

№ 22-07/13744 от 28.07.2026  
№ 22-07/12529 от 14.07.2026

**«Волковгеология»**  
акционерлік қоғамы



Акционерное общество  
**«Волковгеология»**

Утверждена  
Решением Правления  
АО «Волковгеология»  
от « 11 » августа 2026 года  
(протокол № 12 )



**ПОЛИТИКА  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
АО «ВОЛКОВГЕОЛОГИЯ»**



г. Алматы, 2026 г.

Дата: 31.07.2026 10:41. Копия электронного документа. Версия СЭД: Документооборот 8.0.0. Положительный результат проверки ЭЦП



## Содержание

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| 1. Область применения .....                                                               | 4  |
| 2. Нормативные ссылки .....                                                               | 4  |
| 3. Термины, определения и сокращения .....                                                | 4  |
| 4. Общие положения .....                                                                  | 6  |
| 5. Цели, задачи и основополагающие принципы обеспечения информационной безопасности ..... | 6  |
| 6. Объекты обеспечения информационной безопасности .....                                  | 7  |
| 7. Разделение полномочий, ответственность и контроль .....                                | 8  |
| 8. Соблюдение требований, управление рисками и постоянное улучшение .....                 | 9  |
| 9. Порядок введения в действие .....                                                      | 10 |



## 1. Область применения

1.1 Политика информационной безопасности АО «Волковгеология» (далее – Политика) является внутренним документом АО «Волковгеология» (далее – Общество), определяющим цели и принципы системы управления информационной безопасностью (далее – СУИБ) Общества и его филиалов в области обеспечения информационной безопасности.

1.2 Политика определяет основные принципы, направления и требования в области обеспечения информационной безопасности (далее – ИБ) Общества, и является основой обеспечения режима ИБ, служит руководством при разработке соответствующих внутренних документов Общества.

1.3 Политика охватывает всю информацию и все информационные системы, владельцем и/или пользователем которых является Общество.

1.4 Положения Политики распространяются на всех работников Общества, а также работников сторонних организаций (подрядчиков, консультантов), имеющих доступ к активам Общества.

## 2. Нормативные ссылки

2.1 Для применения настоящей Политики необходимы следующие нормативные документы:

СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования».

СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью».

## 3. Термины, определения и сокращения

3.1 В настоящей Политике используются следующие термины и определения:

3.1.1 **Актив** – материальный или нематериальный объект, который является информацией, или содержит информацию, или используется для ее обработки, хранения или передачи и имеет ценность для Общества.

Примечание - Под активами подразумеваются все информационные и телекоммуникационные системы Общества, включая мобильные устройства (принадлежащие Обществу), сети, информационные системы, серверы, рабочие станции (персональные компьютеры), системы управления базами данных СУБД и др. Причем рассматриваются и активы, находящиеся не в собственности Общества, но используемые Обществом в рамках сервисных договоров и пр.

3.1.2 **Анализ риска** – систематическое использование информации для идентификации источников риска и оценки степени риска.

3.1.3 **Заинтересованные стороны** – физические и юридические лица, государственные органы, партнеры, клиенты, поставщики и иные субъекты, чьи требования и ожидания в области информационной безопасности являются значимыми для деятельности Общества.

3.1.4 **Информационная безопасность (ИБ)** – комплекс административно-правовых, организационно-распорядительных и технических мер, направленных на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе её сбора, обработки и хранения.

3.1.5 **Информационная система (ИС)** – совокупность методов, процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку и распространение информации.



**3.1.6 Информация ограниченного распространения** – информация, зафиксированная в документах, делах и изданиях, электронных и иных носителях, с пометками «Для служебного пользования» (далее – ДСП) и/или «Конфиденциально», «Коммерческая тайна», относящаяся к сведениям, ограничения на распространение которых диктуются служебной необходимостью.

**3.1.7 Инцидент информационной безопасности (инцидент ИБ)** – нарушения, сбои в ИС, отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и/или условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных активов Общества.

**3.1.8 Мера контроля** – средства управления рисками, включая политики, процедуры, руководства, правила или организационные структуры, которые могут быть административного, технического, управленческого или юридического характера.

**3.1.9 Объект** – пассивный компонент, единица актива автоматизированной системы (устройство, диск, каталог, файл и т.п.).

**3.1.10 Объект защиты** – информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

**3.1.11 Оценка риска** – общий процесс анализа риска и оценка степени риска.

**3.1.12 Разграничение доступа** – порядок доступа лиц к техническим и программным средствам, защищаемой информации при ее обработке на средствах вычислительной техники (СВТ) в соответствии с заранее разработанными и утвержденными правилами.

**3.1.13 Риск информационной безопасности (риск ИБ)** – вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности активов Общества.

**3.1.14 Событие информационной безопасности (событие ИБ)** – идентифицированное возникновение состояния ИС, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, отказ средств защиты или ранее неизвестную ситуацию, которая может быть связана с безопасностью.

**3.1.15 Средства вычислительной техники (СВТ)** – совокупность программных и технических элементов ИС, обработки информации, в том числе ввода или вывода, способных функционировать самостоятельно или в составе других ИС.

**3.1.16 Система управления информационной безопасностью (СУИБ)** – часть общей системы управления Обществом, основанной на оценке бизнес-рисков и риск-ориентированном подходе, предназначенная для установления, внедрения, функционирования, мониторинга, анализа, сопровождения и постоянного улучшения обеспечения информационной безопасности.

