Приложение 1
к И-137

«ӨСК «NOMAD LIFE» АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ	ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «КСЖ «NOMAD LIFE»
МАЗМҰНЫ	**СОДЕРЖАНИЕ**
1. ЖАЛПЫ ЕРЕЖЕЛЕР	**1. ОБЩИЕ ПОЛОЖЕНИЯ**
1.1. «ӨСК «Nomad Life» АҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) – құжатталған басқарушылық шешімдер жиынтығы, ол ақпараттық жүйеде, соның ішінде қағаз және электрондық құжат айналымында, сондай-ақ құпия ақпараттың ауызша алмасуында ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған. «ӨСК «Nomad Life» АҚ (бұдан әрі – Компания) Ақпараттық қауіпсіздік саясаты негізгі құжат – «Ақпараттық қауіпсіздік саясаты» және ақпараттық қауіпсіздікті қамтамасыз ету, лауазымды тұлғалар мен ақпараттық жүйе пайдаланушыларының қызметін реттейтін құжаттардан тұратын құжаттар пакетін білдіреді. 1.2. **Саясаттың мақсаты** – ақпараттың тиісті қорғалуын қамтамасыз етуге, Компанияның ақпараттық жүйесінің үздіксіз жұмысын қолдауға, сондай-ақ ақпараттық қауіпсіздік қатерлеріне қарсы тиімді алдын алу және қалпына келтіру шараларын әзірлеу арқылы ықтимал залалды барынша азайтуға қабілетті бірыңғай талаптар мен ережелерді әзірлеу және бекіту. 1.3. Ақпараттық қауіпсіздік бөлімшесі (бұдан әрі – АҚБ) саясаттың иесі болып табылады.	1.1. Политика информационной безопасности АО «КСЖ «Nomad Life» (далее – Политика) – совокупность внутренних документов, включающих в себя Политику и иные внутренние документы, определяющие необходимые критерии, параметры, подходы, принципы, стандарты, процедуры и механизмы, обеспечивающие эффективное функционирование Компании и соответствие ее деятельности стратегии и допустимому уровню риска. 1.2. **Цель Политики** – выработать и утвердить единые требования и правила, способные обеспечить надлежащую защиту информации и бесперебойную работу информационной системы Компании и свести к минимуму возможный ущерб от их эксплуатации посредством разработки эффективных превентивных и восстановительных мер противодействия угрозам информационной безопасности. 1.3. Владельцем Политики является подразделение информационной безопасности (далее – ОИБ).
2. ҚОЛДАНЫЛУ САЛАСЫ	**2. ОБЛАСТЬ ПРИМЕНЕНИЯ**
2.1. Бұл Саясат Компанияның барлық бөлімшелеріне, қызметкерлеріне, мердігерлеріне, сондай-ақ барлық пайдаланылатын ақпараттық инфрақұрылымға, соның ішінде серверлерге, дерекқорларға, желілерге және мобильді құрылғыларға қолданылады.	2.1. Политика распространяется на все подразделения Компании, работников, подрядчиков, а также на всю используемую информационную инфраструктуру, включая серверы, базы данных, сети и мобильные устройства.
3. НОРМАТИВТІК СІЛТЕМЕЛЕР	**3. НОРМАТИВНЫЕ ССЫЛКИ**
3.1. Осы құжат келесі нормативтік құқықтық актілердің талаптарына сәйкес әзірленді: 1) Қазақстан Республикасының «Информатизация туралы» заңы – ақпаратты қорғау және оны басқару мәселелерін реттейді; 2) Қазақстан Республикасының «Жеке деректер және оларды қорғау туралы» заңы – жеке деректерді өңдеу, сақтау және қорғау талаптарын анықтайды; 3) Қазақстан Республикасының «Тұтынушылардың құқықтарын қорғау туралы» заңы – клиенттердің деректерін қорғау мәселелерін реттейді; 4) ҚР Үкіметінің 2018 жылғы 20 маусымдағы №164 қаулысымен бекітілген Ақпараттық қауіпсіздікті қамтамасыз ету ережелері; 5) ҚР Қаржы нарығын реттеу және дамыту агенттігі басқармасының 2020 жылғы 23 қарашадағы №110 қаулысымен бекітілген ақпараттық қауіпсіздік	3.1 Политика разработана в соответствии с требованиями следующих нормативно правовых актов: 1) Закон Республики Казахстан «Об информатизации» – регулирует вопросы обеспечения и защиты информации, а также управление информационными ресурсами; 2) Закон Республики Казахстан «О персональных данных и их защите» – определяет требования к обработке, хранению и защите персональных данных; 3) Закон Республики Казахстан «О защите прав потребителей» – регулирует вопросы защиты данных клиентов, включая их безопасность в цифровой среде; 4) Правила обеспечения информационной безопасности, утверждённые Постановлением Правительства Республики Казахстан № 164 от 20 июня 2018 года; 5) Правила оценки уровня защищённости от угроз информационной безопасности, утверждённые

қатерлерінен қорғаныс деңгейін бағалау ережелері; 6) СТ РК ISO/IEC 27001-2019 «Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздік менеджменті жүйелері – Талаптар»; 7) СТ РК ISO/IEC 27002-2022 «Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздікті басқару бойынша тәжірибелік нұсқаулықтар»; 8) Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 тамыздағы № 198 "Қазақстан Республикасының резиденті емес сақтандыру (қайта сақтандыру) ұйымдары, сақтандыру (қайта сақтандыру) ұйымдары филиалдары үшін тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларын бекіту туралы" Қаулысы. 9) «Құжатталған ақпаратты басқару» құжатталған процедурасы.	Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года №110; 6) СТ РК ISO/IEC 27001-2019 «Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Требования»; 7) СТ РК ISO/IEC 27002-2022 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью»; 8) Постановление Правления Национального Банка Республики Казахстан от 27 августа 2018 года № 198. «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для страховых (перестраховочных) организаций, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан»; 9) Документированная процедура «Управление документированной информацией».
