтау мүмкіндігімен қамтамасыз етілетін қасиет;

3) тұтастық – ақпараттың бұрмаланбаған (оның қандай да бір тұрақты күйіне қатысты өзгермейтін) түрде болу қасиеті.

17. Қордың ақпараттық қауіпсіздігін және Бірыңғай талаптарға сәйкестігін қамтамасыз ету мақсатында, киберқауіпсіздік бөлімшесінің негізінде жедел ақпараттық қауіпсіздік орталығын (ЖАҚО) құру ақпараттық қауіпсіздікті қамтамасыз етудің негізгі міндеттерінің бірі болып табылады.

18. ЖАҚО міндеттеріне мониторинг, талдау және желілік шабуылдарға қарсы іс-қимылдар жүргізу кіреді. ЖАҚО осал тұстарды басқару мәселесін кешенді шешуге, кибершабуыл әрекеттерін уақтылы анықтауға және деректердің қауіпсіздігі мен құпиялылығын қамтамасыз етуге тартылған.

19. ЖАҚО Қордың ақпараттық қауіпсіздігін басқару жүйесін оңтайландыру бойынша міндеттер кешенін келесілер арқылы шешеді:

1) қорғау шараларын жүйелі түрде түзету және толықтыру;

2) әрекет етудің дайын сценарийлерін пайдалану есебінен, шабуылдар мен ақпараттық қауіпсіздік инциденттеріне әрекет ету уақытын қысқарту;

3) ақпараттық қауіпсіздік инциденттерін анықтауға және оларға ден қоюға арналған автоматтандыру құралдарын енгізу.

20. ЖАҚО жұмыс станцияларындағы, серверлердегі және желілердегі, қосымшалардағы, дерекқорлардағы, веб-сайттардағы және басқа да корпоративтік интернет-ресурстардағы белсенділікті бақылайды.

21. ЖАҚО міндеттері:

1) зиянды және аномальды әрекеттерді анықтау;

2) қатерлерді сәйкестендіру;

3) ақпараттық қауіпсіздік инциденттеріне талдау жүргізу және кейіннен ақпараттық қауіпсіздік саласында туындайтын тәуекелдерді бағалау;

4) әрбір оқиғаны тіркеу және тексеру;

5) корпоративтік деректердің бұзылуына (компроматқа) жол бермеу.

22. АЖ міндеттері Қор басшылығының жалпы саясатының элементі болып табылады, Қор қызметінің, басшылықтың және Қазақстан Республикасы заңнамасының талаптарына негізделеді, Қорда тәуекелдерді басқару жөніндегі талаптарға сәйкес әзірленеді және іске асырылады.

23. АҚ-ны қамтамасыз ету ақпаратты және оны қолдайтын инфрақұрылымды қорғауға бағытталған кез келген қызметті қамтиды.

24. АҚ-ны ұйымдастырудың ажырамас бөлігі қабылданатын шаралардың тиімділігін үздіксіз бақылау, қызметкерлер үшін жол берілмейтін әрекеттердің (әрекетсіздіктің), ықтимал салдарлар мен жауапкершіліктің тізбесін айқындау болып табылады.

25. АҚ-ның сенімді жүйесін қамтамасыз ету мақсатында оның параметрлерін тұрақты реттеу, сыртқы және ішкі ортадан шығатын жаңа қауіптерді көрсету үшін бейімдеу қажет. Стандарттарға, рәсімдерге немесе Саясатқа өзгерістер енгізу кезінде, мұндай қажеттіліктің туындауына қарай қандай да бір кедергілер болмауы тиіс.