**3.1.17 Угроза** – потенциальная причина инцидента, которая может нанести ущерб ИС или Обществу.

**3.1.18 Уязвимость** – слабость одного или нескольких активов Общества, которая может быть использована одной или несколькими угрозами.

**3.2** В настоящей Политике используются следующие сокращения:

**3.2.1 ИБ** – Информационная безопасность.

**3.2.2 ИС** – Информационная система.

**3.2.3 СВТ** – Средства вычислительной техники.

**3.2.4 СУИБ** – Система управления информационной безопасностью.



#### 4. Общие положения

4.1 Настоящая Политика направлена на развитие СУИБ Общества и его филиалов, достижение целей в области информационной безопасности, позволяющих надежно защитить информацию вне зависимости от формы, места и средств ее обработки и хранения, обеспечивая высокую эффективность деятельности Общества, в том числе:

4.1.1 обеспечение конфиденциальности, целостности и доступности информации и иных активов Общества;

4.1.2 соблюдение применимых требований законодательства Республики Казахстан, договорных обязательств и внутренних документов Общества в области информатизации/цифровизации, ИБ и защиты персональных данных;

4.1.3 обеспечение устойчивости и непрерывности основных бизнес-процессов, сервисов и информационных систем, функционирующих в Обществе.

4.1.4 обеспечение своевременного выявления, регистрации, расследования и реагирования на события и инциденты ИБ, а также постоянное улучшение СУИБ.

4.2 Руководство Общества осознает важность СУИБ и осуществляет управление информационной безопасностью, создавая необходимые условия развития, совершенствования мер и средств защиты информационных активов в контексте актуальных угроз информационной безопасности, изменения законодательства в данной сфере и рассматривает СУИБ как инструмент, направленный на обеспечение информационной безопасности и на сохранение конфиденциальности, целостности и доступности активов Общества.

4.3 Внедрение, функционирование и модернизация СУИБ Общества осуществляются на основе проводимого анализа рисков в соответствии с требованиями национальных стандартов по информационной безопасности.

4.4 Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Общества, защиты прав интеллектуальной собственности и персональной информации.

4.5 Политика разработана в соответствии с Уставом, внутренними документами Общества и Стратегией развития Общества, а также с учетом требований СТ РК ISO/IEC 27001, СТ РК ISO/IEC 27002 и применимых нормативных правовых актов Республики Казахстан в области информатизации/цифровизации, информационной безопасности и защиты персональных данных, а также с учетом лучших международных практик управления информационной безопасностью.

#### 5. Цели, задачи и основополагающие принципы обеспечения информационной безопасности

5.1 Основной целью ИБ является защита информации, связанной с деятельностью Общества, вне зависимости от формы, места и средств ее обработки и хранения, от возможного нанесения Обществу материального, физического, морального или иного ущерба.

5.2 Для достижения указанных целей Общество решает следующие задачи:

5.2.1 обеспечение лидерства и вовлеченности руководства в развитие и постоянное улучшение СУИБ;

5.2.2 определение контекста Общества, области действия СУИБ, применимых требований и ожиданий заинтересованных сторон;

5.2.3 внедрение и поддержание организационных и технических мер защиты, соразмерных уровню рисков и критичности активов;



5.2.4 повышение осведомленности, обучение и развитие культуры ИБ среди работников Общества;

5.2.5 четкое распределение ответственности и обязанностей работников по соблюдению и обеспечению ИБ;

5.2.6 своевременное выявление угроз ИБ, причин и условий, способствующих нанесению ущерба;

5.2.7 обеспечение безопасного управления изменениями, уязвимостями, обновлениями и конфигурациями информационных систем и сервисов Общества;

5.2.8 создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц;

5.2.9 разработка и внедрение правил и инструкций по обеспечению ИБ, контроль исполнения соответствующих требований всеми работниками Общества;

5.2.10 реализация нормативно-правовых, организационно-административных и материально-технических мер по обеспечению ИБ;

5.2.11 интеграция требований ИБ в проекты, закупки, разработку, внедрение и эксплуатацию информационных систем и сервисов;

5.2.12 эффективное реагирование Обществом на современные угрозы и риски в области ИБ;

5.2.13 вовлечение всего персонала в реализацию мероприятий по обеспечению ИБ;

5.2.14 реализация мероприятий по оценке и управлению информационными рисками;

5.2.15 обеспечение ИБ во взаимоотношениях с поставщиками, подрядчиками и иными третьими лицами, имеющими доступ к активам Общества;

5.2.16 обеспечение исполнения требований комплаенс и своевременного информирования заинтересованных сторон по вопросам, связанным с ИБ, в пределах установленной компетенции;

5.2.17 управление рисками в области ИБ на основе комплексного и процессного подходов для обеспечения непрерывности основных бизнес-процессов;

5.2.18 совершенствование СУИБ;

5.2.19 проведение внутреннего мониторинга, анализа эффективности мер защиты,

5.2.20 своевременное информирование заинтересованных сторон о деятельности Общества в области ИБ.

5.3 В целях практической реализации Политики Общество ежегодно утверждает и пересматривает измеримые цели в области ИБ.

5.4 Основными принципами обеспечения ИБ в Обществе являются:

5.4.1 соответствие действующей системы ИБ требованиям целей деятельности Общества, бизнес-процессам и уровню принимаемых рисков;

5.4.2 минимизация рисков и угроз в области ИБ Общества;

5.4.3 обеспечение конфиденциальности, санкционированной доступности и целостности информации Общества на протяжении всего её жизненного цикла;

5.4.4 соблюдение требований законодательства, нормативных правовых актов, договорных обязательств, корпоративных и национальных стандартов в области ИБ;

5.4.5 постоянное улучшение СУИБ на основе мониторинга, анализа, внутренних аудитов, результатов расследования инцидентов и пересмотра применяемых требований.

