Приложение 1 к Политике информационной безопасности АО «КСЖ «Nomad Life», утвержденной решением Совета директоров Протокол №270325/1 от «27» Марта 2025 г.

«ӨСК «NOMAD LIFE» АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

МАЗМҰНЫ

1. ЖАЛПЫ ЕРЕЖЕЛЕР

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.

2. ҚОЛДАНЫЛУ САЛАСЫ

2.1. Бұл Саясат Компанияның барлық бөлімшелеріне, қызметкерлеріне, мердігерлеріне, сондай-ақ барлық пайдаланылатын ақпараттық инфрақұрылымға, соның ішінде серверлерге, дерекқорларға, желілерге және мобильді құрылғыларға қолданылады.

3. НОРМАТИВТІК СІЛТЕМЕЛЕР

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 қатерлерінен қорғаныс деңгейін бағалау ережелері;

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «КСЖ «NOMAD LIFE»

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Под Политикой информационной безопасности АО «КСЖ «Nomad Life» (далее – Политика) понимается совокупность документированных управленческих решений, направленных на обеспечение информационной безопасности в информационной системе, включая бумажный и электронный документооборот и обмен речевой конфиденциальной информацией. Политика информационной безопасности представляет собой пакет документов, включающих основной документ – «Политика информационной безопасности» и документы, регламентирующие процессы обеспечения информационной безопасности, деятельность должностных лиц и пользователей информационной системы АО «КСЖ «Nomad Life» (далее – Компания).

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.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

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. НОРМАТИВНЫЕ ССЫЛКИ

3.1. Настоящий документ разработан в соответствии с требованиями следующих документов:

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;

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) «Құжатталған ақпаратты басқару» құжатталған процедурасы.

4. ТЕРМИНДЕР, АНЫҚТАМАЛАР ЖӘНЕ ҚЫСҚАРТУЛАР

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 – ақпаратқа тек уәкілетті тұлғалардың қол жеткізуін қамтамасыз ету қасиеті;
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.

4.2. Осы Саясатта қолданылатын қысқартулар:
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) ВНД – ішкі нормативтік құжат;
6) АҚ – ақпараттық қауіпсіздік;
7) АЖ – ақпараттық жүйе;
8) ИТ – ақпараттық технологиялар;
9) КИП – Компанияның корпоративтік ақпараттық порталы;
10) МФА – көпфакторлы аутентификация (Multi-Factor Authentication).

5. НЕГІЗГІ ПРИНЦИПТЕР

5.1. Құпиялылық – ақпаратқа тек уәкілетті тұлғалар ғана қол жеткізе алады.
5.2. Тұтастық – деректердің дұрыстығы мен толықтығын қамтамасыз ету.

5) Правила оценки уровня защищённости от угроз информационной безопасности, утверждённые 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) Документированная процедура «Управление документированной информацией».

4. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

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 информации, обеспечивающее доступ к ней только уполномоченным лицам;
7) фаервол (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;

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);

5.3. Қолжетімділік – ақпарат қажет болған жағдайда қолжетімді болуы тиіс.

6. ҰЙЫМДАСТЫРУ ШАРАЛАРЫ

6.1. Ақпараттық қауіпсіздікті басқаруға жауапты тұлғаны (CISO) тағайындау:

1) АҚ стратегияларын әзірлеу, мониторинг жүргізу және деректерді қорғау шараларын үйлестіру;

2) Реттеуші органдармен және сыртқы аудиторлармен өзара әрекеттестікті қамтамасыз ету.

6.2. Ішкі нормативтік құжаттарды әзірлеу және қолдау:

1) АҚ қамтамасыз ету жөніндегі ережелер, нұсқаулықтар және рәсімдер;

2) Құпия ақпаратпен жұмыс істеу, парольдерді пайдалану және қол жеткізуді басқару бойынша ВНД.