Осы ережеге сәйкес АҚ-ны басқару циклының мынадай кезеңдері айқындалады (PDCA моделі: Plan-Do-Check-Act):

1) Plan - жоспарлау (әзірлеу) – Қордың жалпы стратегиясы мен мақсаттарына сәйкес нәтижелер алу үшін тәуекелдерді басқаруға және АҚ-ны жетілдіруге жататын тәуекелдерді талдау, Саясатты, мақсаттарды, міндеттерді, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды айқындау;

2) Do - іске асыру (енгізу және пайдалану) – Саясатты, бақылау тетіктерін, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды енгізу және пайдалану;

3) Check - тексеру (мониторинг және талдау) – бағалау және ол қолданылатын жерде – Саясатқа, мақсаттарға және практикалық тәжірибеге сәйкес процестердің орындалу сипаттамаларын өлшеу, ақпараттық ресурстардың қорғалуына әсер ететін сыртқы және ішкі факторлардың өзгеруін талдау, басшылыққа талдау есептерін ұсыну;

4) Act - түзету (ілеспе қызмет көрсету және жетілдіру) – АҚ жүйесін үздіксіз жетілдіруді қамтамасыз ету мақсатында, АҚ жағдайын ішкі және сыртқы тексерулер нәтижелеріне негізделген түзету және алдын алу шараларын, басшылық тарапынан қойылатын талаптарды және басқа да факторларды қабылдау.

26. Қордың ақпараттық қауіпсіздік жүйесін құру және оның жұмыс істеуі келесідей негізгі қағидаттарға сәйкес жүзеге асырылады:

1) заңдылық – Қордың АҚ объектілеріне теріс әсерлерді анықтау, алдын алу, оқшаулау және жолын кесудің Қазақстан Республикасының заңнамасымен рұқсат етілген барлық әдістерін пайдалана отырып, Қазақстан Республикасының қолданыстағы заңнамасы негізінде жүзеге асырылатын ақпараттық қауіпсіздікті қамтамасыз ету бойынша қабылданатын кез келген іс-әрекеттер;

2) Қор қызметін бағдар тұту – АҚ Қор қызметінің негізгі бағыттарын қолдау процесі ретінде қарастырылады. АҚ-ны қамтамасыз ету жөніндегі кез келген шаралар Қордың қызметінде елеулі кедергілерге алып келмеуі тиіс;

3) үздіксіздік – ақпаратты қорғау жүйелерін басқару құралдарын пайдалану, Қордың ақпаратын қорғауды қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру Қордың ағымдағы процестерін үзбей немесе тоқтатпай жүргізілуі тиіс;

4) кешенділік – ақпараттық ресурстардың қауіпсіздігін олардың бүкіл өмірлік циклінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық жұмыс істеу режимдерінде қамтамасыз ету;

5) негізділік және экономикалық орындылық – пайдаланылатын қорғау құралдары мен мүмкіндіктер ғылым мен техниканың тиісті даму деңгейінде іске асырылады, қауіпсіздіктің берілген деңгейі тұрғысынан негізделген және қойылатын талаптар мен нормаларға сәйкес келеді. Барлық жағдайларда АҚ шаралары мен жүйелерінің құны тәуекелдің кез келген түрінен болуы мүмкін залалдың мөлшерінен аз болуы тиіс;

6) басымдылық – АҚ-ның нақты және ықтимал қатерлерін бағалау кезінде Қордың барлық ақпараттық ресурстарын маңыздылық дәрежесі бойынша жіктеу (саралау);

7) қажетті білім және артықшылықтардың ең төменгі деңгейі – пайдаланушы артықшылықтардың ең төменгі деңгейін алады және тек өз өкілеттіктері шегінде қызметін атқаруға қажетті деректерге ғана қол жеткізе алады;

8) мамандандыру – техникалық құралдарды пайдалану мен АҚ шараларын іске асыруды Қордың кәсіби даярлықтан өткен мамандары жүзеге асырады;

9) хабардарлық және жеке жауапкершілік – барлық деңгейдегі басшылар мен барлық қызметкерлер ақпараттық қауіпсіздіктің барлық талаптарынан хабардар және осы талаптарды орындау және ақпараттық қауіпсіздіктің белгіленген шараларын сақтау үшін жеке жауапкершілікте болады;

10) өзара іс-қимыл және үйлестіру – ақпараттық қауіпсіздік шаралары Қордың тиісті құрылымдық бөлімшелерінің өзара іс-қимылы, олардың мақсаттарына жету жолындағы күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіптік қауымдастықтармен және қоғамдастықтармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыстарды орнату негізінде жүзеге асырылады.

