

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 11 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

Приложение 1 к Политике информационной безопасности АО «СК «Номад Иншуранс», утвержденной решением Совета директоров
Протокол № ____
от «17» сентября 2026 г.

««Номад Иншуранс» СК» АҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

МАЗМҰНЫ

1. ЖАЛПЫ ЕРЕЖЕЛЕР

1.1. ««НОМАД Иншуранс» СК» АҚ Ақпараттық қауіпсіздік Саясаты (бұдан әрі – Саясат) ұғымы – ақпараттық жүйедегі, соның ішінде қағаз және электрондық құжат айналымында, сондай-ақ құпия ақпараттың ауызша алмасуында ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған құжатталған басқару шешімдерінің жиынтығы болып танылады. Ақпараттық қауіпсіздік Саясаты - ол «Ақпараттық қауіпсіздік Саясаты» негізгі құжатынан және «НОМАД Иншуранс» СК» АҚ (бұдан әрі – Компания) ақпараттық қауіпсіздікті қамтамасыз ету процестерін, ақпараттық жүйелерінің пайдаланушыларының, лауазымды тұлғаларының іс-әрекеттерін реттейтін құжаттардан тұратын құжаттар жиынтығы.

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. Осы Саясат Компанияның ақпараттық қауіпсіздігін қамтамасыз етуге қатысты бірыңғай тәсілдерін айқындайды, оның ішінде ақпаратты қорғаудың ұйымдастырушылық, құқықтық және техникалық шараларын, ақпараттық қауіпсіздік тәуекелдерін басқаруды, қол жеткізуді басқаруды, ақпараттық қауіпсіздік оқиғаларын мониторингтеуді, инциденттерге ден қоюды, ақпараттық қауіпсіздік талаптарының сақталуын бақылауды, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету процестеріне қатысушылар арасында рөлдер мен жауапкершілікті бөлуді қамтиды.

2. ҚОЛДАНЫЛУ САЛАСЫ

2.1. Бұл Саясат Компанияның барлық бөлімшелеріне, қызметкерлеріне, мердігерлеріне, сондай-ақ барлық пайдаланылатын ақпараттық инфрақұрылымға (серверлерге, дерекқорларға, желілерге, стационарлық телефондар мен мобильді құрылғыларға және т.б. қоса алғанда) қолданылады.

2.2. Компанияның ақпараттық қауіпсіздікті басқару жүйесінің қатысушылары:

- 1) басқару органы;
- 2) атқарушы орган;

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «СК «НОМАД ИНШУРАНС»

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Под Политикой информационной безопасности АО «СК «НОМАД Иншуранс» (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 «СК «НОМАД Иншуранс» (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.

1.3. Настоящая Политика определяет единые подходы Компании к обеспечению информационной безопасности, включая организационные, правовые и технические меры защиты информации, управление рисками информационной безопасности, управление доступами, мониторинг событий информационной безопасности, реагирование на инциденты, контроль соблюдения требований информационной безопасности, а также распределение ролей и ответственности между участниками процессов обеспечения 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, стационарные телефоны и мобильные устройства и т.д.).

2.2. Участниками системы управления информационной безопасностью Компании являются:

- 1) орган управления;

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 12 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

- 3) ақпараттық қауіпсіздік бөлімшесі;
- 4) ақпараттық технологиялар бөлімшесі;
- 5) қауіпсіздік бөлімшесі;
- 6) қызметкерлермен жұмыс жүргізу бөлімшесі;
- 7) заң бөлімшесі;
- 8) комплаенс-бақылау бөлімшесі;
- 9) ішкі аудит бөлімшесі;
- 10) өзінің лауазымдық міндеттерін орындау аясындағы басқа бөлімшелер.

3. НОРМАТИВТІК СІЛТЕМЕЛЕР

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) Қазақстан 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 рәсімі»;
- 9) Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2026 жылғы 20 сәуірдегі №81 «Қаржы нарығында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ең төмен талаптарды бекіту туралы» қаулысы

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;

- 2) исполнительный орган;
- 3) подразделение по информационной безопасности;
- 4) подразделение по информационным технологиям;
- 5) подразделение по безопасности;
- 6) подразделение по работе с персоналом;
- 7) юридическое подразделение;
- 8) подразделение по комплаенс-контролю;
- 9) подразделение внутреннего аудита;
- 10) иные подразделения в рамках исполнения своих должностных обязанностей.

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 управления документацией и записями»;
- 9) Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 20 апреля 2026 года №81 «Об утверждении минимальных требований по обеспечению информационной безопасности на финансовом рынке».

