Утверждено
Решением Совета Директоров
АО «НК «QazaqGaz»
№ 7/22 от «__» _____ 2023 год

ПОЛИТИКА
информационной безопасности АО «НК «QazaqGaz»

Экземпляр _____

г. Астана 2023 г.

Предисловие

Введен: Вводится взамен 10-03-2016 «Политика информационной безопасности АО «КазТрансГаз».

Дата пересмотра: 2028 г.

Содержание

1. Назначение и область применения

1.1. Политика информационной безопасности (далее - Политика) выражает отношение (подход) АО «НК «QazaqGaz» (далее - Общество) к обеспечению защиты информации в рамках своей деятельности. Информационная безопасность является одним из критичных факторов успешной и стабильной работы Общества.

1.2. Политика является основополагающим документом, отражающим видение руководства Общества касательно обеспечения информационной безопасности.

1.3. Цель настоящей Политики заключается в определении цели, направления, принципов и основных правил для управления информационной безопасностью.

1.4. Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам Общества. С этой целью необходимо поддерживать основные свойства информации: Конфиденциальность, Доступность, Целостность.

1.5. Процесс создания надежной информационной защиты не может быть законченным. В целях обеспечения информационной безопасности, необходимо постоянное регулирование ее параметров, адаптация для отражения новых угроз, исходящих из внешней и внутренней среды.

1.6. Не должно существовать каких-либо препятствий при внесении изменений в Политику, процедуры и прочие документы по информационной безопасности по мере возникновения такой необходимости.

1.7. Требования Политики обязательны к исполнению всеми сотрудниками Общества.

2. Нормативные ссылки

В Политике использованы ссылки на следующие нормативные документы:

- Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации» №418-V;
- Постановление Правительства РК от 20 декабря 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
- Документированная процедура «Общие требования к разработке, оформлению и изложению внутренних регламентирующих документов АО «НК «QazaqGaz» (ДП-01);
- Стандарт СТ РК ISO/IEC 27001 разделы 5.2 и 5.3.
- Корпоративный стандарт безопасности АО ФНБ «Самрук-Казына», протокол №46/18 от 26.12.2018 года.

3. Термины и определения

3.1. В настоящей Политике применяются термины и соответствующие им определения в соответствии с Таблицей 1.

Таблица 1.

Термины	Определения
Доступность	характеристика информации, означающая, что эта информация и соответствующие физические и логические ресурсы доступны авторизованным лицам по мере необходимости, когда необходима и там где необходима.

ИБ	информационная безопасность – процесс обеспечения конфиденциальности, целостности и доступности информации;
ИС	информационная система - совокупность всех серверов и клиентов, сетевой инфраструктуры, системного и прикладного программного обеспечения, данных и иных компьютерных подсистем, а также компонентов, которые являются объектом владения и используются Обществом или за которые Общество несет ответственность. В использование информационных систем также входит использование всех внутренних и внешних сервисов, таких как доступ к интернету, электронной почте и т.д.;
Ответственное структурное подразделение	структурное подразделение Общества, отвечающее за разработку и управление Политикой, занимающихся вопросами в области информационной безопасности.
Информационные активы	информация и соответствующие физические и логические ресурсы с реквизитами, позволяющими ее идентифицировать; имеющая ценность для Общества; находящаяся в распоряжении Общества и представленная на любом материальном или цифровом носителе в пригодной для ее обработки, хранения или форме передачи.
Конфиденциальность	характеристика информации, означающая, что эта информация доступна только авторизованным лицам или системам;
Мобильное устройство	переносное электронно-вычислительное устройство, способное принимать, отображать, хранить, обрабатывать и передавать информацию (ноутбук, планшет, USB накопитель и переносной жесткий диск).
Носитель информации	любой материальный объект, используемый для хранения и передачи электронной информации.
СУИБ	система управления информационной безопасностью – часть общих процессов управления, которая относится к планированию, внедрению, поддержанию, пересмотру и улучшению информационной безопасности.
Контролируемая зона	территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств без постоянного или разового допуска.
Целостность	свойство информации, характеризующее точность и надежность информации, источника или системы

4. Сокращения и обозначения

4.1. В настоящей Политике применены следующие обозначения и сокращения в соответствии с Таблицей 2.

Таблица 2.

№ п/п	Обозначения и сокращения	Расшифровка приведенных сокращений и обозначений
1.	Общество	Акционерное общество «НК «QazaqGaz»
2.	ВНД	Внутренние нормативные документы
3.	ДП-01	Документированная процедура «Общие требования к разработке, оформлению и изложению внутренних регламентирующих документов АО «НК «QazaqGaz»
4.	ДКБ	Департамент по корпоративной безопасности
5.	ДИТ	Департамент информационных технологий

5. Ответственность и полномочия

5.1. Руководство Общества принимает на себя ответственность за реализацию настоящей Политики.