11) растау – маңызды құжаттама және барлық жазбалар – АҚ талаптарының орындалуын және оны ұйымдастыру жүйесінің тиімділігін растайтын құжаттар жылдам қол жеткізу және қалпына келтіру мүмкіндігімен жасалады және сақталады.

4-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету және ақпаратты қорғау объектілері

27. Мына элементтер Қордағы ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері болып танылады:

1) жеке деректерді және Қазақстан Республикасының қолданыстағы заңнамасына және Қордың ішкі нормативтік құжаттарына сәйкес Қордың құпия ақпаратына, коммерциялық құпиясына жатқызылған мәліметтерді қамтитын ақпараттық ресурстар, Қордың қалыпты жұмыс істеуін қамтамасыз етуге қажетті кез келген басқа ақпарат (бұдан әрі – қорғалатын ақпарат);

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

3) соның көмегімен қорғалатын ақпаратты өңдеу жүргізілетін Қордың автоматтандырылған жүйесінің бағдарламалық құралдары (операциялық жүйелер, деректер базасын басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық жасақтама);

4) ақпараттық ресурстарды басқару мен пайдалануға байланысты Қор процестері;

5) қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

6) қызметкерлердің кабинеттері және Қордың басқа да үй-жайлары;

7) қорғалатын ақпаратқа рұқсаты бар Қор қызметкерлері;

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

28. Қорғауға жататын ақпарат:

1) қағазға түсірілуі;

2) электрондық түрде болуы (есептеу техникасы құралдарымен өңделуі, жіберілуі және сақталуы, техникалық құралдардың көмегімен жазылуы және көбейтілуі);

3) телефон, телефакс, телекс және басқа да осыған ұқсас құрылғылар арқылы электр сигналдары түрінде берілуі мүмкін.

5-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары

29. Қордың АҚ-ны қамтамасыз ету бойынша негізгі шаралары:

1) әкімшілік-құқықтық және ұйымдастыру шаралары;

2) жеке қауіпсіздік шаралары;

3) бағдарламалық-техникалық шаралар.

30. Әкімшілік-құқықтық және ұйымдастыру шаралары келесілерден тұрады (бірақ олармен шектелмейді):

1) бағалы қағаздар нарығында коммерциялық құпияны, зейнетақы жинақтарының, шартты зейнетақы шоттарының, нысаналы жинақтардың құпиясын құрайтын мәліметтердің сақталуын қамтамасыз ету және оларды Қордың, олардың қызметкерлерінің немесе үшінші тұлғалардың өз мүдделеріне пайдалануына жол бермеу жөніндегі рәсімдерді белгілеу;

2) конфеденциалды ақпаратқа жататын ақпарат тізбесін, конфеденциалды ақпараттан тұратын құжаттарды жасау, ресімдеу, тіркеу, есепке алу және сақтау тәртібін белгілеу;

3) лауазымды адамдарды көрсете отырып, конфеденциалды ақпаратқа рұқсат беру тәртібін белгілеу;

4) конфеденциалды ақпараттың таралуын және келесілерді: қолжетімділігі шектеулі ақпараттық деректер тізбесі, ақпараттық деректерге қолжетімділікті алу тәртібі, қолжетімділікті бақылау тәртібі мен ақпараттық деректерге қолжетімділігі бар адамдар лауазымдарының тізбесі қарастырылған ақпараттық деректердің бұрмалануын болдырмау тетіктерін (механизмдерін) белгілеу;

5) деректер қорын пайдаланушыларды мониторингтеу және сәйкестендіру және ақпараттық жүйені пайдаланушыны сәйкестендіруге мүмкіндік беретін жүйемен қамтамасыз ету арқылы дерекқорға рұқсатсыз кіруді болдырмау жөнінде іс-шаралар әзірлеу;

6) Қазақстан Республикасының заңнамасы мен Қордың ішкі нормативтік құжаттары талаптарының сақталуын бақылау;

