Приложение 1 к Политике информационной безопасности АО «СК «Номад Иншуранс», утвержденной решением Совета директоров
Протокол № ___
от «___» _____ 2026 г.

««Номад Иншуранс» СК» АҚ
АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

МАЗМҰНЫ

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «СК «НОМАД ИНШУРАНС»

СОДЕРЖАНИЕ

3.1. Саясат келесі нормативтік-құқықтық актілердің талаптарына сәйкес әзірленді:

1) Қазақстан Республикасының «Информатизация туралы» заңы – ақпаратты қамтамасыз ету және қорғау, сондай-ақ ақпараттық ресурстарды басқару мәселелерін жүзеге асырады;

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 сандық қорғау мәселелерін, соның ішінде цифрлық ортадағы қауіпсіздігін реттейді;

4) Қазахстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 30 шілдедегі №164 «Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарды бекіту туралы» қаулысы;

5) Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі басқармасының 2020 жылдың 23 қарашасындағы №110 қаулысымен бекітілген ақпараттық қауіпсіздік қатерлерінен қорғаныс деңгейін бағалау ережелері;

6) СТ РК ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері – Талаптар»;

7) СТ РК ISO/IEC 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері»;

8) «Құжаттама мен жазбаларды басқару» процедурасы.

4. ТЕРМИНДЕР, АНЫҚТАМАЛАР ЖӘНЕ ҚЫСҚАРТУЛАР

4.1. Осы Саясатта келесі терминдер тиісті анықтамаларымен қолданылады:

1) қолжетімділік – қажетті уақытта уәкілетті тұлғалар үшін ақпаратты қолдану мүмкіндігін қамтамасыз ету;

2) нұсқаулық – қызметкерлерге ақпараттық қауіпсіздік талаптарын, ережелерін және шараларын түсіндіру процесі;

3) ақпараттық қауіпсіздік – ақпаратты және ақпараттық инфрақұрылымды рұқсатсыз қол жеткізуден, жойылудан, өзгертілуден және басқа да қауіптерден қорғау;

4) ақпараттық қауіпсіздік оқыс оқиғасы – ақпараттың құпиялылығына, тұтастығына 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 (желіаралық экран) – желілік трафикті белгіленген қауіпсіздік ережелеріне сәйкес бақылау

3. НОРМАТИВНЫЕ ССЫЛКИ

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) Постановление Правления Национального Банка Республики Казахстан от 30 июля 2018 года № 164 «Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации»;

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 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»;

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

8) Процедура «Управление документацией и записями».

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 – 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;

және сүзгілеуге арналған бағдарламалық немесе аппараттық құрал;
8) фишинг – өзін сенімді дереккөз ретінде таныстырып, құпия ақпаратты алу алаяқтық әдісі;
9) тұтастық – ақпараттың сақтау, өңдеу және жіберу 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) ІНҚ – ішкі нормативтік құжат;
6) АҚ – ақпараттық қауіпсіздік;
7) АЖ – ақпараттық жүйе;
8) АТ – ақпараттық технологиялар;
9) КАП – Компанияның корпоративтік ақпараттық порталы;
10) КФА – көпфакторлы аутентификация (Multi-Factor Authentication).

5. НЕГІЗГІ ПРИНЦИПТЕР

5.1. Құпиялылық: ақпаратқа тек уәкілетті тұлғалар ғана қол жеткізеді.
5.2. Тұтастық: мәліметтердің туралығын, растығын және толықтығын қамтамасыз ету.
5.3. Қолжетімділік – ақпарат қажет болған жағдайда қолжетімді болуы тиіс.

6. ҰЙЫМДАСТЫРУ ШАРАЛАРЫ

6.1. Ақпараттық қауіпсіздікті басқаруға жауапты тұлғаны (CISO) тағайындау:
1) АҚ үшін жауапты стратегияларды әзірлейді, жүйелі бақылау жүргізеді және деректерді қорғау шараларын үйлестіреді;
2) реттеуші органдармен және сыртқы аудиторлармен өзара әрекеттестікті қамтамасыз етеді.
6.2. Ішкі нормативтік құжаттарды әзірлеу және қолдау:
1) АҚ қамтамасыз ету жөніндегі ережелер, нұсқаулықтар және рәсімдер;
2) құпия ақпаратпен жұмыс істеу, құпиясөздерді пайдалану және қол жеткізуді басқару бойынша ІНҚ.
6.3. Қызметкерлерді оқыту:
1) басқарушылар құрамынмен қоса барлық қызметкерлер үшін арналған АҚ тақырыбындағы тұрақты тренингтер;
2) киберқауіптер туралы ақпараттандыру бойынша мерзімді тарату және тестілеу.
6.4. Тұрақты аудиттер мен тексерулер жүргізу:
1) процестер мен ақпараттық жүйелердегі осалдылықтарды бағалау;
2) қауіпсіздік нормалары мен стандарттарының сақталуын талдау;
3) IT-инфрақұрылымға және/немесе ақпараттық қауіпсіздікті басқару жүйесінің мерзімді тәуелсіз сыртқы аудит жүргізу, сондай-ақ заңнаманың, реттеуші органның және ішкі нормативтік құжаттардың талаптарында айқындалған жағдайлар мен тәртіпке