4. ТЕРМИНДЕР, АНЫҚТАМАЛАР ЖӘНЕ ҚЫСҚАРТУЛАР	**4. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ**
4.1. Осы Саясатта келесі терминдер қолданылады: 1) **қолжетімділік** – ақпараттың уәкілетті тұлғалар үшін қажетті уақытта қолжетімділігін қамтамасыз ету; 2) **нұсқаулық** – ақпараттық қауіпсіздік талаптарын, ережелерін және шараларын қызметкерлерге түсіндіру процесі; 3) **ақпараттық қауіпсіздік (АҚ)** – ақпаратты және ақпараттық инфрақұрылымды рұқсатсыз қолжетімділіктен, жойылудан, өзгертілуден және басқа да қауіптерден қорғау; 4) **ақпараттық қауіпсіздік инциденті** – ақпараттың құпиялылығы, тұтастығы немесе қолжетімділігіне қауіп төндіретін немесе оны бұзатын оқиға; 5) **киберқауіп** – ақпараттық жүйелерге әсер ету арқылы олардың жұмысына нұқсан келтіру немесе рұқсатсыз қол жеткізу мақсатындағы ықтимал немесе нақты қауіп; 6) **құпиялылық** –; 7) **фаервол** (брандмауэр) – желілік трафикті белгіленген қауіпсіздік ережелеріне сәйкес бақылау және сүзгілеуге арналған бағдарламалық немесе аппараттық құрал; 8) **фишинг** – алаяқтық әдісі, онда шабуылдаушы сенімді дереккөз ретінде өзін таныстырып, құпия ақпаратты алуға тырысады; 9) **тұтастық** – ақпараттың сақтау, өңдеу және беру барысында өзгертілмеуі және бұзылмауы. 10) уәкілетті орган-Қазақстан Республикасының Қаржы нарығын реттеу және қадағалау жөніндегі агенттігі 4.2. Осы Саясатта қолданылатын қысқартулар:	4.1. В настоящей Политике используются следующие термины с соответствующими определениями: 1) **доступность** – обеспечение возможности использования информации уполномоченными лицами в нужный момент; 2) **инструктаж** – процесс разъяснения работникам требований, правил и мер по обеспечению информационной безопасности; 3) **информационная безопасность (ИБ)** – защита информации и информационной инфраструктуры от несанкционированного доступа, уничтожения, модификации и других угроз; 4) **инцидент информационной безопасности** – событие, которое нарушает или угрожает конфиденциальности, целостности или доступности информации; 5) **киберугроза** – потенциальная или реальная угроза, связанная с воздействием на информационные системы с целью нарушения их работы или получения несанкционированного доступа; 6) **конфиденциальность –** свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право. 7) **фанеровал** (межсетевой экран) – программное или аппаратное средство, предназначенное для контроля и фильтрации сетевого трафика в соответствии с заданными правилами безопасности; 8) **фишинг** – мошеннический метод получения конфиденциальной информации путём выдачи себя за доверенный источник; 9) **целостность** – сохранность и неизменность информации в процессе её хранения, обработки и передачи.