7) Саясатты қолдайтын ережелерді, әдістер мен нұсқауларды әзірлеу, енгізу және орындалуын бақылау;

8) процестердің Саясат талаптарына сәйкестігін бақылау;

9) Қор қызметкерлеріне ақпараттық жүйелермен жұмыс істеу және АҚ талаптары жөнінде ақпарат беру және оқыту;

10) тосын оқиғаларға ден қою, салдарларын оқшаулау және азайту;

11) АҚ жаңа тәуекелдерін талдау және бағалау;

12) ұжымдағы моральдық және іскерлік ахуалды бақылау және жақсарту;

13) төтенше жағдайлар кезіндегі іс-қимылдарды анықтау;

14) Қор қызметкерлерін жұмысқа қабылдау және жұмыстан босату кезінде профилактикалық іс-шараларды жүргізу.

31. Физикалық қауіпсіздік шаралары келесілерді қамтиды (бірақ олармен шектелмейді):

1) өткізу және объектішілік режимдерді ұйымдастыру;

2) қорғалатын объектілердің қауіпсіздік периметрін құру;

3) күзетілетін объектілерді тәулік бойы күзетуді, оның ішінде техникалық қауіпсіздік құралдарын пайдалана отырып күзетуді, ұйымдастыру;

4) күзетілетін объектілердің өртке қарсы қауіпсіздігін ұйымдастыруды;

5) кіру шектеулі үй-жайларға Қор қызметкерлерінің кіруін бақылау;

6) жоспарланған іс-шараларды орындау.

32. Бағдарламалық-техникалық шаралар келесілерді қамтиды (бірақ олармен шектелмейді):

1) лицензиялық бағдарламалық жасақтаманы және ақпаратты қорғаудың сертификатталған құралдарын пайдалану;

2) периметрді қорғау құралдарын пайдалану (firewall, Data Loss Prevention (DLP) және т.б.);

3) вирусқа қарсы кешенді қорғауды қолдану;

4) ақпараттық жүйелерге орнатылған АҚ құралдарын пайдалану;

5) ақпаратты тұрақты резервтік көшіруді қамтамасыз ету;

6) пайдаланушылардың, ең алдымен кеңейтілген қол жеткізу құқықтары барлардың, құқықтары мен әрекеттерін бақылау;

7) ақпаратты криптографиялық қорғауды пайдалану;

8) аппараттық құралдардың тоқтаусыз жұмыс істеуін қамтамасыз ету;

9) ақпараттық жүйенің маңызды элементтері жай-күйінің мониторингі.

6-тарау. Ақпараттық қауіпсіздік қатерлері

33. АҚ қатерлері ақпараттың негізгі қасиеттерінің ықтималды бұзылуын білдіреді.

34. АҚ қатерлері келесілерге бөлінеді (бірақ олармен шектелмейді):

1) кездейсоқ – табиғи апаттар, абайсызда жасалған қателер, аппараттық және бағдарламалық құралдардың қателері және істен шығуы;

2) қасақана, яғни деректерді бұрмалау немесе жою, деректерді заңсыз пайдалану, компьютерлік қылмыстар және басқа да құқық бұзушылықтар.

35. АҚ қатерлерінің қатарына мыналар жатады (бірақ олармен шектелмейді):

1) коммерциялық құпияны құрайтын ақпаратты (конфеденциалды ақпаратты) және басқа да қорғалатын ақпаратты жоғалту;

2) қорғалатын ақпаратты бұрмалау (рұқсат етілмеген өзгерту, қолдан жасау);

3) жария болу – бөгде адамдардың қорғалатын ақпаратпен рұқсатсыз танысуы (рұқсатсыз алу, көшірме жасау, ұрлау және басқа да құқық бұзушылықтар);

4) ақпараттық ресурстарды рұқсатсыз пайдалану (теріс пайдалану, алаяқтық және басқа да құқық бұзушылықтар);

5) ақпараттың бұғатталуы, жабдықтың немесе бағдарламаның істен шығуы, жұмыс станцияларының операциялық жүйелерінің, серверлердің, белсенді желілік жабдықтардың, деректер қорын басқару жүйелерінің, бөлінген есептеуіш желілері жұмысының бұзылуы, вирустардың, табиғи апаттардың (төтенше және дағдарыстық жағдайлар) басқа форс-мажор жағдайлары мен зиянды іс-әрекет әсерлерінің нәтижесінде ақпараттың қолжетімсіз болуы.