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;

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 13 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

- 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 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) 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 құрамымен қоса барлық қызметкерлер үшін арналған АҚ тақырыбындағы тұрақты тренингтер;

- 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;
- 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) 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;

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 14 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

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 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,

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;
- 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 средств межсетевого экранирования, предотвращения вторжений и защиты веб-приложений;
- 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;

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 15 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

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, талдау, сондай-ақ ақпараттық қауіпсіздік инциденттері туралы ақпаратты жинау, шоғырландыру және сақтау.

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 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. ЖАУАПҚЕРШІЛІК

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 требованиям 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 отчетность высшему руководству Компании.

9. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

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

9.2. Непрерывный мониторинг, выявление угроз, анализ, а также осуществление сбора, консолидации и хранения информации об инцидентах ИБ 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 защищенные каналы связи и механизмы аутентификации для удаленного доступа.

10.3. Проводится контроль за безопасностью веб-ресурсов Компании.

10.4. Регулярно проводится аудит и тестирование защищенности 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. Отчетность 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;

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 16 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

13.1. Компанияның бірінші басшысы Қазақстан Республикасының заңнамасына, қаржы нарығын және қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті органның нормативтік құқықтық актілеріне, сондай-ақ Компанияның ішкі нормативтік құжаттарына сәйкес Компанияның ақпараттық қауіпсіздігін қамтамасыз ету үшін дербес жауапты болады.

13.2. Ақпараттық қауіпсіздік департаменті өзіне жүктелген функциялар мен өкілеттіктер шегінде Компанияның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі іс-шараларды ұйымдастыруды, үйлестіруді, әдіснамалық сүйемелдеуді, мониторингтеуді және бақылауды қамтамасыз етеді.

13.3. Ақпараттық қауіпсіздік бөлімшесінің басшысы осы Саясатты уақтылы өзектендіруге, оған өзгерістер енгізу жөніндегі ұсыныстарды дайындауға, сондай-ақ ақпараттық қауіпсіздіктің өзекті талаптарын мүдделі тараптарға жеткізуді ұйымдастыруға жауапты болады.

13.4. Осы Саясатты келісу мерзімдерінің сақталуына жауапкершілік құжатты әзірлеушіге жүктеледі.

13.5. Осы Саясаттың Компанияның сайтында жариялануына жауапкершілік ақпараттық қауіпсіздік жөніндегі бөлімшенің басшысына жүктеледі.

13.6. Осы Саясатқа өзгерістер және/немесе толықтырулар енгізілген жағдайда ақпараттық қауіпсіздік жөніндегі бөлімше Саясаттың өзекті редакциясын Компанияның ішкі нормативтік құжаттарында белгіленген тәртіппен мүдделі тараптарға жеткізуді, оның ішінде корпоративтік пошта, электрондық құжат айналымы жүйесі, Компанияның корпоративтік порталы не өзге де белгіленген коммуникация арналары арқылы қамтамасыз етеді.

13.7. Әрбір жұмыскер осы Саясатты, ақпараттық қауіпсіздік мәселелері жөніндегі ішкі нормативтік құжаттардың талаптарын сақтауға және ақпараттық қауіпсіздік инциденттерінің алдын алу жөнінде шаралар қабылдауға міндетті. Сондай-ақ ақпараттық жүйелермен және құпия деректермен жұмыс істеу кезінде анықталған барлық күмәнді жағдайлар мен бұзушылықтар туралы өзінің тікелей басшысын және Ақпараттық қауіпсіздік департаментін хабардар етуге міндетті.

13.8. Автоматтандыру департаменті өз құзыреті шегінде және Компанияның ішкі нормативтік құжаттарына сәйкес ақпаратты қорғаудың техникалық шараларын іске асыруды, цифрлық инфрақұрылымды, цифрлық жүйелерді, цифрлық ресурстарды, есептеу техникасы құралдарын, желілік жабдықты, серверлік инфрақұрылымды және өзге де техникалық компоненттерді сүйемелдеуді қамтамасыз етеді.

13.9. Бизнес-процестердің иелері және цифрлық жүйелердің иелері өз құзыреті шегінде өздеріне бекітілген бизнес-процестер мен цифрлық жүйелердің ақпараттық қауіпсіздігін қамтамасыз етуге қатысады, оның ішінде қол жеткізуге қойылатын талаптарды айқындайды, пайдаланушылардың қол жеткізу құқықтарын беруді, өзгертуді және тоқтатуды келіседі,

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

13.1. Первый руководитель Компании несет персональную ответственность за обеспечение информационной безопасности Компании в соответствии с законодательством Республики Казахстан, нормативными правовыми актами уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организации, а также внутренними нормативными документами Компании.

