

Выписка из Протокола № 50
заседания Совета директоров акционерного общества
«Национальная платежная корпорация Национального Банка
Республики Казахстан» от 9 сентября 2026 года

10 сентября 2026 года

<i>Полное наименование акционерного общества</i>	Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – Общество)
<i>Место нахождения Общества</i>	Республика Казахстан, город Алматы, A15C9T5, микрорайон «Коктем-3», дом 21
<i>Форма проведения заседания</i>	Заочно
<i>Кворум заседания</i>	Соблюден, на голосование представлены 5 бюллетеней.
<i>Корпоративный секретарь</i>	Байтасов Д.Б.

По вопросу повестки дня заседания:

...

2. Об утверждении Политики информационной безопасности в акционерном обществе «Национальная платежная корпорация Национального Банка Республики Казахстан».

...

Решение:

1. Признать утратившей силу Политику информационной безопасности в акционерном обществе «Национальная платежная корпорация Национального Банка Республики Казахстан», утвержденную решением Совета директоров АО «НПК» от 21 ноября 2023 года (Протокол № 3).

2. Утвердить Политику информационной безопасности в акционерном обществе «Национальная платежная корпорация Национального Банка Республики Казахстан» согласно приложению № 7 к настоящему Протоколу.

3. Правлению Общества (Самаева Ж.Т.) довести настоящее решение до сведения руководителей структурных подразделений Общества.

4. Настоящее решение вступает в силу с даты его принятия.

Выписка верна
Корпоративный секретарь



Д. Байтасов



**Акционерное общество «Национальная платежная корпорация
Национального Банка Республики Казахстан»**

Приложение № 7
к Протоколу заседания
Совета директоров АО «Национальная платежная корпорация
Национального Банка Республики Казахстан»
от 9 сентября 2026 года № 50

Дата вступления в силу с
9 сентября 2026 года

**Политика
информационной безопасности в акционерном обществе «Национальная
платежная корпорация Национального Банка Республики Казахстан»**

Рег. № _____

г. Алматы

Содержание

Глава 1. Общие положения.....	3
Глава 2. Цели и задачи	3
Глава 3. Основные положения СУИБ.....	4
Глава 4. Модель управления.....	6
Глава 5. Ответственность и контроль.....	6
Глава 6. Заключительные положения.....	7

Глава 1. Общие положения

1. Политика информационной безопасности акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – Политика) является основополагающим документом, отражающим основные принципы в обеспечении информационной безопасности в акционерном обществе «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – Общество).

2. Политика разработана в соответствии с требованиями:

- 1) Цифрового кодекса Республики Казахстан;
- 2) Закона Республики Казахстан «О Национальном Банке Республики Казахстан»;
- 3) Закона «О банках и банковской деятельности в Республике Казахстан»;
- 4) Закона Республики Казахстан «О платежах и платежных системах»;
- 5) Закона Республики Казахстан «О персональных данных и их защите»;
- 6) правовых актов Национального Банка Республики Казахстан и Агентства Республики Казахстан по регулированию и развитию финансового рынка, регулирующих вопросы информационной безопасности;
- 7) национального стандарта Республики Казахстан СТ РК ISO/IEC 27001.

3. Орган управления Общества осознает важность и необходимость создания, развития и постоянного совершенствования системы управления информационной безопасностью (далее – СУИБ) в условиях существующих и потенциальных угроз информационной безопасности, а также изменений законодательства Республики Казахстан и технологической среды.

4. Общество обеспечивает соответствие своей деятельности применимым законодательным и регуляторным требованиям, а также международным и государственным стандартам в области информационной безопасности.

5. В целях соблюдения применимых законодательных и регуляторных требований, а также международных и государственных стандартов в области информационной безопасности Общество обеспечивает своевременный мониторинг изменений таких требований и стандартов, а также актуализацию внутренних нормативных документов СУИБ в соответствии с указанными изменениями.

Глава 2. Цели и задачи

6. Целью Политики является определение единого подхода в обеспечении информационной безопасности в Обществе, направленного на организацию защиты активов Общества.