36. Осы қатерлер әсерінің нәтижесінде Қордың АҚ жағдайына және оның қалыпты жұмыс істеуіне ықпал ететін мынадай жағымсыз салдарлар туындауы мүмкін (қоса алғанда, бірақ олармен шектелмей):

1) зейнетақы жинақтары, шартты зейнетақы шоттары, нысаналы жинақтар мен қорғалатын басқа да ақпарат құпияларының заңсыз жария болуына байланысты, Қорға санкциялардың, өкімдер мен өзге де реттеу шараларының қолданылуы;

2) қорғалатын ақпараттың таралуына немесе жария етілуіне байланысты қаржылық шығындар;

3) ақпараттың жойылуына және жоғалған ақпаратты кейіннен қалпына келтіруге байланысты қаржылық шығындар;

4) Қор қызметінің бұзылуынан келген залал және оның өз міндеттемелерін орындай алмауына байланысты шығындар;

5) басқару шешімдерін теріс (дұрыс емес) ақпарат негізінде қабылдаудан келетін залал;

6) Қор басшылығында объективті ақпараттың болмауынан келетін залал;

7) Қордың беделіне нұқсан келтіру;

8) басқа залал түрлері

7-тарау. Өкілеттіктер мен жауапкершіліктерді бөлу

37. АҚ құрудың негізгі қағидаты Қордың әрбір қызметкері АҚ саясатын сәтті жүзеге асыру үшін жауапты болады.

38. Қор басшылығы:

1) стратегиялық жоспарлауды жүзеге асырады;

2) ішкі нормативтік құжаттарды бекітеді;

3) АҚ саласындағы бөлімшелердің өкілеттіктері мен жауапкершілігін айқындайды;

4) Қор қызметінің ақпараттық қауіпсіздігінің тиісті деңгейін ұйымдастыру және қолдау үшін барлық бөлімшелердің қызметін үйлестіреді;

5) АҚ жүйесін әзірлеу, енгізу, пайдалану, мониторингтеу, талдау, қолдау және жетілдіру үшін жеткілікті ресурстарды бөледі;

6) тәуекелдерді қабылдау өлшемдері мен тәуекелдің рұқсат етілетін деңгейі туралы шешімдер қабылдайды;

7) АҚ жағдайына сыртқы және ішкі тексеру жүргізуді қамтамасыз етеді;

8) киберқауіпсіздік бөлімшесі арқылы АҚ жағдайына жыл сайын талдау жүргізеді;

9) АҚ жалпы жағдайына жауап береді.

39. Киберқауіпсіздік бөлімі:

1) ЖАҚО ретінде, оқиғаларды орталықтандырылған жинақтау мен желілік белсенділік арқылы нақты уақыт режимінде АҚ жағдайы туралы ақпаратты, Қорға қауіп төндіретін ықтимал қауіпті және күдікті белсенді әрекеттер туралы ақпаратты алады.

2) АҚ тосын оқиғаларына талдау жасайды, әзірлейді және негіздер болған жағдайда, олардың туындауының алдын алуға бағытталған ұсынымдар береді;

3) Қор басшылығының шешімдерін іске асырады және АҚ қамтамасыз ету жүйесін жалпы ұйымдастыруды жүзеге асырады, Қордың барлық бөлімшелерінің АҚ саласындағы қызметін үйлестіреді және бақылайды;

4) Қорда АҚ дамыту стратегиясын, сондай-ақ Қордың ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жылдық бюджеттердің жобаларын қарайды, Қордың АҚ бойынша бағдарламалық-техникалық шешімдерін дамыту және енгізуге мониторинг жүргізеді, Қордың АҚ бойынша ұйымдастыру шараларын енгізеді, өзінің өзектілігін жоғалтқан АҚ жөніндегі қолданыстағы жобалардан бас тартады;