1) **CISO (Chief Information Security Officer)** – ақпараттық қауіпсіздікті басқаруға жауапты тұлға; 2) **IPS (Intrusion Prevention System)** – шабуылдарды болдырмау жүйесі; 3) **SIEM (Security Information and Event Management)** – ақпараттық қауіпсіздік оқиғаларын басқару жүйесі; 4) **VPN (Virtual Private Network)** – виртуалды жеке желі; 5) **ІНҚ** – ішкі нормативтік құжат; 6) **БСДБ – Бірыңғай сақтандыру деректер базасы;** 7) **АҚ** – ақпараттық қауіпсіздік; 8) **АЖ** – ақпараттық жүйе; 9) **АТ** – ақпараттық технологиялар; 10) **КИП** – Компанияның корпоративтік ақпараттық порталы; 11) **МФА** – көпфакторлы аутентификация (Multi-Factor Authentication); 12) **АҚБ** – ақпараттық қауіпсіздік бөлімшесі.	10) **уполномоченный орган** – Агентство Республики Казахстан по регулированию и надзору финансового рынка. 4.2. В настоящей Политике используются следующие сокращения: 1) **CISO (Chief Information Security Officer)** – ответственное лицо за управление информационной безопасностью; 2) **IPS** – система предотвращения вторжений (Intrusion Prevention System); 3) **SIEM** – система управления событиями информационной безопасности (Security Information and Event Management); 4) **VPN** – виртуальная частная сеть (Virtual Private Network); 5) **ВНД** – внутренний нормативный документ; 6) **ЕСБД** – Единая страховая база данных; 7) **ИБ** – информационная безопасность; 8) **ИС** – информационная система; 9) **ИТ** – информационные технологии; 10) **КИП** – корпоративный информационный портал Компании; 11) **МФА** – многофакторная аутентификация (Multi-Factor Authentication); 12) **ОИБ** – подразделение информационной безопасности.
5. АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ НЕГІЗГІ ПРИНЦИПТЕР	**5. ОСНОВНЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
5.1. **Құпиялылық:** ақпарат қауіпсіздігінің қасиеті, оған тек оған құқығы бар қол жеткізу субъектілері ғана қол жеткізеді, оған тек уәкілетті тұлғалардың қол жеткізуін қамтамасыз ететін ақпарат қасиеті. 5.2. **Тұтастық** – деректердің дұрыстығы мен толықтығын қамтамасыз ету. 5.3. **Қолжетімділік** – ақпарат қажет болған жағдайда қолжетімді болуы тиіс.	5.1. **Конфиденциальность**: свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право. 5.2. **Целостность**: обеспечение корректности, достоверности и полноты данных. 5.3. **Доступность:** информация должна быть доступна пользователям при необходимости.
6. ҰЙЫМДАСТЫРУ ЖӘНЕ ТЕХНИКАЛЫҚ ШАРАЛАРЫ	**6. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ**
6.1. Компанияның тиісті ақпараттық қауіпсіздігін қамтамасыз ету үшін АҚБ ұйымдастырушылық және техникалық шараларды қабылдайды. 6.2. Компанияның ішкі құжаттарының талаптарына сәйкес ақпараттық қауіпсіздікті басқаруға жауапты адамды (CISO) тағайындау. Компанияның ақпараттық қауіпсіздігін басқаруға жауапты тұлға (CISO) қауіпсіздік департаментінің директоры болып табылады. 6.3. Ұйымдастырушылық шараларға мыналар жатады: 1) ақпараттық қауіпсіздік стратегиясын әзірлеу, компанияда деректерді қорғау жөніндегі іс-шараларға тұрақты мониторинг жүргізу және үйлестіру; 2) уәкілетті органмен және сыртқы аудиторлармен өзара іс-қимылды қамтамасыз ету 3) ішкі нормативтік құжаттарды өзекті жағдайда әзірлеу және қолдау: қауіпсіздікті қамтамасыз ету жөніндегі регламенттер, нұсқаулықтар мен рәсімдер, құпия сөздерді пайдалану жөніндегі ЖҰӨ, құпия	6.1. Для обеспечения надлежащей информационной безопасности Компании ОИБ принимает организационные и технические меры. 6.2. Назначение ответственного лица за управление информационной безопасностью (CISO), в соответствии с требованиями внутренних документов Компании. Лицом, ответственным за управление информационной безопасностью Компании (CISO) является Директор Департамента безопасности. 6.3. Организационные меры включают: 1) разработка стратегии Информационной безопасности, проведение регулярного мониторинга и координации мероприятий по защите данных в Компании; 2) обеспечение взаимодействия с уполномоченным органом и внешними аудиторами 3) разработку и поддержание внутренних нормативных документов в актуальном состоянии:

ақпаратқа қол жеткізуді басқару және онымен жұмыс істеу; 1) басшылық құрамды қоса алғанда, барлық қызметкерлер үшін ақ тақырыптары бойынша қызметкерлерді оқытуды, тұрақты тренингтерді, мерзімді таратуларды және киберқауіптер туралы хабардар болу тесттерін өткізу; 2) тұрақты ішкі аудиттерді ұйымдастыру және жүргізу процестер мен ақпараттық жүйелердегі осалдықтарды бағалауға бағалауға, қауіпсіздік нормалары мен стандарттарының сақталуын талдауға бағытталған тексерулер; 6.4. Техникалық шараларға мыналар жатады: 1) шифрлауды қолдану тыныштық жағдайында және беру кезінде деректерді қорғау, сертификатталған криптографиялық құралдарды пайдалану; 2) қол жеткізуді аутентификациялау және басқару, сыни жүйелер үшін көп факторлы аутентификацияны (МФА) енгізу, қол жеткізу құқықтарын тұрақты қайта қаралумен пайдаланушылардың есептік жазбаларын басқару; 3) желінің периметрін қорғау, брандмауэрлерді, кіруді болдырмау жүйелерін (IPS) орнату және конфигурациялау, қауіпсіз байланыс арналары бар VPN арқылы корпоративтік желіге кіруді шектеу; 4) қауіп-қатерлерге мониторинг және ден қою, қауіпсіздік оқиғаларын талдау үшін SIEM-жүйелерді пайдалану, хабарламаларды Автоматтандыру және инциденттерге ден қою;	регламенты, инструкции и процедуры по обеспечению безопасности, ВНД по использованию паролей, управления доступом и обращения с конфиденциальной информацией; 1) проведение обучения работников, регулярные тренинги для всех работников, включая руководящий состав, на темы ИБ, периодические рассылки и тесты на осведомлённость о киберугрозах; 2) организацию и проведение регулярных внутренних аудитов и проверок, направленных на оценку оценку уязвимостей в процессах и информационных системах, анализ соблюдения норм и стандартов безопасности; 6.4. Технические меры включают: 1) применение шифрования защита данных в состоянии покоя и при передаче, использование сертифицированных криптографических средств; 2) аутентификация и управление доступом, внедрение многофакторной аутентификации (МФА) для критических систем, управление учётными записями пользователей с регулярным пересмотром прав доступа; 3) защита периметра сети, установка и настройка файерволов, систем предотвращения вторжений (IPS), ограничение доступа к корпоративной сети через VPN с безопасными каналами связи; 4) мониторинг и реагирование на угрозы, использование SIEM-систем для анализа событий безопасности, автоматизация уведомлений и реагирования на инциденты;
7. ТӘУЕКЕЛДЕРДІ БАСҚАРУ	**7. УПРАВЛЕНИЕ РИСКАМИ**
7.1. Ақпараттық қауіпсіздік тәуекелдерін басқару мақсатында Компанияның Басқармасы бекіткен "NOMAD Life" ӨСК" АҚ-да ақпараттық қауіпсіздік тәуекелдерін басқару қағидаларында көзделген рәсімдер мен іс-шаралар жүзеге асырылады, олар мыналарды қамтиды: 7.2. Тәуекелдерді анықтау: 1) компанияның АҚ тәуекелдерін басқару жөніндегі ІНҚ сәйкес аса маңызды активтер үшін қауіптер мен осалдықтарды бағалауды тұрақты жүргізу; 2) оларды кейіннен мониторингілеу және басқару үшін сәйкестендірілген тәуекелдер тізілімін құру. 7.3. Талдау және бағалау: 1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ІНҚ талаптарына сәйкес, тәуекелдердің ықтималдығы мен салдарын бағалау; 2) тәуекелдердің маңыздылығына қарай басымдық беру. 7.4. Ақпараттық тәуекелдерді басқару және оларды азайту: 1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ІНҚ әзірлеу;	7.1. С целью управления рисками информационной безопасности осуществляются процедуры и мероприятия, предусмотренные Правилами управления рисками информационной безопасности в АО «КСЖ «Nomad Life», утверждёнными Правлением Компании, которые включают в том числе: 7.2. Идентификацию рисков: 1) регулярное проведение оценки угроз и уязвимостей для критически важных активов, согласно ВНД по управлению рисками ИБ Компании; 2) создание реестра идентифицированных рисков для их последующего мониторинга и управления. 7.3. Анализ и оценку: 1) оценка вероятности и последствий реализации рисков, согласно ВНД по управлению рисками ИБ Компании; 2) приоритизация рисков на основе их критичности. 7.4. Управление информационными рисками и их минимизация: 1) разработка ВНД по управлению рисками ИБ в Компании;

2) Компанияның резервтік көшіру жөніндегі ВНД талаптарына сәйкес, резервтік көшіруді және ақаусыз жүйелерді пайдалану. 7.5. Тұрақты жаңарту: 1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ІНҚ талаптарына сәйкес, бизнес-процестер, технологиялар немесе қауіптер өзгерген кезде тәуекелдерді қайта бағалау; 2) жоғары басшылыққа тұрақты есеп беру.	2) использование резервного копирования данных и отказоустойчивых систем, согласно требованиям ВНД и законодательства Республики Казахстан к резервному копированию данных Компании. 7.5. Постоянное обновление: 1) обновление оценки рисков при изменении бизнес-процессов, технологий или угроз, согласно требованию ВНД по управлению рисками ИБ в Компании; 2) предоставление регулярной отчётности высшему руководству.