6.3. Қызметкерлерді оқыту:

1) Барлық қызметкерлерге, соның ішінде топ-менеджментке арналған тұрақты тренингтер;

2) Киберқауіптер туралы ақпараттандыру бойынша мерзімді тарату және тестілеу.

7. ТЕХНИКАЛЫҚ ШАРАЛАР

7.1. Шифрлауды қолдану:

1) Деректерді сақтау және беру кезінде қорғау;

2) Сертификатталған криптографиялық құралдарды пайдалану.

7.2. Аутентификация және қолжетімділікті басқару:

1) Маңызды жүйелер үшін көпфакторлы аутентификацияны (МФА) енгізу;

2) Пайдаланушы тіркелгілерін басқару және қолжетімділік құқықтарын тұрақты түрде қайта қарау.

7.3. Желінің периметрін қорғау:

1) Фаерволдарды (брандмауэрлерді), шабуылдардың алдын алу жүйелерін (IPS) орнату және баптау;

2) Қауіпсіз байланыс арналары арқылы VPN көмегімен корпоративтік желіге қолжетімділікті шектеу.

7.4. Қауіп-қатерлерді бақылау және әрекет ету:

1) Ақпараттық қауіпсіздік оқиғаларын талдау үшін SIEM жүйелерін пайдалану;

2) Инциденттер туралы хабарландырулар мен оларға жауап қайтаруды автоматтандыру.

8. ТӘУЕКЕЛДЕРДІ БАСҚАРУ

8.1. Тәуекелдерді анықтау:

1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ВНД талаптарына сәйкес, аса маңызды активтерге қатысты қауіптер мен осалдықтарды бағалауды тұрақты түрде жүргізу;

2) Тәуекелдерді басқару үшін олардың тізілімін жасау.

8.2. Талдау және бағалау:

1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ВНД талаптарына сәйкес, тәуекелдердің ықтималдығы мен салдарын бағалау;

2) Тәуекелдердің маңыздылығына қарай басымдық беру.

8.3. Басқару және минимизация:

1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ВНД әзірлеу;

5) ВНД – внутренний нормативный документ;

6) ИБ – информационная безопасность;

7) ИС – информационная система;

8) ИТ – информационные технологии;

9) КИП – корпоративный информационный портал Компании;

10) МФА – многофакторная аутентификация (Multi-Factor Authentication).

5. ОСНОВНЫЕ ПРИНЦИПЫ

5.1. Конфиденциальность: доступ к информации получают только уполномоченные лица.

5.2. Целостность: обеспечение корректности и полноты данных.

5.3. Доступность: информация должна быть доступна пользователям при необходимости.

6. ОРГАНИЗАЦИОННЫЕ МЕРЫ

6.1. Назначение ответственного лица за управление информационной безопасностью (CISO):

1) ответственный за ИБ разрабатывает стратегии, проводит регулярный мониторинг и координирует мероприятия по защите данных;

2) обеспечтвает взаимодействие с регуляторами и внешними аудиторами.

6.2. Разработка и поддержание внутренних нормативных документов:

1) регламенты, инструкции и процедуры по обеспечению безопасности;

2) ВНД по использованию паролей, управления доступом и обращения с конфиденциальной информацией.

6.3. Обучение работников:

1) регулярные тренинги для всех работников, включая топ-менеджмент, на темы ИБ;

2) периодические рассылки и тесты на осведомлённость о киберугрозах.

6.4. Проведение регулярных аудитов и проверок:

1) оценка уязвимостей в процессах и информационных системах;

2) анализ соблюдения норм и стандартов безопасности.

7. ТЕХНИЧЕСКИЕ МЕРЫ

7.1. Применение шифрования:

1) защита данных в состоянии покоя и при передаче;

2) использование сертифицированных криптографических средств.

7.2. Аутентификация и управление доступом:

1) внедрение многофакторной аутентификации (МФА) для критических систем;

2) управление учётными записями пользователей с регулярным пересмотром прав доступа.