## **6. Объекты обеспечения информационной безопасности**

6.1 Основными объектами обеспечения ИБ в Обществе являются следующие элементы:



6.1.1 информационные активы, содержащие сведения ограниченного распространения и представленные в виде документов или записей на носителях на магнитной, оптической и другой основе, информационных физических полях, массивах и базах данных (далее – защищаемая информация);

6.1.2 программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационных систем, с помощью которых производится обработка информации;

6.1.3 автоматизированные ИС связи и передачи данных (средства телекоммуникаций);

6.1.4 каналы связи, по которым передается информация (в том числе ограниченного распространения);

6.1.5 помещения, предназначенные для ведения закрытых переговоров и совещаний;

6.1.6 помещения, в которых расположены средства обработки защищаемой информации;

6.1.7 технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

6.2 Подлежащая защите информация может:

6.2.1 находиться на бумажных носителях;

6.2.2 находиться в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);

6.2.3 передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

6.2.4 быть представлена в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;

6.2.5 записываться и воспроизводиться с помощью технических средств (диктофоны, видеоманитофоны и др.).

## **7. Разделение полномочий, ответственность и контроль**

7.1 Руководство Общества осуществляет общий контроль и несет персональную ответственность за выполнение целей и основных положений Политики, обеспечивает выделение необходимых ресурсов, демонстрирует лидерство и приверженность развитию СУИБ, утверждает цели в области ИБ, обеспечивает выполнение применимых требований и принимает решения по постоянному улучшению СУИБ.

7.2 Руководители структурных подразделений Общества, а также руководители организаций, СВТ которых подключены к автоматизированным и телекоммуникационным системам Общества:

7.2.1 обеспечивают ознакомление работников с внутренними документами Общества, содержащими требования к ИБ;

7.2.2 несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях.

7.3 Бизнес-владельцы ИС или подсистем:

7.3.1 определяют критичность активов, требования к защите информации и обеспечивают соблюдение требований ИБ при предоставлении и пересмотре прав доступа к ИС;

7.3.2 обеспечивают актуальность требований к резервному копированию, восстановлению, журналированию, мониторингу, обновлениям и иным мерам защиты, применимым к соответствующим ИС.



7.4 Администраторы ИС обеспечивают функционирование ИС в согласованных временных рамках, реализуют технические меры защиты, обеспечивают своевременное обновление и настройку средств защиты, ведение журналов событий, участие в реагировании на инциденты и выполнение требований Политики и иных внутренних документов Общества.

7.5 Работники структурных подразделений Общества:

7.5.1 соблюдают требования по ИБ, защите персональных данных и использованию информационных активов, принятые в Обществе;

7.5.2 контролируют исполнение требований к ИБ третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

7.5.3 незамедлительно извещают своего непосредственного руководителя и ответственных лиц по ИБ обо всех событиях, инцидентах, подозрительных действиях, уязвимостях и иных обстоятельствах, способных повлиять на безопасность активов Общества.

7.6 Решение вопросов стратегического планирования по ИБ, а также контроль нештатных ситуаций и инцидентов в области защиты ИС, осуществляет ответственный по ИБ совместно с Департаментом информационных технологий и Департаментом безопасности.

7.7 В рамках исполнения норм и правил настоящей Политики в Обществе проводится регулярный мониторинг и аудит ИБ. Аудит ИБ проводится подразделениями Общества при общем участии Департамента безопасности, с представлением отчетности руководству курирующих подразделений.

7.8 Независимый аудит ИБ может быть проведен по решению Правления Общества с привлечением независимой аудиторской компании.

7.9 Ответственный по ИБ, Департамент информационных технологий и Департамент безопасности выполняют мониторинг защищенности информационных активов, разрабатывают правила и инструкции, контролируют соблюдение требований ИБ всеми участниками информационного обмена. Расследование инцидентов осуществляет ответственный по ИБ совместно с Департаментом информационных технологий и Департаментом безопасности.

7.10 За несоблюдение порядка и правил использования информационных активов к виновным могут быть применены меры, предусмотренные трудовыми договорами, заключенными между Обществом и работником, а также действующим законодательством Республики Казахстан.

## **8. Соблюдение требований, управление рисками и постоянное улучшение**

8.1 Общество обеспечивает выявление, анализ и соблюдение применимых требований законодательства Республики Казахстан, нормативных правовых актов, национальных стандартов, договорных обязательств и внутренних документов в области информатизации/цифровизации, ИБ и защиты персональных данных.

8.2 Управление рисками ИБ осуществляется на регулярной основе и пересматривается при существенных изменениях в деятельности Общества, технологиях, архитектуре, составе активов, угрозах, уязвимостях и применимых требованиях.

8.3 Политика, цели в области ИБ, применимость мер контроля и иные документы СУИБ подлежат периодическому пересмотру не реже одного раза в 3 (три) года, а также при существенных изменениях законодательства, бизнес-процессов, технологической инфраструктуры, состава заинтересованных сторон, после существенных инцидентов ИБ и/или по итогам аудитов и анализа со стороны руководства.



8.4 Общество обеспечивает проведение внутреннего мониторинга и аудита, анализ результативности мер защиты, расследование инцидентов, корректирующие действия и реализацию мероприятий по постоянному улучшению СУИБ.