5.2. Руководители и работники Общества несут ответственность за безусловное полное выполнение своих обязанностей по поддержанию деятельности по обеспечению и

выполнению требований ИБ, а представители третьих сторон, имеющие доступ к информационным ресурсам Общества - в соответствии с договорными обязательствами.

5.3. Специалист ИБ отвечает за координацию, контроль исполнения и актуальность настоящей Политики, а также за отчёт о функционировании СУИБ перед руководством Общества;

5.4. Ответственным за разработку и управление Политикой является ответственное структурное подразделение Общества.

5.5. Ответственность за правильное применение требований Политики несет каждый сотрудник Общества.

5.6. Ответственность за рассылку Политики возлагается на ответственное структурное подразделение Общества.

5.7. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами Общества и законодательством Республики Казахстан.

6. Управление информационной безопасностью

6.1. Информация, созданная с помощью или хранящаяся на программно-аппаратных средствах Общества, принадлежит Обществу. Управление информационной безопасностью Общества заключается в планировании, развертывании и поддержании комплекса регламентов и процедур, а также применение программно-аппаратных средств, направленных на минимизацию рисков нарушения информационной безопасности.

Цели и система мер

6.1.1 Главной целью СУИБ Общества является снижение вероятности нанесения материального, физического, репутационного или иного ущерба Общества, его партнёрам и клиентам в результате реализации угроз информационной безопасности.

6.1.2 Осуществление в установленном порядке сбора, обработки, анализа информации по вопросам безопасности, согласно Перечню и своевременное информирование руководства Общества.

6.1.3 Указанная цель достигается посредством решения задач по обеспечению и постоянному поддержанию следующего состояния информационных ресурсов и сервисов:

1) конфиденциальность информации Общества, сотрудников, клиентов и партнёров (в том числе персональные данные);

2) безопасность предоставляемых Обществом сервисов для инфраструктуры его клиентов, своевременное информирование их, о нарушениях работы сервисов и своевременное восстановление их (сервисов) работы;

3) обеспечение высокой доступности всех внутренних и внешних (предоставляемых клиентам и партнёрам) информационных активов Общества.

Требования информационной безопасности

6.2.1. В целях защиты перечисленных ценностей Общество осуществляет деятельность по управлению информационной безопасностью, основными принципами которой являются:

1) Вовлеченность каждого сотрудника Общества в процесс обеспечения информационной безопасности. Деятельность по обеспечению информационной безопасности инициирована и контролируется руководством Общества.

2) Реагирование на инциденты ИБ. Общество стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения ИБ;

3) Осведомлённость в вопросах обеспечения ИБ. Требования в области ИБ доводятся до сведения работников Общества и контрагентов в части их касающейся. С целью обеспечения свободного доступа всех заинтересованных сторон к настоящей Политике, ее текст размещается на корпоративном сайте Общества;

4) Компетентность персонала. Общество тщательно производит процедуру найма работников, повышает квалификацию, вырабатывает и поддерживает корпоративную этику, что создаёт благоприятную среду для деятельности Общества и снижает риски ИБ. Общество на периодической основе осуществляет информирование и обучение работников по вопросам обеспечения ИБ;

5) Учёт действий с информационными активами. Общество стремится вести учёт, инвентаризацию и категоризацию информационных активов, а такжевсех действий работников Общества и контрагентов с информационными активами Общества;

6) Учёт требований ИБ в проектной деятельности. Общество учитывает требования ИБ в проектной деятельности. Разработка и документирование требований по обеспечению ИБ осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации;

7) Персональная ответственность. Работники Общества несут персональную ответственность за соблюдение требований ИБ. Обязанности по обеспечению ИБ включаются в трудовые договоры и должностные инструкции работников, а также в договоры с контрагентами.

8) Управление корпоративными рисками. Управленческие решения в Обществе (в том числе и в области ИБ) принимаются на основании результатов оценки рисков, выполненной в рамках разработанного и внедрённого в Обществе внутреннего процесса принятия решения с учетом рисков.

9) Согласованность действий и решений по обеспечению ИБ с поставленными стратегическими целями Общества. Деятельность по обеспечению ИБ учитывает контекст управления стратегическими рисками.

10) Соответствие законодательным и нормативным актам Республики Казахстан, требованиям внешних регуляторов и договоров с контрагентами. Общество реализует меры обеспечения ИБ в строгом соответствии с действующим законодательством Республики Казахстан и договорными обязательствами;

11) Функционирование системы обеспечения информационной безопасности строится в соответствии с применимыми требованиями стандартов Республики Казахстан, международных стандартов.

12) Экономическая целесообразность. Общество стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.