5) жоба жетекшілері ұсынатын есептер бойынша жобалардың іске асырылуына аралық бақылау жасайды, сондай-ақ Қор басшылығына жобаларды табысты іске асырғаны үшін қызметкерлерді көтермелеу және киберқауіпсіздік бөлімшесінің шешімдерін орындамағаны немесе жобаларды орындау мерзімдерін бұзғаны үшін тәртіптік жауапкершілікке тарту туралы ұсынымдар енгізеді;

6) Қордың АҚ басқару және қамтамасыз ету процесін қолдауды қамтамасыз етеді;

7) Қордың АҚ бақылау, басқару және қамтамасыз ету құралдары мен тетіктерін таңдайды;

8) Қордың АҚ құралдары кешенінің штаттық жұмыс істеуін қамтамасыз етеді;

9) Қордың АҚ саласындағы қатерлерді талдайды және бағалайды;

10) ақпарат алмасуға барлық қатысушылардың АҚ талаптарын сақтауын бақылайды;

11) қызметкерлерді басқару бөлімшесімен бірлесіп, бейімдеу/электрондық/жыл сайынғы курстарды ұйымдастыруға көмектесу бөлігінде, жаңадан келген және бұрыннан жұмыс істейтін қызметкерлерді АҚ талаптарымен оқыту процесін қамтамасыз етеді;

12) Қордың АҚ жағдайына мониторинг жүргізеді;

13) ақпараттық қауіпсіздікті бұзуға байланысты оқиғалар мен инциденттерді өңдейді, тиісті қорытындылар мен ұсынымдар дайындайды;

14) ішкі нормативтік құжаттар регламентіне сәйкес АҚ қамтамасыз ету жүйесінің жай-күйі туралы Қор басшылығына хабарлайды;

15) тәуекелдерді талдау және бағалау процесіне әдіснамалық қолдау көрсетеді;

16) Қордың негізгі және операциялық тәуекелдерді басқару жөніндегі ішкі құжаттарының талаптарына сәйкес тәуекелдерді басқару бөліміне Қордың ақпараттық қауіпсіздігін қамтамасыз ету саласындағы оқиғалар мен инциденттер туралы хабарлайды;

17) негізгі және операциялық тәуекелдерді басқару мәселелері жөніндегі ішкі құжаттардың талаптарына сәйкес АҚ бұзушылықтарына байланысты оқиғалар мен инциденттерді тіркеуді бақылайды;

18) «БЖЗҚ» АҚ ақпараттық қауіпсіздікті басқару жүйесінің тәуекелдерін бағалау және өңдеу әдістемесіне сәйкес, тәуекелдерді өңдеу және АҚ тәуекелдерін азайту шараларын әзірлей отырып, АҚ тәуекелдерін сәйкестендіру және бағалау процесінің жұмыс істеуін қамтамасыз етеді;

19) тартылған бөлімшелермен бірлесіп, «БЖЗҚ» АҚ үздіксіз қызметін қамтамасыз ету және қалпына келтіру жоспарында көзделген іс-шараларды, оның ішінде төтенше дағдарыс және/немесе дағдарысты емес жағдайлар туындағанға дейін жүргізілген іс-шараларды іске асыруға қатысады.

40. АЖ ресурстарының әкімшілері желінің үздіксіз жұмысын қамтамасыз етеді және қауіпсіздік саясатын іске асыруға қажетті техникалық шаралардың орындалуына жауап береді:

1) пайдаланушылардың Қорда қабылданған талаптарға сәйкес Қордың ақпараттық ресурстарына қолжетімділігін қамтамасыз етеді;

2) Қорда қабылданған талаптарға сәйкес жүйелік және қолданбалы бағдарламалық жасақтаманы конфигурациялайды;

3) Қордың ақпараттық ресурстарының үздіксіз жұмысын, тұтастығын және қолжетімділігін (ақпаратты архивтеу және резервтік көшірмелерін жасауды қоса алғанда), оларда өңделетін ақпараттың конфеденциалдылығын (орнатылған қауіпсіздік механизмдерін басқару) қамтамасыз етеді;

4) Қордың АТ-қызметтерін басқару жүйесінің тиісті деңгейде жұмыс істеуін қамтамасыз етеді;

5) Қордың барлық процестерінің үздіксіздігін қамтамасыз етеді, Қор қызметтері саласындағы бұзушылықтардан болатын ықтимал шығындар мен залалдарды азайтады.