8.5 При обработке электронных информационных активов, содержащих персональные данные ограниченного доступа, Общество применяет меры защиты, предусмотренные законодательством Республики Казахстан и внутренними нормативными документами, включая разграничение доступа, журналирование, использование защищенных каналов передачи данных и многофакторную аутентификацию в предусмотренных случаях.

## **9. Порядок введения в действие**

9.1 Настоящая Политика вступает в силу с даты ее утверждения решением Правления Общества и подлежит доведению до сведения работников Общества и иных лиц, на которых распространяется ее действие.

9.2 Анализ Политики проводится раз в 3 года.

9.3 Политика подлежит актуализации при необходимости, а также в случаях изменения законодательства Республики Казахстан, применимых стандартов, бизнес-процессов, существенных изменениях в оценке рисков ИБ, возникновении существенных инцидентов ИБ, появлении новых угроз, изменении организационной или технологической инфраструктуры Общества, по результатам пересмотра СУИБ или по итогам аудитов и анализа со стороны руководства.

9.4 Актуализированная Политика вводится в действие решением Правления Общества.

**«Волковгеология»**  
акционерлік қоғамы



Акционерное общество  
**«Волковгеология»**

Бекітілген  
Басқармасының шешімімен  
«Волковгеология» АҚ  
2026 жылғы «14»  
(№ 22-07/12529 хаттама)



**САЯСАТ**  
**АҚПАРАТТЫҚ ҚАУІПСІЗДІК**  
**«ВОЛКОВГЕОЛОГИЯ» АҚ**

Алматы қ., 2026 ж.



## Мазмұны

|                                                                                                    |   |
|----------------------------------------------------------------------------------------------------|---|
| 1. Қолданылу саласы.....                                                                           | 3 |
| 2. Нормативтік сілтемелер.....                                                                     | 3 |
| 3. Терминдер, анықтамалар және қысқартулар.....                                                    | 3 |
| 4. Жалпы ережелер.....                                                                             | 4 |
| 5. Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары, міндеттері және негізгі қағидаттары..... | 5 |
| 6. Ақпараттық қауіпсіздікті қамтамасыз ету объектілері.....                                        | 6 |
| 7. Өкілеттіктерді бөлу, жауапкершілік және бақылау.....                                            | 7 |
| 8. Талаптарды сақтау, тәуекелдерді басқару және тұрақты жетілдіру.....                             | 8 |
| 9. Қолданысқа енгізу тәртібі.....                                                                  | 9 |



## 1. Қолданылу саласы

1.1 «Волковгеология» АҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «Волковгеология» АҚ-ның (бұдан әрі – Қоғам) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы Қоғам мен оның филиалдарының ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) мақсаттары мен қағидаттарын айқындайтын ішкі құжаты болып табылады.

1.2 Саясат Қоғамның ақпараттық қауіпсіздікті (бұдан әрі – АҚ) қамтамасыз ету саласындағы негізгі қағидаттарды, бағыттар мен талаптарды айқындайды, АҚ режимін қамтамасыз етудің негізі болып табылады және Қоғамның тиісті ішкі құжаттарын әзірлеу кезінде басшылыққа алынады.

1.3 Саясат Қоғам иесі және/немесе пайдаланушысы болып табылатын барлық ақпарат пен барлық ақпараттық жүйелерді қамтиды.

1.4 Саясаттың ережелері Қоғамның барлық қызметкерлеріне, сондай-ақ Қоғам активтеріне қол жеткізе алатын бөгде ұйымдардың қызметкерлеріне (мердігерлерге, консультанттарға) қолданылады.

## 2. Нормативтік сілтемелер

2.1 Осы Саясатты қолдану үшін мынадай нормативтік құжаттар қажет:

ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар».

ҚР СТ ISO/IEC 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары».

## 3. Терминдер, анықтамалар және қысқартулар

3.1 Осы Саясатта мынадай терминдер мен анықтамалар пайдаланылады:

3.1.1 Актив – ақпарат болып табылатын немесе ақпаратты қамтитын не оны өңдеу, сақтау немесе беру үшін пайдаланылатын және Қоғам үшін құндылығы бар материалдық немесе материалдық емес объект.

Ескертпе – Активтер деп Қоғамның барлық ақпараттық және телекоммуникациялық жүйелері, оның ішінде мобильді құрылғылар (Қоғамға тиесілі), желілер, ақпараттық жүйелер, серверлер, жұмыс станциялары (дербес компьютерлер), дерекқорларды басқару жүйелері және т.б. түсініледі. Бұл ретте Қоғамның меншігіндегі емес, бірақ сервистік шарттар және т.б. шеңберінде Қоғам пайдаланатын активтер де қарастырылады.

3.1.2 Тәуекелді талдау – тәуекел көздерін сәйкестендіру және тәуекел дәрежесін бағалау үшін ақпаратты жүйелі пайдалану.

3.1.3 Мүдделі тараптар – ақпараттық қауіпсіздік саласындағы талаптары мен күтулері Қоғам қызметі үшін маңызды болып табылатын жеке және заңды тұлғалар, мемлекеттік органдар, әріптестер, клиенттер, жеткізушілер және өзге де субъектілер.

3.1.4 Ақпараттық қауіпсіздік (АҚ) – ақпаратты жинау, өңдеу және сақтау процесінде оның құпиялылығын, тұтастығын және санкцияланған қолжетімділігін қамтамасыз етуге бағытталған әкімшілік-құқықтық, ұйымдастырушылық-өкімдік және техникалық шаралар кешені.

3.1.5 Ақпараттық жүйе (АЖ) – ақпаратты жинауды, сақтауды, өңдеуді және таратуды қамтамасыз ететін технологиялық тізбекке біріктірілген әдістердің, процестердің және бағдарламалық-техникалық құралдардың жиынтығы.