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) 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 исключительно уполномоченные лица.
5.2. Целостность: обеспечение корректности, достоверности 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) обеспечивает взаимодействие с регуляторами и внешними аудиторами.
6.2. Разработка и поддержание внутренних нормативных документов:
1) регламенты, инструкции и процедуры по обеспечению ИБ;
2) ВНД по использованию паролей, управления доступом и обращения с конфиденциальной информацией.
6.3. Обучение работников:
1) регулярные тренинги для всех работников, включая руководящий состав, на темы ИБ;

сәйкес деректер қауіпсіздігі рәсімдерінің сақталуын бағалау.

7. ТЕХНИКАЛЫҚ ШАРАЛАР

7.1. Шифрлауды қолдану:

1) деректерді тыныштық күйінде сақтау және беру кезінде қорғау;

2) сертификатталған криптографиялық құралдарды пайдалану.

7.2. Аутентификация және қолжетімділікті басқару:

1) маңызды жүйелер үшін көпфакторлы аутентификацияны (КФА) енгізу;

2) пайдаланушы тіркеулік жазбасын басқару мен қолжетімділік құқықтарын тұрақты түрде қайта қарау.

7.3. Желінің периметрін қорғау:

1) фаерволдарды, 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 АҚ тәуекелдерін басқару жөніндегі ІНҚ талаптарына сәйкес, аса маңызды активтерге қатысты қауіптер мен осалдықтарды бағалауды жүргізу;

2) тәуекелдердің кейінгі басқару үшін олардың тізілімін жасау.

8.2. Талдау және бағалау:

1) компанияның АҚ тәуекелдерін басқару жөніндегі ІНҚ талаптарына сәйкес, тәуекелдердің ықтималдығы мен салдарын бағалау;

2) тәуекелдердің маңыздылығына қарай басымдық беру.

8.3. Басқару және минимизация:

1) компанияның АҚ тәуекелдерін басқару жөніндегі ІНҚ әзірлеу;

2) компанияның резервтік көшіру жөніндегі ІНҚ талаптарына сәйкес, резервтік көшіруді және бұзылысқа төзімді жүйелерді пайдалану.

8.4. Тұрақты жаңарту:

1) компанияның АҚ тәуекелдерін басқару жөніндегі ІНҚ талаптарына сәйкес, бизнес-процестер, технологиялар немесе қауіптер өзгерген кезде тәуекелдерді қайта бағалау;

2) Компания басшылығына тұрақты есеп беру.

9. ИНЦИДЕНТТЕРДІ БАСҚАРУ

9.1. АҚ инциденттеріне жауап беру жөніндегі ІНҚ әзірлеу және енгізу.

9.2. Компанияның ІНҚ талаптарына сәйкес, қауіп-қатерлерді үздіксіз бақылау және анықтау.

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

10. ҚАШЫҚТАН ҚЫЗМЕТ КӨРСЕТУ

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;

3) проведение периодического независимого внешнего аудита IT-инфраструктуры и/или системы управления информационной безопасностью, а также оценки соблюдения процедур безопасности данных, в случаях и порядке, определяемых требованиями законодательства, регулятора и внутренними нормативными документами.

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

8.1. Идентификация рисков:

1) 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) приоритизация 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 Компании.

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 қызмет көрсетуге қолжетімділігі бақыланады.

11. СӘЙКЕСТІКТІ БАҚЫЛАУ

11.1. АҚ-ке жауапты бөлім жүзеге асыратын ІНҚ мен Қазақстан Республикасының заңнамасына сәйкестігін тұрақты тексеру.
11.2. Реттеуішке белгіленген мерзімде есеп беру.
11.3. Ішкі аудит қызметі ақпарат қауіпсіздігін басқару жүйесінің жағдай бағалауын бес жылда кемінде бір рет орындайды. Бағалау тәуекелдің дәрежесі мен Компанияның қажеттіліктеріне байланысты жоспарлы және жоспардан тыс ретте орындалуы мүмкін.

12. ТАЛДАУ ЖӘНЕ ҚАЙТА ҚАРАУ

12.1. Саясатты тұрақты түрде қайта қарау:
1) Ақпараттық қауіпсіздік Саясаты қажеттілігіне қарай және/немесе заңнамадағы өзгерістерге, реттеуіштің жаңа талаптарына сәйкес қайта қаралады.
12.2. Тиімділікті талдау:
1) қолданылып жатқан қауіпсіздік шараларының тиімділігін тоқсан сайын талдау;
2) тиімділік туралы түзетуші шешімдер қабылдау мақсатында есептерді жоғары басшылыққа ұсыну.
12.3. Жақсарту бастамалары:
1) анықталған кемшіліктер түзету әрекеттері жоспары аясында жойылады;
2) деректерді қорғау деңгейін арттыру үшін жаңа технологиялар мен әдістер енгізіледі.
12.4. Кері байланыс:
1) Компанияның барлық қызметкерлері белгіленген каналдар (мысалы, корпоративті портал немесе АҚ бойынша бөлімше) арқылы Саясатты жетілдіру бойынша ұсыныстарын енгізе алады.