7. Основными задачами для выполнения цели Политики являются:

- 1) обеспечение конфиденциальности, целостности и доступности хранимой, передаваемой и обрабатываемой информации, а также защита информации третьих сторон;
- 2) выявление, предупреждение и нейтрализация угроз информационной безопасности, а также установление причин и условий их возникновения;
- 3) минимизация и локализация последствий реализации угроз информационной безопасности, а также проведение анализа инцидентов

информационной безопасности для предотвращения их повторного возникновения;

4) обеспечение соответствия деятельности Общества применимым законодательным, регуляторным требованиям, международным и национальным стандартам в области обеспечения информационной безопасности, а также постоянная актуализация внутренних нормативных документов Общества в области обеспечения информационной безопасности;

5) повышение уровня осведомленности работников Общества в области информационной безопасности и формирование культуры безопасной работы с активами;

6) контроль эффективности и достаточности применяемых организационных и технических мер защиты активов.

8. Основные направления реализации Политики и соблюдения требований информационной безопасности в Обществе осуществляются за счёт:

1) реализации организационных и технических мер защиты активов;

2) соблюдения законодательных и регуляторных требований, а также применимых требований национальных и международных стандартов в области обеспечения информационной безопасности;

3) разработки и соблюдения внутренних нормативных документов, регулирующих различные аспекты обеспечения информационной безопасности, включая, но не ограничиваясь, процессы управления аутентификацией и разграничением прав доступа, управления учетными записями пользователей, управления информационными активами и их классификацией, защиты информации при ее обработке, хранении и передаче, управления криптографическими средствами защиты информации, обеспечения безопасности сетевой инфраструктуры и информационных систем, управления уязвимостями и анализа защищенности, мониторинга событий информационной безопасности и реагирования на инциденты информационной безопасности, обеспечения безопасности при разработке и сопровождении программного обеспечения, управления изменениями информационных систем, резервного копирования и восстановления информации, обеспечения безопасности при взаимодействии с поставщиками и третьими сторонами, а также обеспечения физической безопасности объектов информационно-коммуникационной инфраструктуры.

Глава 3. Основные положения СУИБ

9. Для достижения цели настоящей Политики Общество обеспечивает функционирование и постоянное совершенствование СУИБ, направленной на обеспечение конфиденциальности, целостности, доступности активов Общества на основе применения риск-ориентированного подхода.

10. Функционирование СУИБ осуществляется в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются в соответствии с законодательством Республики Казахстан с применением разрешённых

законодательством методов выявления, предупреждения, локализации и пресечения негативных воздействий на активы Общества;

2) комплексность – обеспечение безопасности активов на всех этапах жизненного цикла, а также во всех режимах функционирования активов;

3) персональная ответственность – члены Правления, руководители структурных подразделений и работники Общества должны быть осведомлены о требованиях информационной безопасности и несут персональную ответственность за соблюдение установленных мер защиты активов;

4) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимодействия структурных подразделений Общества, координации их деятельности для достижения поставленных целей, а также взаимодействия с государственными органами, профессиональными сообществами и иными организациями по вопросам обеспечения информационной безопасности.

11. Функционирование СУИБ в Обществе обеспечивается при соблюдении следующих требований:

1) определение и поддержание области действия СУИБ;

2) идентификация, анализ, оценка и обработка рисков информационной безопасности на регулярной основе, а также при существенных изменениях в деятельности Общества;

3) определение ролей, ответственности и полномочий работников в области обеспечения информационной безопасности;

4) разработка, утверждение и актуализация внутренних нормативных документов в области информационной безопасности;

5) обеспечение осведомленности работников по вопросам информационной безопасности;

6) мониторинг, анализ и оценка эффективности функционирования СУИБ;

7) обеспечение соответствия требованиям законодательства Республики Казахстан и внутренним нормативным документам Общества;

8) непрерывное совершенствование СУИБ на основе результатов мониторинга, проверок и анализа инцидентов;

9) проведение внутренних проверок функционирования СУИБ;

10) проведение анализа функционирования СУИБ со стороны руководства Общества с целью оценки её достаточности, результативности и соответствия целям деятельности Общества, а также принятия решений по её совершенствованию.