3.1.6 Таратылуы шектелген ақпарат – құжаттарда, істерде және басылымдарда, электрондық және өзге де тасымалдағыштарда тіркелген, «Қызмет бабында пайдалану



үшін» (бұдан әрі – ҚБПУ) және/немесе «Құпия», «Коммерциялық құпия» белгілері бар, таратылуын шектеу қызметтік қажеттіліктен туындайтын мәліметтерге жататын ақпарат.

3.1.7 Ақпараттық қауіпсіздік инциденті (АҚ инциденті) – АЖ-дағы бұзушылықтар, іркілістер, ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қауіп төндіретін және/немесе Қоғамның электрондық ақпараттық активтерін заңсыз алуға, көшіруге, таратуға, түрлендіруге, жоюға немесе бұғаттауға жағдай жасайтын іркілістер.

3.1.8 Бақылау шарасы – тәуекелдерді басқару құралдары, оның ішінде әкімшілік, техникалық, басқарушылық немесе заңдық сипатта болуы мүмкін саясаттар, рәсімдер, нұсқаулықтар, қағидалар немесе ұйымдық құрылымдар.

3.1.9 Объект – автоматтандырылған жүйе активінің пассивті компоненті, бірлігі (құрылғы, диск, каталог, файл және т.б.).

3.1.10 Қорғау объектісі – ақпаратты қорғаудың қойылған мақсатына сәйкес қорғауды қамтамасыз ету қажет ақпарат немесе ақпарат тасымалдағыш не ақпараттық процесс.

3.1.11 Тәуекелді бағалау – тәуекелді талдау мен тәуекел дәрежесін бағалаудың жалпы процесі.

3.1.12 Қолжетімділікті ажырату – алдын ала әзірленген және бекітілген қағидаларға сәйкес есептеу техникасы құралдарында (ЕТҚ) қорғалатын ақпаратты өңдеу кезінде тұлғалардың техникалық және бағдарламалық құралдарға, қорғалатын ақпаратқа қол жеткізу тәртібі.

3.1.13 Ақпараттық қауіпсіздік тәуекелі (АҚ тәуекелі) – Қоғам активтерінің құпиялылығының бұзылуы, тұтастығының қасақана бұзылуы немесе қолжетімділігінің бұзылуы салдарынан залалдың туындау ықтималдығы.

3.1.14 Ақпараттық қауіпсіздік оқиғасы (АҚ оқиғасы) – ақпараттық қауіпсіздік саясатының ықтимал бұзылуын, қорғау құралдарының істен шығуын немесе қауіпсіздікпен байланысты болуы мүмкін бұрын белгісіз жағдайды көрсететін АЖ, сервис немесе желі жай-күйінің анықталған туындауы.

3.1.15 Есептеу техникасы құралдары (ЕТҚ) – дербес немесе басқа АЖ құрамында жұмыс істей алатын, ақпаратты өңдеуге, оның ішінде енгізуге немесе шығаруға арналған АЖ бағдарламалық және техникалық элементтерінің жиынтығы.

3.1.16 Ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ) – Қоғамды басқарудың бизнес-тәуекелдерді бағалауға және тәуекелге бағдарланған тәсілге негізделген, ақпараттық қауіпсіздікті әзірлеуге, енгізуге, оның жұмыс істеуін қамтамасыз етуге, мониторингтеуге, талдауға, сүйемелдеуге және тұрақты жетілдіруге арналған жалпы жүйесінің бір бөлігі.

3.1.17 Қауіп – АЖ-ға немесе Қоғамға залал келтіруі мүмкін инциденттің ықтимал себебі.

3.1.18 Осалдық – бір немесе бірнеше қауіп пайдалануы мүмкін Қоғамның бір немесе бірнеше активінің әлсіз тұсы.

3.2 Осы Саясатта мынадай қысқартулар пайдаланылады:

3.2.1 АҚ – Ақпараттық қауіпсіздік.

3.2.2 АЖ – Ақпараттық жүйе.

3.2.3 ЕТҚ – Есептеу техникасы құралдары.

3.2.4 АҚБЖ – Ақпараттық қауіпсіздікті басқару жүйесі.

#### 4. Жалпы ережелер



4.1 Осы Саясат Қоғам мен оның филиалдарының АҚБЖ-сын дамытуға, ақпараттың нысанына, оны өңдеу мен сақтау орнына және құралдарына қарамастан оны сенімді қорғауға мүмкіндік беретін, Қоғам қызметінің жоғары тиімділігін қамтамасыз ететін ақпараттық қауіпсіздік саласындағы мақсаттарға қол жеткізуге бағытталған, оның ішінде:

4.1.1 Қоғам ақпараты мен өзге де активтерінің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету;

4.1.2 Қазақстан Республикасы заңнамасының қолданылатын талаптарын, шарттық міндеттемелерді және Қоғамның ақпараттандыру/цифрландыру, АҚ және дербес деректерді қорғау саласындағы ішкі құжаттарын сақтау;

4.1.3 Қоғамда жұмыс істейтін негізгі бизнес-процестердің, сервистердің және ақпараттық жүйелердің орнықтылығы мен үздіксіздігін қамтамасыз ету.

4.1.4 АҚ оқиғалары мен инциденттерін уақтылы анықтауды, тіркеуді, тергеп-тексеруді және оларға ден қоюды, сондай-ақ АҚБЖ-ны тұрақты жетілдіруді қамтамасыз ету.