8. ИНЦИДЕНТТЕРДІ БАСҚАРУ	**8. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ**
8.1. Ақпараттық қауіпсіздік инциденттеріне жауап беру жөніндегі ІНҚ әзірлеу және енгізу. 8.2. Компанияның ІНҚ талаптарына сәйкес, қауіп-қатерлерді үздіксіз мониторингтеу және анықтау. 8.3. Деректердің таралуы орын алған жағдайда, заңнамада белгіленген мерзімде уәкілетті органдарды хабардар ету.	8.1. Разработка и внедрение ВНД по управлению инцидентами ИБ. 8.2. Непрерывный мониторинг и выявление угроз, согласно требованиям ВНД Компании. 8.3. Своевременное уведомление уполномоченных органов в случае утечки данных в порядке и сроки, установленные законодательством Республики Казахстан.
9. ҚАШЫҚТАН ҚЫЗМЕТ КӨРСЕТУ	**9. ДИСТАНЦИОННОЕ ОКАЗАНИЕ УСЛУГ**
9.1. Қашықтан қызмет көрсету кезінде клиенттердің жеке деректерін және құпия ақпаратын қорғау қамтамасыз етіледі. 9.2. Қауіпсіз байланыс арналары мен қашықтан қолжетімділік үшін аутентификация механизмдері пайдаланылады. 9.3. Компанияның веб-ресурстарының қауіпсіздігі бақыланады. 9.4. Қашықтан қызмет көрсету жүйелерінің қорғалуын тексеру және аудит тұрақты түрде жүргізіледі. 9.5. Заңнама талаптарына сәйкес, деректердің берілуі және пайдаланушылардың қашықтан сервистерге қолжетімділігі бақыланады.	9.1. При оказании дистанционных услуг обеспечивается защита персональных данных и конфиденциальной информации клиентов. 9.2. Используются защищённые каналы связи и механизмы аутентификации для предоставления удалённого доступа к ИС и ресурсам Компании. 9.3. Проводится контроль за безопасностью веб-ресурсов Компании. 9.4. Регулярно проводится аудит и тестирование защищённости сервисов дистанционного обслуживания. 9.5. Контролируется передача данных и доступ пользователей к дистанционным сервисам согласно требованиям законодательства.
10. АҚБ-НІҢ ҚҰЗЫРЕТТІ ОРГАНДАРМЕН СӘЙКЕСТІГІН БАҚЫЛАУ ЖӘНЕ ӨЗАРА ІС-ҚИМЫЛ ТӘРТІБІ	**10. КОНТРОЛЬ СООТВЕТСТВИЯ И ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОИБ С КОМПЕТЕНТНЫМИ ОРГАНАМИ**
10.1. Ақпараттық қауіпсіздікке жауапты бөлімше ішкі нормативтік құжаттарға және Қазақстан Республикасының заңнамасына сәйкестікті тұрақты түрде тексеруді жүзеге асырады. 10.2. Жүргізілген тексерулердің нәтижелері бойынша, сондай-ақ талаптарды реттеуші белгілеген талаптар шеңберінде АҚБ-ның жауапты бөлімшесі есептілікті дайындауды және уәкілетті органға белгіленген мерзімдерде ұсынуды қамтамасыз етеді. 10.3. АҚБ жауапты тұлғасы ақпараттық қауіпсіздік мәселелері бойынша мынадай құзыретті органдармен тұрақты негізде өзара іс-қимылды жүзеге асырады: 1) Қаржы нарығын және қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті органмен (бұдан әрі – мәселелер жөніндегі уәкілетті орган:	10.1. ОИБ проводит регулярный внутренний контроль на соответствие требований внутренней нормативной документации Компании требованиям законодательства Республики Казахстан в части обеспечения информационной безопасности. Проверки направлены на выявление отклонений, устаревших норм и несоответствий фактических процессов установленным требованиям. 10.2. По результатам проведённых проверок, а также в рамках требований, установленных регулятором требований, ответственное подразделение ОИБ обеспечивает подготовку и представление отчётности в Уполномоченный орган в установленные сроки. 10.3. Ответственное лицо ОИБ на постоянной основе осуществляет взаимодействие со следующими компетентными органами по вопросам информационной безопасности:

а) АҚ қатерлері бойынша хабарламаларды АҚБ-нің жауапты тұлғасы электрондық мекенжайға хабарлама алу арқылы алу/жіберу;