13. ЖАУАПКЕРШІЛІК

13.1. Компанияның әрбір қызметкері осы Саясатты сақтауға және АҚ инциденттерінің алдын алуға шаралар қабылдауға міндетті.
13.2. Осы Саясаттың өзектілігін уақтылы жаңартуға жауапкершілік АҚ бөлімшесінің басшысына жүктеледі.
13.3. Осы Саясаттың келісу мерзімдерін сақтауға жауапкершілік құжат әзірлеушіге жүктеледі.
13.4. Осы Саясатты дайындауға және онда қамтылған деректердің дұрыстығына жауапкершілік АҚ бөлімшесінің басшысына жүктеледі.
13.5. Осы Саясатты Компания сайтында жариялауға жауапкершілік АҚ бөлімшесінің басшысына жүктеледі.
13.6. Егер Саясатқа өзгерістер енгізілген жағдайда АҚ жөніндегі бөлімінің басшысы өзекті ақпаратты мүдделі

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 ВНД и законодательству Республики Казахстан, которые осуществляет ответственное подразделение за ИБ.
11.2. Отчётность перед регулятором в установленные сроки.
11.3. Служба внутреннего аудита проводит оценку состояния системы управления информационной безопасности не реже одного раза в пять лет. Оценка может проводиться в плановом и внеплановом порядке в зависимости от степени риска и потребности Компании.

12. АНАЛИЗ И ПЕРЕСМОТР

12.1. Регулярный пересмотр Политики:
1) Политика информационной безопасности пересматривается по мере необходимости и/или в соответствии с изменениями законодательства, новым требованиям регулятора.
12.2. Анализ эффективности:
1) ежеквартально проводится анализ эффективности применяемых мер безопасности;
2) доклады об эффективности представляются высшему руководству Компании 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 подразделение по ИБ).

13. ОТВЕТСТВЕННОСТЬ

тараптарға жеткізуді қамтамасыз етуге міндетті. Ол үшін барлық қызметкерлерді жеке немесе электрондық пошта арқылы хабарлауы қажет.

13.7. Осы Саясат талаптарын орындауға жауапкершілік Компанияның барлық қызметкерлеріне жүктеледі.

13.8. Саясаттың түпнұсқасын қағаз түрінде сақтау және оның электрондық көшірмесін КАП-ке орналастыру Әдістеме және СМЖ 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 Саясат 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 Саясатты бекіту күні Директорлар кеңесінің шешімімен белгіленген күн болып есептеледі.

14.4. Осы Саясат өзектілігін қамтамасыз ету және стандарттарға сәйкестігін сақтау үшін ол тұрақты түрде қайта қаралады.

14.5. Осы Саясатқа өзгерістер мен толықтырулар енгізу «Құжаттама мен жазбаларды басқару» Рәсіміне сәйкес жүзеге асырылады.

14.6. Саясаттың қағаз түріндегі түпнұсқасы Әдістеме және СМЖ бөлімшесінде сақталады.

14.7. Саясаттың электрондық нұсқасын КАП-та Әдістеме және СМЖ бөлімшесі орналастырады.

14.8. Егер осы Саясаттың қандай да бір нормалары Қазақстан Республикасының заңнамасына қайшы келсе, онда Қазақстан Республикасының заңнамасы қолданылады.

14.9. Осы Саясатпен реттелмеген мәселелер Қазақстан Республикасының заңнамасы және/немесе Компанияның ішкі құжаттары негізінде реттеледі.

14.10. Егер Қазақстан Республикасының заңнамасына енгізілген өзгерістер нәтижесінде Саясаттың жекелеген тармақтары (нормалары) Қазақстан Республикасының заңнамасына қайшы келсе, мұндай тармақтар (нормалар) күшін жояды және Саясатқа тиісті өзгерістер енгізілгенге дейін Тараптар Қазақстан Республикасының нормативтік құқықтық актілерін басшылыққа алады.

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 ИБ.

13.3. Ответственность за соблюдение сроков согласования Политики возлагается на разработчика документа.

13.4. Ответственность за подготовку Политики и достоверность содержащихся в нём данных, возлагается на руководителя подразделения ИБ.

13.5. Ответственность за публикацию Политики на сайте Компании несёт руководитель подразделения ИБ.

13.6. В случае внесения изменений в Политику руководитель подразделения по ИБ 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 настоящей 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 Методологии и СМК.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Настоящий документ действует со дня вступления в силу и пересматривается в соответствии с внутренними документами Компании.

14.2. Политика 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 Процедуры «Управление документацией и записями».

14.6. Оригинал Политики на бумажном носителе хранится в подразделении Методологии и СМК.

14.7. Электронная версия Политики размещается в КИП подразделением Методологии и СМК.

14.8. В случае, если какие-либо нормы Политики, противоречат законодательству Республики Казахстан, то 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 в 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.