4.2 Қоғам басшылығы АҚБЖ-ның маңыздылығын түсінеді және ақпараттық қауіпсіздіктің өзекті қауіптері, осы саладағы заңнаманың өзгеруі контекстінде ақпараттық активтерді қорғау шаралары мен құралдарын дамытуға және жетілдіруге қажетті жағдайлар жасай отырып, ақпараттық қауіпсіздікті басқаруды жүзеге асырады және АҚБЖ-ны ақпараттық қауіпсіздікті қамтамасыз етуге әрі Қоғам активтерінің құпиялылығын, тұтастығын және қолжетімділігін сақтауға бағытталған құрал ретінде қарастырады.

4.3 Қоғамның АҚБЖ-сын енгізу, оның жұмыс істеуі және жаңғыртылуы ақпараттық қауіпсіздік жөніндегі ұлттық стандарттардың талаптарына сәйкес жүргізілетін тәуекелдерді талдау негізінде жүзеге асырылады.

4.4 Ақпараттық қауіпсіздікті қамтамасыз ету – Қоғам қызметін табысты жүзеге асырудың, зияткерлік меншік құқықтары мен дербес ақпаратты қорғаудың қажетті шарты.

4.5 Саясат Қоғамның Жарғысына, ішкі құжаттарына және Даму стратегиясына сәйкес, сондай-ақ ҚР СТ ISO/IEC 27001, ҚР СТ ISO/IEC 27002 талаптарын және Қазақстан Республикасының ақпараттандыру/цифрландыру, ақпараттық қауіпсіздік және дербес деректерді қорғау саласындағы қолданылатын нормативтік құқықтық актілерін, сондай-ақ ақпараттық қауіпсіздікті басқарудың үздік халықаралық практикаларын ескере отырып әзірленді.

## **5. Ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары, міндеттері және негізгі қағидаттары**

5.1 АҚ-ның негізгі мақсаты – Қоғамның қызметіне байланысты ақпаратты оның нысанына, өңдеу және сақтау орны мен құралдарына қарамастан, Қоғамға материалдық, физикалық, моральдық немесе өзге де залал келтіру ықтималдығынан қорғау.

5.2 Көрсетілген мақсаттарға қол жеткізу үшін Қоғам мынадай міндеттерді шешеді:

5.2.1 басшылықтың көшбасшылығын және АҚБЖ-ны дамыту мен тұрақты жетілдіруге қатысуын қамтамасыз ету;

5.2.2 Қоғамның контекстін, АҚБЖ-ның қолданылу аясын, қолданылатын талаптар мен мүдделі тараптардың күтулерін айқындау;

5.2.3 тәуекелдер деңгейі мен активтердің сындарлылық деңгейіне сәйкес келетін ұйымдастырушылық және техникалық қорғау шараларын енгізу және қолдау;

5.2.4 Қоғам қызметкерлерінің АҚ саласындағы хабардарлығын арттыру, оларды оқыту және АҚ мәдениетін дамыту;



5.2.5 АҚ талаптарын сақтау және қамтамасыз ету бойынша қызметкерлердің жауапкершілігі мен міндеттерін нақты бөлу;

5.2.6 АҚ қауіптерін, залал келтіруге ықпал ететін себептер мен жағдайларды уақтылы анықтау;

5.2.7 Қоғамның ақпараттық жүйелері мен сервистеріндегі өзгерістерді, осалдықтарды, жаңартуларды және конфигурацияларды қауіпсіз басқаруды қамтамасыз ету;

5.2.8 жеке және заңды тұлғалардың заңсыз әрекеттерінен келтірілетін залалды барынша азайту және оқшаулау үшін жағдайлар жасау;

5.2.9 АҚ қамтамасыз ету жөніндегі қағидалар мен нұсқаулықтарды әзірлеу және енгізу, Қоғамның барлық қызметкерлерінің тиісті талаптарды орындауын бақылау;

5.2.10 АҚ қамтамасыз ету жөніндегі нормативтік-құқықтық, ұйымдастырушылық-әкімшілік және материалдық-техникалық шараларды іске асыру;

5.2.11 АҚ талаптарын жобаларға, сатып алуға, ақпараттық жүйелер мен сервистерді әзірлеуге, енгізуге және пайдалануға интеграциялау;

5.2.12 Қоғамның АҚ саласындағы қазіргі заманғы қауіптер мен тәуекелдерге тиімді ден қоюы;

5.2.13 АҚ қамтамасыз ету жөніндегі іс-шараларды іске асыруға барлық персоналды тарту;

5.2.14 ақпараттық тәуекелдерді бағалау және басқару жөніндегі іс-шараларды іске асыру;

5.2.15 Қоғам активтеріне қол жеткізе алатын жеткізушілермен, мердігерлермен және өзге де үшінші тұлғалармен өзара қатынастарда АҚ-ны қамтамасыз ету;

5.2.16 белгіленген құзырет шегінде комплаенс талаптарының орындалуын және АҚ-ға байланысты мәселелер бойынша мүдделі тараптарды уақтылы хабардар етуді қамтамасыз ету;

5.2.17 негізгі бизнес-процестердің үздіксіздігін қамтамасыз ету үшін кешенді және процестік тәсілдер негізінде АҚ саласындағы тәуекелдерді басқару;

5.2.18 АҚБЖ-ны жетілдіру;

5.2.19 ішкі мониторинг жүргізу, қорғау шараларының тиімділігін талдау,

5.2.20 мүдделі тараптарды Қоғамның АҚ саласындағы қызметі туралы уақтылы хабардар ету.