б) үшінші тұлғалардың Қоғамның есептік жазбасына (криптографиялық кілттерге, электрондық цифрлық қолтаңба кілттеріне) рұқсатсыз қол жеткізу фактісін жою жөнінде қабылданған шаралар туралы ақпаратты уәкілетті органға БСДБ-ға рұқсатсыз қол жеткізу фактісі анықталған күннен бастап 2 (екі) жұмыс күнінен кешіктірілмейтін мерзімде жібергенде;
в) егер үшінші тұлғалардың есептік жазбаға рұқсатсыз қол жеткізу фактісін жою жөнінде шаралар қабылдаған жағдайда, жоспарланған іс - шараларды, олардың аяқталу мерзімдерін және жауапты тұлғаларды көрсете отырып, Қоғамның есептік жазбасына (криптографиялық кілттерге, электрондық цифрлық қолтаңба кілттеріне) үшінші тұлғалардың рұқсатсыз қол жеткізу фактісін жою жөніндегі іс-шаралар жоспарын (бұдан әрі-іс-шаралар жоспары) уәкілетті органға жіберу қоғамның (криптографиялық кілттерге, электрондық цифрлық қолтаңба кілттеріне) 2 (екі) жұмыс күнінен артық уақыт қажет;
г) Қоғамның қолданыстағы заңнамада көзделген АҚ талаптарын сақтау мәселелері бойынша есептілікті жіберу, сондай-ақ Уәкілетті органға соңғысының сұрау салулары негізінде жауаптар, ақпарат жіберу;
д) АҚ мәселелері бойынша заңнамалық актілердің жобаларын келісуге / талқылауға бірлесіп қатысу;
е) АҚ мәселелері бойынша қолданыстағы заңнаманың талаптарын түсіндіру жұмысы бойынша жұмыс топтарының отырыстарына бірлесіп қатысу;

2) **БСДБ өкілдерімен бірге келесі мәселелер бойынша:**
   а) БСДБ-ға рұқсатсыз кіруді анықтау туралы ақпаратты БСДБ-ға жіберу (ақпарат қағаз жеткізгіште және (немесе) электрондық тәсілмен табылған сәттен бастап 12 (он екі) сағат ішінде жіберіледі);
   б) үшінші тұлғалардың Қоғамның есептік жазбасына (криптографиялық кілттерге, электрондық цифрлық қолтаңба кілттеріне) рұқсатсыз қол жеткізу фактісін жою бойынша қабылданған шаралар туралы ақпаратты БСДБ-ға рұқсатсыз қол жеткізу фактісі анықталған күннен бастап 2 (екі) жұмыс күнінен кешіктірілмейтін мерзімде БСДБ-ға жіберу;
   в) егер үшінші тұлғалардың есептік жазбаға рұқсатсыз қол жеткізу фактісін жою жөнінде шаралар қабылдаған жағдайда, жоспарланған іс - шараларды, олардың аяқталу мерзімдерін және жауапты тұлғаларды көрсете отырып, Қоғамның есептік жазбасына (криптографиялық кілттерге, электрондық цифрлық қолтаңба кілттеріне) үшінші тұлғалардың рұқсатсыз қол жеткізу фактісін жою жөніндегі іс-шаралар жоспарының (бұдан

1) **с уполномоченным органом по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – Уполномоченный орган по вопросам:**
   а) получения/отправки оповещений по угрозам ИБ, посредством получения уведомлений Ответственным лицом ОИБ на электронный адрес;
   б) отправки Уполномоченному органу информации о предпринятых мерах по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества в срок не позднее 2 (двух) рабочих дней со дня выявления факта несанкционированного доступа в ЕСБД;
   в) отправки Уполномоченному органу плана мероприятий по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества с указанием запланированных мероприятий, сроков их завершения и ответственных лиц (далее - план мероприятий) в случае, если принятие мер по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества требует более 2 (двух) рабочих дней;
   г) отправки отчётности по вопросам соблюдения требований Общества к ИБ, предусмотренной действующим законодательством, а также отправки ответов, информации Уполномоченному органу на основании запросов последнего;
   д) совместного участия в согласовании/обсуждении проектов законодательных актов по вопросам ИБ;
   е) совместного участия на заседаниях рабочих групп по разъяснительной работе требований действующего законодательства по вопросам ИБ.