7.3. Защита периметра сети:

1) установка и настройка фаерволов, систем предотвращения вторжений (IPS);

2) ограничение доступа к корпоративной сети через VPN с безопасными каналами связи.

7.4. Мониторинг и реагирование на угрозы:

1) использование SIEM-систем для анализа событий безопасности;

2) автоматизация уведомлений и реагирования на инциденты.

8. УПРАВЛЕНИЕ РИСКАМИ

2) Компанияның резервтік көшіру жөніндегі ВНД талаптарына сәйкес, резервтік көшіруді және ақаусыз жүйелерді пайдалану.

8.4. Тұрақты жаңарту:

1) Компанияның ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ВНД талаптарына сәйкес, бизнес-процестер, технологиялар немесе қауіптер өзгерген кезде тәуекелдерді қайта бағалау;

2) Жоғары басшылыққа тұрақты есеп беру.

9. ИНЦИДЕНТТЕРДІ БАСҚАРУ

9.1. Ақпараттық қауіпсіздік инциденттеріне жауап беру жөніндегі ВНД әзірлеу және енгізу.

9.2. Компанияның ВНД талаптарына сәйкес, қауіп-қатерлерді үздіксіз мониторингтеу және анықтау.

9.3. Деректердің таралуы орын алған жағдайда, заңнамада белгіленген мерзімде уәкілетті органдарды хабардар ету.

10. ҚАШЫҚТАН ҚЫЗМЕТ КӨРСЕТУ

10.1. Қашықтан қызмет көрсету кезінде клиенттердің жеке деректерін және құпия ақпаратын қорғау қамтамасыз етіледі.

10.2. Қауіпсіз байланыс арналары мен қашықтан қолжетімділік үшін аутентификация механизмдері пайдаланылады.

10.3. Компанияның веб-ресурстарының қауіпсіздігі бақыланады.

10.4. Қашықтан қызмет көрсету жүйелерінің қорғалуын тексеру және аудит тұрақты түрде жүргізіледі.

10.5. Заңнама талаптарына сәйкес, деректердің берілуі және пайдаланушылардың қашықтан сервистерге қолжетімділігі бақыланады.

11. СӘЙКЕСТІКТІ БАҚЫЛАУ

11.1. Ақпараттық қауіпсіздікке жауапты бөлімше ішкі нормативтік құжаттарға және Қазақстан Республикасының заңнамасына сәйкестікті тұрақты түрде тексеруді жүзеге асырады.

11.2. Регуляторға белгіленген мерзімде есеп беру.

12. ТАЛДАУ ЖӘНЕ ҚАЙТА ҚАРАУ

12.1. 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.

12.2. Тиімділікті талдау:

1) Қолданылып жатқан қауіпсіздік шараларының тиімділігін тоқсан сайын талдау;

2) Тиімділік туралы есептерді жоғары басшылыққа ұсынып, түзетуші шешімдер қабылдау.

12.3. Жақсарту бастамалары:

1) Анықталған кемшіліктер түзетуші іс-шаралар жоспары аясында жойылады;

2) Деректерді қорғау деңгейін арттыру үшін жаңа технологиялар мен әдістер енгізіледі.

12.4. Кері байланыс:

Компанияның барлық қызметкерлері ақпараттық қауіпсіздік саясатын жетілдіру бойынша ұсыныстарды арнайы байланыс арналары (мысалы, корпоративтік портал немесе АҚ қызметі) арқылы енгізе алады.

13. ЖАУАПКЕРШІЛІК

8.1. Идентификация рисков:

1) регулярное проведение оценки угроз и уязвимостей для критически важных активов, согласно ВНД по управлению рисками ИБ Компании;

2) создание реестра рисков для их последующего управления.

8.2. Анализ и оценка:

1) оценка вероятности и последствий реализации рисков, согласно ВНД по управлению рисками ИБ Компании;

2) приоритезация рисков на основе их критичности.