5.3 Саясатты іс жүзінде іске асыру мақсатында Қоғам жыл сайын АҚ саласындағы өлшенетін мақсаттарды бекітеді және қайта қарайды.

5.4 Қоғамдағы АҚ қамтамасыз етудің негізгі қағидаттары:

5.4.1 қолданыстағы АҚ жүйесінің Қоғам қызметінің мақсаттарына, бизнес-процестеріне және қабылданатын тәуекелдер деңгейіне сәйкестігі;

5.4.2 Қоғамның АҚ саласындағы тәуекелдері мен қауіптерін барынша азайту;

5.4.3 Қоғам ақпаратының бүкіл өмірлік циклі бойы құпиялылығын, санкцияланған қолжетімділігін және тұтастығын қамтамасыз ету;

5.4.4 заңнама талаптарын, нормативтік құқықтық актілерді, шарттық міндеттемелерді, АҚ саласындағы корпоративтік және ұлттық стандарттарды сақтау;

5.4.5 мониторинг, талдау, ішкі аудиттер, инциденттерді тергеп-тексеру нәтижелері және қолданылатын талаптарды қайта қарау негізінде АҚБЖ-ны тұрақты жетілдіру.

## **6. Ақпараттық қауіпсіздікті қамтамасыз ету объектілері**

6.1 Қоғамдағы АҚ қамтамасыз етудің негізгі объектілері мынадай элементтер болып табылады:



6.1.1 таратылуы шектелген мәліметтерді қамтитын және магниттік, оптикалық және өзге де негіздегі тасымалдағыштардағы құжаттар немесе жазбалар, ақпараттық физикалық өрістер, массивтер мен дерекқорлар түрінде ұсынылған ақпараттық активтер (бұдан әрі – қорғалатын ақпарат);

6.1.2 ақпарат өңделетін ақпараттық жүйелердің бағдарламалық құралдары (операциялық жүйелер, дерекқорларды басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз ету);

6.1.3 автоматтандырылған байланыс және деректерді беру АЖ (телекоммуникация құралдары);

6.1.4 ақпарат (оның ішінде таратылуы шектелген ақпарат) берілетін байланыс арналары;

6.1.5 жабық келіссөздер мен кеңестер өткізуге арналған үй-жайлар;

6.1.6 қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

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

6.2 Қорғалуға жататын ақпарат:

6.2.1 қағаз тасымалдағыштарда болуы;

6.2.2 электрондық түрде болуы (есептеу техникасы құралдарымен өңделуі, берілуі және сақталуы);

6.2.3 телефон, телефакс, телекс және т.б. арқылы электр сигналдары түрінде берілуі;

6.2.4 кеңестер мен келіссөздер кезінде ауа ортасында және қоршау конструкцияларында акустикалық және діріл сигналдары түрінде ұсынылуы;

6.2.5 техникалық құралдардың (диктофондар, бейнемагнитофондар және т.б.) көмегімен жазылуы және ойнатылуы мүмкін.

## 7. Өкілеттіктерді бөлу, жауапкершілік және бақылау

7.1 Қоғам басшылығы Саясаттың мақсаттары мен негізгі ережелерінің орындалуына жалпы бақылауды жүзеге асырады және дербес жауапты болады, қажетті ресурстардың бөлінуін қамтамасыз етеді, АҚБЖ-ны дамытуға көшбасшылық пен бейілділікті көрсетеді, АҚ саласындағы мақсаттарды бекітеді, қолданылатын талаптардың орындалуын қамтамасыз етеді және АҚБЖ-ны тұрақты жетілдіру бойынша шешімдер қабылдайды.

7.2 Қоғамның құрылымдық бөлімшелерінің басшылары, сондай-ақ ЕТҚ-сы Қоғамның автоматтандырылған және телекоммуникациялық жүйелеріне қосылған ұйымдардың басшылары:

7.2.1 қызметкерлердің АҚ талаптарын қамтитын Қоғамның ішкі құжаттарымен танысуын қамтамасыз етеді;

7.2.2 өздері басқаратын бөлімшелерде АҚ-ны қамтамасыз ету үшін дербес жауапты болады.

7.3 АЖ-ның немесе кіші жүйелердің бизнес-иелері:

7.3.1 активтердің сындарлылығын, ақпаратты қорғауға қойылатын талаптарды айқындайды және АЖ-ға қол жеткізу құқықтарын беру және қайта қарау кезінде АҚ талаптарының сақталуын қамтамасыз етеді;

7.3.2 резервтік көшіруге, қалпына келтіруге, журналдауға, мониторингке, жаңартуларға және тиісті АЖ-ға қолданылатын өзге де қорғау шараларына қойылатын талаптардың өзектілігін қамтамасыз етеді.

7.4 АЖ әкімшілері АЖ-ның келісілген уақыт шеңберінде жұмыс істеуін қамтамасыз етеді, техникалық қорғау шараларын іске асырады, қорғау құралдарының



уақтылы жаңартылуы мен бапталуын, оқиғалар журналдарының жүргізілуін, инциденттерге ден қоюға қатысуды және Саясат пен Қоғамның өзге де ішкі құжаттары талаптарының орындалуын қамтамасыз етеді.