13) Документированность требований информационной безопасности. Общества стремится, чтобы все требования в области информационной безопасности, сбор, консолидация и хранения информации об инцидентах ИБ были зафиксированы во внутренних нормативных документах, утвержденных руководством Общества.

14) Предоставление минимально необходимых прав доступа. Работникам Общества и контрагентам предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств. При этом Общество стремится предоставлять права доступа таким образом, чтобы выполнение особо важной (критичной) операции осуществлялось с участием как минимум двух работников.

Средства управления информационной безопасностью

6.3.1. Основными мерами по обеспечению информационной безопасности Общества являются:

1) **Административно-правовые и организационные меры включают:**

– контроль исполнения требований Законодательства РК и внутренних документов;

– разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;

– контроль соответствия бизнес-процессов требованиям Политики;

– информирование и обучение работников Общества работе с информационными системами и требованиям информационной безопасности;

– реагирование на инциденты, локализацию и минимизацию последствий;

– анализ рисков информационной безопасности;

– отслеживание и улучшение морального и делового климата в коллективе;

– определение действий при возникновении чрезвычайных ситуаций;

– проведение профилактических мер при приеме на работу и увольнении работников Общества.

2) **Меры физической безопасности включают:**

– организацию пропускного и внутриобъектового режимов;

– построение периметра безопасности защищаемых объектов;

– организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;

– организацию противопожарной безопасности охраняемых объектов;

– контроль доступа работников Общества в помещения ограниченного доступа.

3) Программно-технические меры включают:

– использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

– использование средств защиты периметра;

– применение комплексно антивирусной защиты;

– использование средств информационной безопасности, встроенных в информационные системы;

– обеспечение регулярного резервного копирования информации;

– контроль за правами и действиями всех пользователей информационных активов Общества;

– применение систем криптографической защиты информации;

– обеспечение безотказной работы аппаратных средств;

– мониторинг состояния критичных элементов информационной системы.

Непрерывность бизнеса

6.4.1. В Обществе внедрен процесс аварийного восстановления с целью снижения убытков, вызываемых авариями и сбоями в информационных системах Общества до приемлемого уровня путем комбинирования предупреждающих и корректирующих мер.

6.4.2. В Обществе разработаны и реализованы планы, которые позволят восстановить операции основных бизнес-процессов и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя. Планы аварийного восстановления должны регулярно тестироваться и пересматриваться.

6.4.3 Обеспечение непрерывности бизнеса в Обществе направлены на снижение влияния чрезвычайной ситуации на жизнь и здоровье работников Общества, минимизацию влияния на клиентов, сохранение активов, оценку влияния чрезвычайной ситуации на деятельность Общества с целью ее скорейшего восстановления.

Поддержка внедрения СУИБ

6.5.1.В Обществе поддерживаются регулярные проведения следующих мероприятий:

1) выявление возможности улучшения СУИБ;

2) принятие необходимых корректирующих и предупреждающих действий, использование на практике опыт по обеспечению ИБ, полученный как в собственном Обществе, так и в других организациях;

3) передача подробной информации о действиях по улучшению СУИБ всем заинтересованным сторонам, при этом степень ее детализации соответствует обстоятельствам и, при необходимости, согласовываются дальнейшие действия;

4) обеспечение внедрения улучшений СУИБ для достижения запланированных целей.

6.5.2. Для предоставления свидетельств соответствия требованиям и результативности функционирования СУИБ введены и поддерживаются в рабочем состоянии учетные записи и записи о выполнении процессов.

6.5.3. Руководство Общества ответственно за обеспечение и управление ресурсами, необходимыми для создания СУИБ, а также организацию подготовки персонала.

6.5.4. На ежегодной основе проводится аудит, в том числе аудит информационных систем для соответствия фактической деятельности Общества положениям настоящей Политики, а также контроль достигнутых целей Политики, установленных в соответствующем разделе настоящей Политики. По результатам мониторинга в Политику могут вноситься изменения с целью улучшения системы управления информационной безопасности.

Контроль доступа к информационным ресурсам

6.6.1. Все работы в пределах офиса выполняются в соответствии с официальными должностными обязанностями только на компьютерах и мобильных устройствах (кроме сотовых телефонов), разрешенных к использованию в Обществе.

6.6.2. Руководители подразделений должны периодически пересматривать права доступа своих работников и других пользователей к соответствующим информационным ресурсам.

6.6.3. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и запись каждого входа в систему должна сохраняться в централизованном журнале.

6.6.4. Все работники Общества должны соблюдать «Правила «чистого стола» и «чистого экрана» АО «НК «QazaqGaz».