12. Область действия СУИБ распространяется на все структурные подразделения и работников Общества, бизнес-процессы, включая процессы взаимодействия с третьими лицами, а также активы, используемые в деятельности Общества.

13. Работники подразделения информационной безопасности Общества проходят регулярное обучение и повышение квалификации в области информационной безопасности.

Глава 4. Модель управления

14. Функционирование СУИБ в Обществе осуществляется в рамках системы внутреннего контроля на основе модели «трёх линий защиты», обеспечивающей распределение ответственности, независимость контрольных функций и непрерывный контроль соблюдения требований информационной безопасности.

15. Распределение ролей, ответственности, полномочий и функций участников модели «трёх линий защиты», а также порядок их взаимодействия и осуществления контрольных функций определяются внутренними нормативными документами Общества.

Глава 5. Ответственность и контроль

16. Председатель Правления Общества несёт общую ответственность за обеспечение функционирования и совершенствования СУИБ, осуществляет контроль за достижением целей настоящей Политики и обеспечивает выделение необходимых ресурсов для реализации требований информационной безопасности.

17. Организация и координация деятельности по обеспечению информационной безопасности, определение требований к организационным и техническим мерам защиты информации, методологическое сопровождение процессов информационной безопасности, участие в управлении рисками информационной безопасности, а также контроль соблюдения требований в области информационной безопасности осуществляется подразделением информационной безопасности Общества.

18. Руководитель подразделения информационной безопасности несёт ответственность за организацию функционирования СУИБ, координацию процессов обеспечения информационной безопасности, а также осуществление контроля и мониторинга соблюдения требований информационной безопасности в Обществе в пределах компетенции подразделения информационной безопасности.

19. Руководители структурных подразделений и работники Общества несут ответственность за соблюдение требований информационной безопасности, выполнение установленных мер защиты информации и обеспечение безопасного использования активов Общества в пределах своих функциональных обязанностей.

20. Подразделение внутреннего аудита осуществляет независимую оценку эффективности функционирования СУИБ, системы внутреннего контроля и процессов управления рисками информационной безопасности.

21. Представители третьих сторон, имеющие доступ к объектам информатизации и информации Общества, обязаны соблюдать требования информационной безопасности в соответствии с условиями заключённых договоров.

22. Все работники Общества несут персональную ответственность за несоблюдение требований информационной безопасности, установленных внутренними документами СУИБ, и обязаны незамедлительно сообщать обо

всех выявленных нарушениях и инцидентах информационной безопасности в подразделение информационной безопасности.

23. Должностные инструкции работников и договоры с третьими лицами должны содержать требования по обеспечению и соблюдению информационной безопасности Общества. Внутренние документы Общества включают требования информационной безопасности в случае, если регулируемые ими процессы связаны с обработкой, хранением или передачей информации.

Глава 6. Заключительные положения

24. Политика подлежит пересмотру не реже одного раза в 3 года, а также в случаях:

- 1) существенных изменений в деятельности Общества;
- 2) изменений законодательства Республики Казахстан;
- 3) изменения требований государственных органов, осуществляющих регулирование и(или) надзор в сфере деятельности Общества;
- 4) иных обстоятельств, влияющих на функционирование СУИБ.

25. Подразделение информационной безопасности обеспечивает доведение настоящей Политики до сведения всех работников Общества.

26. Политика является общедоступным документом и размещается на официальном интернет-ресурсе Общества.



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

**«Қазақстан Республикасы Ұлттық Банкінің
Ұлттық төлем корпорациясы» АҚ
Директорлар кеңесі отырысының
2026 жылғы 9 қыркүйек № 50 хаттамасына
№ 7 қосымша**

**Күшіне енген күні
2026 жылғы 9 қыркүйек**

**«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.