7.5 Қоғамның құрылымдық бөлімшелерінің қызметкерлері:

7.5.1 Қоғамда қабылданған АҚ, дербес деректерді қорғау және ақпараттық активтерді пайдалану жөніндегі талаптарды сақтайды;

7.5.2 өздерінің функционалдық міндеттері шеңберінде өзара іс-қимыл жасайтын үшінші тұлғалардың АҚ талаптарын орындауын, оның ішінде көрсетілген талаптарды үшінші тұлғалармен жасалатын шарттарға енгізу арқылы бақылайды;

7.5.3 Қоғам активтерінің қауіпсіздігіне әсер етуі мүмкін барлық оқиғалар, инциденттер, күдікті әрекеттер, осалдықтар және өзге де мән-жайлар туралы өзінің тікелей басшысын және АҚ бойынша жауапты тұлғаларды дереу хабардар етеді.

7.6 АҚ бойынша стратегиялық жоспарлау мәселелерін шешуді, сондай-ақ АЖ-ны қорғау саласындағы штаттан тыс жағдайлар мен инциденттерді бақылауды АҚ бойынша жауапты тұлға Ақпараттық технологиялар департаментімен және Қауіпсіздік департаментімен бірлесіп жүзеге асырады.

7.7 Осы Саясаттың нормалары мен қағидаларын орындау шеңберінде Қоғамда АҚ-ға тұрақты мониторинг және аудит жүргізіледі. АҚ аудитін Қоғамның бөлімшелері Қауіпсіздік департаментінің жалпы қатысуымен, кураторлық ететін бөлімшелер басшылығына есептілік ұсына отырып жүргізеді.

7.8 АҚ-ның тәуелсіз аудиті Қоғам Басқармасының шешімі бойынша тәуелсіз аудиторлық компанияны тарта отырып жүргізілуі мүмкін.

7.9 АҚ бойынша жауапты тұлға, Ақпараттық технологиялар департаменті және Қауіпсіздік департаменті ақпараттық активтердің қорғалуына мониторинг жүргізеді, қағидалар мен нұсқаулықтар әзірлейді, ақпарат алмасудың барлық қатысушыларының АҚ талаптарын сақтауын бақылайды. Инциденттерді тергеп-тексеруді АҚ бойынша жауапты тұлға Ақпараттық технологиялар департаментімен және Қауіпсіздік департаментімен бірлесіп жүзеге асырады.

7.10 Ақпараттық активтерді пайдалану тәртібі мен қағидаларын сақтамағаны үшін кінәлі тұлғаларға Қоғам мен қызметкер арасында жасалған еңбек шарттарында, сондай-ақ Қазақстан Республикасының қолданыстағы заңнамасында көзделген шаралар қолданылуы мүмкін.

## **8. Талаптарды сақтау, тәуекелдерді басқару және тұрақты жетілдіру**

8.1 Қоғам Қазақстан Республикасы заңнамасының, нормативтік құқықтық актілердің, ұлттық стандарттардың, шарттық міндеттемелердің және ақпараттандыру/цифрландыру, АҚ және дербес деректерді қорғау саласындағы ішкі құжаттардың қолданылатын талаптарын анықтауды, талдауды және сақтауды қамтамасыз етеді.

8.2 АҚ тәуекелдерін басқару тұрақты негізде жүзеге асырылады және Қоғам қызметінде, технологияларда, архитектурада, активтер құрамында, қауіптерде, осалдықтарда және қолданылатын талаптарда елеулі өзгерістер болған кезде қайта қаралады.

8.3 Саясат, АҚ саласындағы мақсаттар, бақылау шараларының қолданылуы және АҚБЖ-ның өзге де құжаттары кемінде 3 (үш) жылда бір рет, сондай-ақ заңнамада, бизнес-процестерде, технологиялық инфрақұрылымда, мүдделі тараптар құрамында елеулі өзгерістер болғанда, АҚ-ның елеулі инциденттерінен кейін және/немесе аудиттер мен басшылық тарапынан талдау қорытындылары бойынша мерзімді қайта қаралуға жатады.



8.4 Қоғам ішкі мониторинг пен аудит жүргізуді, қорғау шараларының нәтижелілігін талдауды, инциденттерді тергеп-тексеруді, түзету әрекеттерін және АҚБЖ-ны тұрақты жетілдіру жөніндегі іс-шараларды іске асыруды қамтамасыз етеді.

8.5 Қолжетімділігі шектелген дербес деректерді қамтитын электрондық ақпараттық активтерді өңдеу кезінде Қоғам Қазақстан Республикасының заңнамасында және ішкі нормативтік құжаттарда көзделген қорғау шараларын, оның ішінде қолжетімділікті ажыратуды, журналдауды, қорғалған деректерді беру арналарын пайдалануды және көзделген жағдайларда көп факторлы аутентификацияны қолданады.

## 9. Қолданысқа енгізу тәртібі

9.1 Осы Саясат Қоғам Басқармасының шешімімен бекітілген күннен бастап күшіне енеді және Қоғам қызметкерлерінің және оның қолданылуы оларға таралатын өзге де тұлғалардың назарына жеткізілуге тиіс.

9.2 Саясатқа талдау 3 жылда бір рет жүргізіледі.

9.3 Саясат қажеттілігіне қарай, сондай-ақ Қазақстан Республикасының заңнамасы, қолданылатын стандарттар, бизнес-процестер өзгерген, АҚ тәуекелдерін бағалауда елеулі өзгерістер болған, АҚ-ның елеулі инциденттері туындаған, жаңа қауіптер пайда болған, Қоғамның ұйымдық немесе технологиялық инфрақұрылымы өзгерген жағдайларда, АҚБЖ-ны қайта қарау нәтижелері бойынша немесе аудиттер мен басшылық тарапынан талдау қорытындылары бойынша өзектендірілуге жатады.

9.4 Өзектендірілген Саясат Қоғам Басқармасының шешімімен қолданысқа енгізіледі.