6.6.5. Работникам запрещается:

- подключать к сети Общества неавторизованные устройства за исключением беспроводной сети, предоставляемой для гостевого доступа
- нарушать информационную безопасность и работу сети;
- использовать в работе незарегистрированные в ДИТ (по согласованию с ДКБ) носители информации (флэшки, ноутбуки и т.д.), для несанкционированного изъятия информации с персональных компьютеров;

- использовать, изменять или передавать информационные активы Общества третьей стороне без согласования Общества;

- осуществлять действия с использованием программно-аппаратных средств Общества, которые противоречат политикам Общества или нарушают законодательство РК;

- при работе на удаленном доступе, за пределами «контролируемой зоны», передавать информацию и ознакамливать с содержимым документов «третьих» лиц;

6.6.6. Все выданные и отозванные права удаленного доступа регистрируются ответственным работником ДИТ в Журнале учета предоставления удаленного доступа пользователям, согласно Правилам по предоставлению удаленного доступа к информационным системам.

6.6.7. Удаленный доступ пользователей к ИС Общества обеспечивается на основе учетных записей, с использованием технологии VPN.

6.6.8. Внос на территорию Общества мобильных устройств и носителей информации работниками, а также вынос их за его пределы, производится при направлении электронной заявки руководителя подразделения в ДИТ, с согласованием ДКБ, согласно следующим правилам:

–работники и подрядчики, имеющие разрешение на внос/вынос мобильных устройств и носителей информации, должны быть идентифицированы;

–устанавливаются предельные сроки вноса/выноса мобильных устройств и носителей информации;

–внос/вынос мобильных устройств и оборудования, фиксируются в Журнале вноса/выноса мобильных устройств и оборудования согласно Правилам использования мобильных устройств и носителей информации.

6.6.9. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

7. Записи

В настоящей Политике отсутствуют записи, которые должны управляться в соответствии с требованиями документированной процедуры ДП-02 «Управление записями».

8. Пересмотр, внесение изменений, хранение и рассылка

8.1. Политика пересматривается в случае существенных изменений в развитии бизнеса, а также требований законодательства Республики Казахстан или регулирующих органов.

8.2. Пересмотр, внесение изменений, хранение и рассылка настоящей Политики осуществляются в соответствии с требованиями документированной процедуры ДП-02 «Управление документацией».

8.3. «Оригинал» в бумажном виде настоящей документированной процедуры оформляется и хранится в ИСМ Общества.

8.4. Сканированная версия настоящей документированной процедуры размещается в базе данных ВНД Общества.

Лист согласования

Должность	Ф.И.О	Подпись	Дата
Директор Департамента по корпоративной безопасности	Калилуллов А.К.		
Директор Департамента внутреннего контроля и управления рисками	Досов К.Б.		
Руководитель Службы комплаенс	Молдагалиева Г.Ж.		
Главный менеджер Юридического департамента	Жансарин А.Г.		
Директор Департамента маркетинга	Несонов Е.Г.		
Директор Департамента ценовой политики и мониторинга	Бектурова А.Т.		
Директор Департамент по переработке сырого газа	Джилкайдаров Ж.А.		
Директор Департамента информационных технологий	Еркенов Е.А.		
Директор Департамент корпоративного финансирования и казначейства	Круз Д.О.		
Зам. Главного бухгалтера Центральной бухгалтерии	Бокаев Е.Н.		
Директор Департамента бюджетного планирования	Мареков А.С.		
Директор Департамента по инвестиционным проектам и международному сотрудничеству	Аллаярбек Ж.А.		
И.о. Директора Департамент стратегии и устойчивого развития	Агимбетова Л.Е.		
Директор Департамента управления активами	Саткалиев А.М.		
Директор Департамента по перспективным проектам и геологоразведке	Супыгалиев А.И.		
Директор Департамента по добыче	Казиев Н.М.		
Директор Производственно-технического департамента	Жолаев Ш.С.		
Директор Департамента управления бизнес-процессами	Ибраимов Н.А.		
Директор Департамента диспетчеризации	Кусайнов Ж.У.		

Ознакомлен, п. МСФО нет
Умий

Главный менеджер Департамента по управлению человеческими ресурсами и оплате труда	Жусупова А.Е.		
Директор Департамент закупок и местного содержания	Сембай А.К.		
Руководитель пресс-службы	Тулегенов М.Ж.		
Директор Административного департамента	Ахметалиев А.Х.		
Директор Департамента сводно-аналитической работы и протокола	Бекмухамбетова А.А.		
Директор департамента Службы HSE	Джакубалиев А.К.		
Руководитель службы внутреннего аудита	Баймурзин Р.К.		

Лист регистрации изменений

Номер изменения	Номера страниц	Всего листов в документе	Номера разделов, к которым относятся изменения	Описание изменений	Отметка о внесении изменений		
					Ф.И.О.	Подпись	Дата

Лист ознакомления

№ п/п	Ф.И.О	Должность	Подпись	Дата
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				