41. Тәуекелдерді басқару бөлімшесі Қордың АҚ саласындағы тіркелген оқиғалар мен инциденттерге, АҚ тәуекелдерін сәйкестендіру және бағалау нәтижелеріне талдау жүргізеді. АҚ тәуекелдерін өңдеу жоспары мен АҚ тәуекелдерін азайту бойынша, Қор тәуекелдерін басқарудың жұмыс істейтін жүйесі аясындағы негізгі және операциялық тәуекелдерді басқару жөніндегі ішкі нормативтік құжаттардың талаптарына сәйкес, олардың орындалуына кейіннен мониторинг жүргізу үшін, тәуекелдерді азайту жөніндегі жоспарға кіргізудің орындылығын анықтау мақсатында, әзірленген шараларды зерттеп танысады.

42. Қызметкерлерді басқару бөлімі:

1) кандидаттарды жұмысқа қабылдау және Қор қызметкерлерімен, сондай-ақ тағылымдамадан өтушілермен, практиканттармен тиісті келісімдерге (еңбек шарттарына, тағылымдамадан өту туралы шарттарға, - қызметтік, коммерциялық құпияны (конфеденциалды ақпаратты) жария етпеу туралы міндеттемелерге) қол қою кезінде бастапқы құжаттарды жинау бойынша міндетті іс-шаралар кешенін жүргізеді;

2) Қор басшылығының нұсқауымен Саясатты және АҚ бойынша ішкі нормативтік құжаттарды бұзған жағдайда Қор қызметкерлерін тәртіптік жауапкершілікке тарту шараларын қамтамасыз етеді.

43. 43. Заң департаменті ақпараттық қауіпсіздік саласындағы ішкі нормативтік құжаттар жобаларының ішкі нормативтік құжаттың жобасын құқықтық тіркеудің жалпыға бірдей белгіленген тәртібіне және Қазақстан Республикасының заңнамасына сәйкестігіне тексереді.

44. Қордың құрылымдық бөлімшелерінің басшылары:

1) қызметкерлерді ағымдағы АҚ талаптарымен таныстыруды қамтамасыз етеді;

2) өздеріне сеніп тапсырылған бөлімшелерде АҚ қамтамасыз етуге жауап береді.

45. Қордың құрылымдық бөлімшелері:

1) Қор қызметтерін енгізу, түрлендіру, ұсыну кезінде АҚ талаптарының сақталуына жауап береді;

2) өздері бизнес-иелері болып табылатын ақпараттық жүйелерге/процестерге қол жеткізу құқықтарын келіседі.

46. Ақпараттық жүйені пайдаланушылар:

1) осы Саясат талаптарының, сондай-ақ ақпараттық жүйеде қауіпсіз жұмыс істеуді қамтамасыз ету жөніндегі өзге де ішкі нормативтік құжаттардың сақталуына жауап береді;

2) осы Саясатта және Қордың басқа да ішкі құжаттарында жазылған АҚ талаптарын, өздерінің лауазымдық міндеттері шеңберінде байланысатын үшінші тұлғалардың орындауын.

оның ішінде көрсетілген талаптарды үшінші тұлғалармен жасалған шарттарға енгізу арқылы, бақылайды;

3) ақпараттық ресурстармен жұмыс істеу кезіндегі барлық күдікті жағдайлар мен бұзушылықтар туралы тікелей басшысынға және киберқауіпсіздік бөлімшесіне хабарлауға міндетті.