8.3. Управление и минимизация:

1) разработка ВНД по управлению рисками ИБ в Компании

2) использование резервного копирования данных и отказоустойчивых систем, согласно требовании ВНД по резервному копированию Компании.

8.4. Постоянное обновление:

1) обновление оценки рисков при изменении бизнес-процессов, технологий или угроз, согласно требованию ВНД по управлению рисками ИБ в Компании;

2) регулярная отчётность высшему руководству.

9. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

9.1. Разработка и внедрение ВНД по реагированию на инциденты ИБ.

9.2. Непрерывный мониторинг и выявление угроз, согласно требованиям ВНД Компании.

9.3. Уведомление уполномоченных органов в случае утечки данных в сроки, установленные законодательством.

10. ДИСТАНЦИОННОЕ ОКАЗАНИЕ УСЛУГ

10.1. При оказании дистанционных услуг обеспечивается защита персональных данных и конфиденциальной информации клиентов.

10.2. Используются защищённые каналы связи и механизмы аутентификации для удалённого доступа.

10.3. Проводится контроль за безопасностью веб-ресурсов Компании.

10.4. Регулярно проводится аудит и тестирование защищённости сервисов дистанционного обслуживания.

10.5. Контролируется передача данных и доступ пользователей к дистанционным сервисам согласно требованиям законодательства.

11. КОНТРОЛЬ СООТВЕТСТВИЯ

11.1. Проведение регулярных проверок соответствия внутренним нормативным документам и законодательству Республики Казахстан проводит ответственное подразделение за ИБ;

11.2. Отчётность перед регулятором в установленные сроки.

12. АНАЛИЗ И ПЕРЕСМОТР

12.1. Регулярный пересмотр Политики:

1) Политика по информационной безопасности пересматривается не реже одного раза в год для обеспечения актуальности и соответствия изменениям законодательства, новым требованиям регуляторов и международным стандартам, включая ISO/IEC 27001.

12.2. Анализ эффективности:

1) ежеквартально проводится анализ эффективности применяемых мер безопасности;

13.1. Компанияның әрбір қызметкері осы Саясатты сақтауға және АҚ инциденттерінің алдын алуға шаралар қабылдауға міндетті.
13.2. Осы құжаттың өзектілігін уақтылы жаңартуға жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі.
13.3. Осы құжатты келісу мерзімдерін сақтауға жауапкершілік құжат әзірлеушіге жүктеледі.
13.4. Осы құжатты дайындауға және онда қамтылған деректердің дұрыстығына жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі.
13.5. Осы құжатты Компания сайтында жариялауға жауапкершілік ақпараттық қауіпсіздік бөлімшесінің басшысына жүктеледі.
13.6. 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, әсіресе егер олардың жұмысы осы құжатпен тікелей байланысты болса. Бұл қызметкерлердің ескі нұсқамен жұмыс істеуінің алдын алу үшін қажет.
13.7. Осы рәсімнің талаптарын орындауға жауапкершілік Компанияның барлық басшылары мен қызметкерлеріне жүктеледі.
13.8. Құжаттың түпнұсқасын қағаз түрінде сақтау және оның электрондық көшірмесін КИП-ке орналастыру процестер және өнімдер бөлімшесінің басшысына жүктеледі.

14. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

14.1. Осы құжат күшіне енген күннен бастап қолданылады және Компанияның ішкі құжаттарына сәйкес қайта қаралады.
14.2. 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.
14.3. Осы құжатты бекіту күні Директорлар кеңесінің шешімімен белгіленген күн болып есептеледі.
14.4. Осы құжаттың өзектілігін қамтамасыз ету және стандарттарға сәйкестігін сақтау үшін ол тұрақты түрде қайта қаралады.
14.5. Осы құжатқа өзгерістер мен толықтырулар енгізу «Құжатталған ақпаратты басқару» рәсіміне сәйкес жүзеге асырылады.
14.6. Құжаттың түпнұсқасы қағаз түрінде процестер және өнімдер бөлімінде сақталады.
14.7. Құжаттың электрондық нұсқасы КИП-те процестер және өнімдер бөлімшесімен орналастырылады.
14.8. Егер осы құжаттың қандай да бір нормалары Қазақстан Республикасының заңнамасына қайшы келсе, онда Қазақстан Республикасының заңнамасы қолданылады.
14.9. Осы құжатпен реттелмеген мәселелер Қазақстан Республикасының заңнамасы және/немесе Компанияның ішкі құжаттары негізінде реттеледі.
14.10. Егер Қазақстан Республикасының заңнамасына өзгерістер енгізілуіне байланысты осы құжаттың жекелеген нормалары заңнамаға қайшы келсе, онда бұл

2) доклады об эффективности представляются высшему руководству для принятия корректирующих решений.
12.3. Инициативы по улучшению:
1) выявленные недостатки устраняются в рамках плана корректирующих действий;
2) новые технологии и подходы внедряются для повышения уровня защиты данных.
12.4. Обратная связь:
1) все работники Компании могут вносить предложения по улучшению Политики через выделенные каналы связи (например, корпоративный портал или службу ИБ).

13. ОТВЕТСТВЕННОСТЬ

13.1. Каждый работник Компании обязан соблюдать настоящую Политику и принимать меры для предотвращения инцидентов ИБ.
13.2. Ответственность за своевременную актуализацию Политики несёт руководитель подразделения информационной безопасности.
13.3.
13.4. Ответственность за подготовку Политики и достоверность содержащихся в нём данных, возлагается на руководителя подразделения информационной безопасности.
13.5. Ответственность за публикацию Политики на сайте Компании несёт руководитель подразделения информационной безопасности.
13.6. В случае внесения изменений в Политику, руководитель Отдела информационной безопасности обязан обеспечить доведение актуальной информации до заинтересованных сторон. Для этого, он должен дополнительно уведомить всех работников лично или посредством электронной почты.
13.7. Ответственность за выполнение требований Политики возлагается на всех работников Компании.
13.8. Ответственность за хранение оригинала на бумажном носителе и размещение электронной копии Политики в КИП несёт руководитель подразделения процессов и продуктов.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1.
14.2. Политики утверждается решением Совета директоров Компании, вступает в силу и становится обязательным для исполнения с даты, указанной в решении Совета директоров Компании, и действует до его отмены или замены новым.
14.3. Датой утверждения Политики считается дата его утверждения решением Совета директоров Компании.
14.4. Политика подлежит регулярному пересмотру для обеспечения его актуальности и соответствия требованиям стандартов.
14.5. Внесение изменений и дополнений в Политику осуществляется согласно нормам Документированной процедуры «Управление документированной информацией».
14.6. Оригинал Политики на бумажном носителе хранится в подразделении процессов и продуктов.
14.7. Электронная версия Политики размещается в КИП подразделением процессов и продуктов.
14.8. В случае, если какие-либо нормы Политики, противоречат законодательству Республики Казахстан, то

нормалар өз күшін жояды және тиісті өзгерістер енгізілгенге дейін Қазақстан Республикасының нормативтік құқықтық актілері басшылыққа алынады.

применяются нормы законодательства Республики Казахстан.

14.9. Вопросы, не урегулированные Политикой, регулируются в соответствии с законодательством Республики Казахстан и/или внутренними документами Компании.

14.10. Если в результате изменения законодательством Республики Казахстан отдельные пункты (нормы) Политики вступают с противоречие с законодательством Республики Казахстан, эти пункты (нормы) утрачивают силу и до момента внесения соответствующих изменений в Политику, Стороны руководствуются нормативными правовыми актами Республики Казахстан.