13.2. Департамент информационной безопасности обеспечивает организацию, координацию, методологическое сопровождение, мониторинг и контроль мероприятий по обеспечению информационной безопасности Компании в пределах, возложенных функции и полномочий.

13.3. Руководитель подразделения информационной безопасности несет ответственность за своевременную актуализацию настоящей Политики, подготовку предложений по ее изменению, а также организацию доведения актуальных требований информационной безопасности до заинтересованных сторон.

13.4. Ответственность за соблюдение сроков согласования настоящей Политики возлагается на разработчика документа.

13.5. Ответственность за публикацию настоящей Политики на сайте Компании несёт руководитель подразделения информационной безопасности.

13.6. В случае внесения изменений и/или дополнений в настоящую Политику подразделения информационной безопасности обеспечивает доведение актуальной редакции Политики до заинтересованных сторон в порядке, установленном внутренними нормативными документами Компании, в том числе посредством корпоративной почты, системой электронного документооборота корпоративного портала Компании, либо иных установленных каналов коммуникации.

13.7. Каждый работник обязан соблюдать настоящую Политику, требования внутренних нормативных документов по вопросам информационной безопасности и принимать меры для предотвращения инцидентов информационной безопасности. Также обязан извещать своего непосредственного руководителя и Департамент информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 17 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

цифрлық жүйелерді сыныптауға, ақпараттық қауіпсіздік тәуекелдерін бағалауға және түзету іс-шараларын іске асыруға қатысады.

13.10. Компанияның құрылымдық бөлімшелерінің басшылары ақпараттық қауіпсіздік талаптарымен таныстыруды қамтамасыз етеді және өздері басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін дербес жауапты болады, сондай-ақ анықталған бұзушылықтар, инциденттер немесе ақпараттық қауіпсіздік тәуекелдері туралы Ақпараттық қауіпсіздік департаментін уақтылы хабардар етуге міндетті.

13.11. Осы Саясаттың қағаз жеткізгіштегі түпнұсқасын сақтауға және Саясаттың электрондық көшірмесін корпоративтік порталда орналастыруға жауапкершілік Әдіснама және СМЖ бөлімшесінің басшысына жүктеледі.

13.12. Осы Саясаттың талаптарын бұзуға кінәлі Компания жұмыскерлері, мердігерлер, қызмет көрсетушілер және өзге де үшінші тұлғалар Қазақстан Республикасының заңнамасына, еңбек шарттарына, азаматтық-құқықтық сипаттағы шарттарға, құпиялылық туралы келісімдерге, қызмет көрсету туралы шарттарға және ішкі нормативтік құжаттарға сәйкес жауапты болады.

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

информационными системами и конфиденциальными данными.

13.8. Департамент автоматизации обеспечивает реализацию технических мер защиты информации, сопровождение цифровой инфраструктуры, цифровых систем, цифровых ресурсов, средств вычислительной техники, сетевого оборудования, серверной инфраструктуры и иных технических компонентов в пределах своей компетенции и в соответствии с внутренними нормативными документами Компании.

13.9. Владельцы бизнес-процессов и владельцы цифровых систем в пределах своей компетенции участвуют в обеспечении информационной безопасности закрепленных за ними бизнес-процессов и цифровых систем, в том числе определяют требования к доступу, согласовывают предоставления, изменение и прекращение прав доступа пользователь, участвуют в классификации цифровых систем, оценке рисков информационной безопасности и реализации корректирующих мероприятий.

13.10. Руководители структурных подразделений Компании обеспечивает ознакомление с требованиями к информационной безопасности и несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях, а также своевременное информирование Департамента информационной безопасности о выявленных нарушениях, инцидентах или рисках информационной безопасности.

13.11. Ответственность за хранение оригинала настоящей Политики на бумажном носителе и размещение электронной копии Политики на корпоративном портале несёт руководитель подразделения Методологии и СМК.

13.12. Работники Компании, подрядчики, поставщики услуг и иные третьи лица, виновные в нарушении требований настоящей Политики, несут ответственность в соответствии с законодательством Республики Казахстан, трудовым договором, договорами гражданско-правового характера, соглашениями о конфиденциальности, договорами об оказании услуг и внутренними нормативными документами.

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.

Insurance Nomad	Политика информационной безопасности И-23	Издание: 8 от «17» сентября 2026г.	Стр. 18 из 18
		Взамен издания: 7 от «06» февраля 2026г.	

Республикасының нормативтік құқықтық актілерін басшылыққа алады.

14.5. Внесение изменений и дополнений в Политику осуществляется согласно нормам «Процедуры управления документацией и записями».

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

14.7. Электронная версия Политики размещается на корпоративном портале 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.