2) **с представителями ЕСБД по вопросам:**
   а) отправки информации в ЕСБД об обнаружении несанкционированного доступа в ЕСБД (информация направляется в течение 12 (двенадцати) часов с момента обнаружения на бумажном носителе и (или) электронным способом);
   б) отправки ЕСБД информации о предпринятых мерах по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества в срок не позднее 2 (двух) рабочих дней со дня выявления факта несанкционированного доступа в ЕСБД;

әрі-іс-шаралар жоспары) бқбж жіберуі (қоғамның криптографиялық кілттеріне, электрондық цифрлық қолтаңба кілттеріне) 2 (екі) жұмыс күнінен артық уақыт қажет; г) АҚ мәселелері бойынша өзге де өзара іс-қимыл; 3) **Қазақстан сақтандырушылар қауымдастығымен, Қазақстан Қаржыгерлер қауымдастығымен келесі мәселелер бойынша:** а) АҚ мәселелері бойынша заңнамалық актілердің жобаларын келісуге / талқылауға бірлесіп қатысу; б) Ақ мәселелері бойынша Қазақстан Республикасының заңнамалық актілеріне өзгерістер мен толықтырулар енгізу жөнінде ұсыныстар жіберу; в) Ақ мәселелері бойынша талаптарды түсіндіру мәселелері жөніндегі мемлекеттік органдардың өкілдерімен, уәкілетті органмен жұмыс топтарына қатысу; 4) **мемлекеттік органдардың өкілдерімен келесі мәселелер бойынша:** а) АҚ мәселелері бойынша заңнама талаптарын сақтау, сондай-ақ Ақ мәселелері бойынша заңнамалық жобаларды талқылау мәселелері; б) дербес деректерді қорғау мәселелері бойынша тартылған мемлекеттік органдарды дербес деректерді қорғау жөніндегі заңнамалық талаптардың бұзылуы туралы хабардар ету; 5**) өрт сөндіру қызметтерімен келесі мәселелер бойынша:** а) Компания үй-жайларындағы өрттер кезіндегі деректерді талдау және іс-қимылдарды үйлестіру. 6) **құқық қорғау органдарымен келесі мәселелер бойынша:** а) Компанияда үшінші тұлғалардың үй-жайларға рұқсатсыз кіруінде және құпия ақпаратта көрсетілген ақпараттық қауіпсіздік инциденттері болған кезде (оның ішінде Компанияның ақпараттық жүйелеріне рұқсатсыз кіру кезінде).	в) отправки ЕСБД плана мероприятий по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества с указанием запланированных мероприятий, сроков их завершения и ответственных лиц (далее - план мероприятий) в случае, если принятие мер по устранению факта несанкционированного доступа третьих лиц к учётной записи (криптографическим ключам, ключам электронной цифровой подписи) Общества требует более 2 (двух) рабочих дней; г) иное взаимодействие по вопросам ИБ. 3) **с Ассоциацией страховщиков Казахстана, Ассоциацией финансистов Казахстана по вопросам:** а) совместного участия в согласовании/обсуждении проектов законодательных актов по вопросам ИБ; б) направления предложений по внесению изменений и дополнений в законодательные акты Республики Казахстан по вопросам ИБ; в) участия в рабочих группах с представителями государственных органов, Уполномоченным органом по вопросам разъяснений требований по вопросам ИБ. 4) **с представителями государственных органов по вопросам:** а) вопросов соблюдения требований законодательства по вопросам ИБ, а также обсуждения проектов законодательных актов по вопросам ИБ; б) информирования государственных органов, задействованных по вопросам защиты персональных данных о нарушении законодательных требований по защите персональных данных. 5) **с пожарными службами по вопросам:** а) анализа данных и координации действий при пожарах в помещениях Компании. 6) **с правоохранительными органами по вопросам:** а) связанных с инцидентами информационной безопасности в Компании, выраженных в несанкционированном доступе третьих лиц к помещениям и конфиденциальной информации (в том числе, при несанкционированном доступе в информационные системы Компании.
11. ТАЛДАУ ЖӘНЕ ҚАЙТА ҚАРАУ	**11. АНАЛИЗ И ПЕРЕСМОТР**
11.1. Саясатты тұрақты түрде қайта қарау: 1) Ақпараттық қауіпсіздік саясаты жылына кемінде бір рет жаңартылып, заңнамалық өзгерістерге, реттеуші органдардың жаңа талаптарына және ISO/IEC 27001 сияқты халықаралық стандарттарға сәйкестігі қамтамасыз етіледі.	11.1. Регулярный пересмотр Политики: 1) Политика пересматривается Советом директоров Компании не реже одного раза в год для обеспечения актуальности и соответствия изменениям законодательства, требованиям регулятора и международным стандартам, включая ISO/IEC 27001.

11.2. Тиімділікті талдау: 1) қолданылып жатқан қауіпсіздік шараларының тиімділігін тоқсан сайын талдау; 2) тиімділік туралы есептерді жоғары басшылыққа ұсынып, түзетуші шешімдер қабылдау. 11.3. Жақсарту бастамалары: 1) анықталған кемшіліктер түзетуші іс-шаралар жоспары аясында жойылады;	11.2. Инициативы по улучшению: 1) выявленные недостатки устраняются в рамках плана корректирующих действий; 2) новые технологии и подходы внедряются для повышения уровня защиты данных; 11.3. Обратная связь: 1) все работники Компании могут вносить предложения по улучшению Политики через выделенные каналы связи (например, корпоративный портал или ОИБ).