8-тарау. Талдау және қайта қарау

47. Осы саясатты, Қордың ақпараттық қауіпсіздік, ақпараттық жүйелер және АҚ жүйесі жөніндегі туынды құжаттарын талдау және бағалау мынадай іс-шаралардың нәтижелері негізінде кемінде екі жылда бір рет қайта қаралады:

1) Қор басшылығының АҚ жүйесінің жағдайы мен тиімділігіне талдау жасауы;

2) кибер қауіпсіздік бөлімшесінің АҚ жағдайын ағымдағы тексеруі;

3) ақпараттық жүйелерді күдікті осал жерлердің бар-жоғы тұрғысынан сканерлеу және киберқауіпсіздік бөлімшесі немесе сыртқы білікті аудиторлар жүргізетін жүйеге кіріп кетулер бойынша тесттен өткізу;

4) қауіпсіздік бөлімі анықтаған инциденттер мен АҚ талаптарының бұзылуы;

5) аудиторлық тексерулер кезінде АҚ жағдайын тексеру;

6) АҚ жүйесіне жүргізілетін басқа да аудиттер мен тексерулер.

48. Қолданыстағы жүйелерді тексеруді талап ететін аудиторлық іс-шаралар бизнестің тоқтау қаупін барынша азайтатындай етіп жоспарлануы және келісілуі керек.

49. Ақпараттық жүйелердің аудит құралдары мен нәтижелеріне қолжетімділік рұқсатсыз пайдалану, компромат жасау немесе өзгерту мүмкіндіктерінің алдын алу мақсатында қорғалады және шектеледі.

50. Осы Саясатты және Қордың ақпараттық қауіпсіздік жөніндегі туынды құжаттарын қайта қарау Саясаттың 46-тармағына сәйкес талдау және бағалау процесінің нәтижелері бойынша жүзеге асырылады.

9-тарау. Қорытынды ережелер

50. Ақпараттық ресурстарды пайдалану тәртібі мен қағидаларын және Қорда қабылданған АҚ шараларын сақтамау Қазақстан Республикасының заңнамасына және Қордың ішкі нормативтік құжаттарына сәйкес жауаптылыққа апарады.

51. Осы Саясат Қор қызметіндегі өзгерістерді, Қазақстан Республикасының заңнамасындағы өзгерістерді ескере отырып және қажет болған жағдайда осы Саясаттың 2-тарауының талаптарын ескере отырып қайта қаралады.

52. Саясаттың ережелерінде қарастырылмаған мәселелер Қазақстан Республикасының заңнамасына, Қордың ішкі құжаттарына және Директорлар кеңесінің шешімдеріне сәйкес шешіледі (бұл ретте Қазақстан Республикасы заңнамасының күші басым болады).

53. Осы Саясаттың өзекті мазмұнына Киберқауіпсіздік бөлімі жауапты.

54. Саясат жария құжат болып табылады және Қордың кез келген ақпараттық ресурстарында орналастырылуы мүмкін.

«БЖЗҚ» АҚ Басқарма Төрағасы **Ж. Курманов**

«БЖЗҚ» АҚ ақпараттық қауіпсіздік саясатын келісу парағы

Лауазым атауы	Атының инициалы, тегі	Қолы	Ескерту
Сыбайлас жемқорлыққа қарсы комплаенс басқармасы	А. Жукенова		
Заң департаменті директорының орынбасары	А. Бимен		
Тәуекел-менеджмент департаментінің директоры	Э. Талаева		
Қызметкерлерді басқару департаменті директорының орынбасары	Г. Жиеналина		
Төлемдерді ұйымдастыру және хабарландыру департаментінің директоры	Н. Рахимова		
Зейнетақы активтерін есепке алу және есептілік департаменті	А.Тусеева		
Инфрақұрылымды дамыту және қолдау департаментінің директоры	Р. Лосевской		

Осы арқылы қағаз нұсқадағы туынды құжаттың электрондық нұсқада келісілген құжатқа сәйкес келетінін растаймыз.

Әзірлеуші:
Киберқауіпсіздік департаментінің **директоры** _____ (қолы) Е. Алдабеков

Прошито и пронумеровано

на 12 (двенадцать) листах

Директор Департамента кибербезопасности

_____ Е. Алдабеков