12. ЖАУАПКЕРШІЛІК ЖӘНЕ СЫРТҚЫ АУДИТТІ ЖҮРГІЗУ	**12. ОТВЕТСТВЕННОСТЬ И ПРОВЕДЕНИЕ ВНЕШНЕГО АУДИТА**
12.1. Ақпараттық қауіпсіздікті басқару жүйесінің сыртқы аудиті компанияның уәкілетті органының шешіміне сәйкес кемінде үш жылда бір рет жүргізіледі. 12.2. Компанияның әрбір қызметкері осы Саясатты сақтауға және АҚ инциденттерінің алдын алуға шаралар қабылдауға міндетті. 12.3. Осы құжаттың өзектілігін уақтылы жаңартуға жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі. 12.4. Осы құжатты келісу мерзімдерін сақтауға жауапкершілік құжат әзірлеушіге жүктеледі. 12.5. Осы құжатты дайындауға және онда қамтылған деректердің дұрыстығына жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі. 12.6. Осы құжатты Компания сайтында жариялауға жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі. 12.7. Егер осы құжатқа өзгерістер енгізілсе, осы процеске жауапты құрылымдық бөлімшенің басшысы мүдделі тараптарға жаңартылған ақпаратты жеткізуі тиіс. Ол тиісті қызметкерлерге жеке немесе электрондық пошта арқылы хабарлауы қажет. 12.8. Осы рәсімнің талаптарын орындауға жауапкершілік Компанияның барлық басшылары мен қызметкерлеріне жүктеледі. 12.9. Құжаттың түпнұсқасын қағаз түрінде сақтау және оның электрондық көшірмесін КИП-ке орналастыру процестер және өнімдер бөлімшесінің басшысына жүктеледі.	12.1. Внешний аудит системы управления информационной безопасностью проводится в соответствии с решением уполномоченного органа Компании не реже одного раза в три года. 12.2. Каждый работник Компании обязан соблюдать Политику и принимать меры для предотвращения инцидентов ИБ. 12.3. Ответственность за своевременную актуализацию Политики несёт руководитель подразделения информационной безопасности. 12.4. Ответственность за соблюдение сроков согласования Политики возлагается на разработчика документа. 12.5. Ответственность за подготовку Политики и достоверность содержащихся в нём данных, возлагается на руководителя подразделения информационной безопасности. 12.6. Ответственность за своевременную публикацию Политики на сайте Компании несёт руководитель подразделения информационной безопасности. 12.7. В случае внесения изменений в Политику руководитель ОИБ обязан обеспечить доведение актуальной информации до заинтересованных сторон. Для этого, он должен дополнительно уведомить всех работников лично или посредством электронной почты. 12.8. Ответственность за выполнение требований настоящей Политики возлагается на всех работников Компании. 12.9. Ответственность за хранение оригинала на бумажном носителе и размещение электронной копии Политики в КИП несёт руководитель подразделения методологи.
13. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР	**13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**
13.1. Осы құжат Компанияның Директорлар кеңесінің шешімімен бекітіледі, күшіне енеді және онда көрсетілген күннен бастап орындалуға міндетті болады, оны жою немесе жаңа құжатпен ауыстыруға дейін қолданылады. 13.2. Осы құжатты бекіту күні Директорлар кеңесінің шешімімен белгіленген күн болып есептеледі.	13.1. Политика утверждается решением Совета директоров Компании, вступает в силу и становится обязательной для исполнения с даты, указанной в решении Совета директоров Компании, и действует до его отмены или замены новым. 13.2. Датой утверждения Политики считается дата её утверждения решением Совета директоров Компании.

13.3. Осы құжаттың өзектілігін қамтамасыз ету және стандарттарға сәйкестігін сақтау үшін ол тұрақты түрде қайта қаралады.	13.3. Политика подлежит регулярному пересмотру для обеспечения ее актуальности и соответствия требованиям стандартов.
13.4. Осы құжатқа өзгерістер мен толықтырулар енгізу «Құжатталған ақпаратты басқару» рәсіміне сәйкес жүзеге асырылады.	13.4. Внесение изменений и дополнений в Политику осуществляется согласно нормам Документированной процедуры «Управление документированной информацией».
13.5. Құжаттың түпнұсқасы қағаз түрінде Әдіснама бөлімінде сақталады.	13.5. Оригинал Политики на бумажном носителе хранится в подразделении методологии.
13.6. Құжаттың электрондық нұсқасы КИП-те Әдіснама бөлімімен орналастырылады.	13.6. Электронная версия Политики размещается в КИП подразделением методологии.
13.7. Осы құжатпен реттелмеген мәселелер Қазақстан Республикасының заңнамасы және/немесе Компанияның ішкі құжаттары негізінде реттеледі.	13.7. Вопросы, не урегулированные Политикой, регулируются в соответствии с законодательством Республики Казахстан и/или внутренними документами Компании.
13.8. Егер Қазақстан Республикасының заңнамасына өзгерістер енгізілуіне байланысты осы құжаттың жекелеген нормалары заңнамаға қайшы келсе, онда бұл нормалар өз күшін жояды және тиісті өзгерістер енгізілгенге дейін Қазақстан Республикасының нормативтік құқықтық актілері басшылыққа алынады.	13.8. Если в результате изменения законодательства Республики Казахстан отдельные пункты (нормы) Политики вступают в противоречие с законодательством Республики Казахстан, эти пункты (нормы) утрачивают силу до момента внесения соответствующих изменений в Политику.