Бекітілген
Бас директордың бұйрығымен
«ҚазМұнайГаз-Аэро» ЖШС

«27» ақпан 2024 ж.

№18-ОД

«ҚазМұнайГаз-Аэро» ЖШС-нің ақпараттық қауіпсіздік саясаты

Астана қ.

МАЗМҰНЫ

1. Жалпы ережелер

1.1. Осы «ҚазМұнайГаз-Аэро» ЖШС-нің ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «ҚазМұнайГаз-Аэро» ЖШС (бұдан әрі – Серіктестік) күнделікті қызмет процесінде басшылыққа алатын ақпараттың қорғалуын қамтамасыз ету саласындағы мақсаттарды, міндеттерді және тәсілдерді белгілейді.

1.2. Саясат Серіктестіктің Бас директорының ақпараттық қауіпсіздікті қамтамасыз етуге қатысты көзқарасын көрсететін іргелі құжат болып табылады.

2. Негізгі мақсаттар мен міндеттер

2.1. Саясат келесі мақсаттарға жетуге бағытталған:

2.1.1. ақпаратты нақты және ықтимал қауіптерден қорғауға;

2.1.2. қауіп-қатерге ұшыраған кезде салдарды азайтуға және оқшаулауға;

2.1.3. ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мәдениетті дамытуға;

2.2. Саясаттың негізгі міндеттері болып табылады:

2.2.1. ақпараттық қауіпсіздіктің нақты және ықтимал қатерлерін анықтау, алдын алу және бейтараптандыру, сондай-ақ олардың пайда болу себептері мен жағдайларын анықтау;

2.2.2. ақпараттық қауіпсіздік қатерлеріне жедел ден қою тетіктерін жетілдіру

2.2.3. ақпараттық қауіпсіздік тәуекелдерін тиімді басқару;

2.2.4. Серіктестік қызметкерлерін ақпараттық қауіпсіздік мәселелері бойынша ақпараттандыру, оқыту, білімдерін бақылау;

2.2.5. маңызды ақпараттық ресурстардың құпиялылығын сақтау;

2.2.6. бизнес-қызметті қолдау үшін Серіктестіктің ақпараттық ресурстарына қолжетімділіктің үздіксіздігін қамтамасыз ету;

2.2.7. Серіктестіктің жоғары сапалы қызмет көрсету және тиімді басқару шешімдерін қабылдау мүмкіндіктерін қолдау мақсатында іскерлік ақпараттың тұтастығын қорғау;

2.2.8. Серіктестіктің ақпараттық ресурстарына байланысты қауіптер саласында пайдаланушылардың хабардарлығын арттыру;

2.2.9. Серіктестікте ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметкерлердің жауапкершілік дәрежесін және міндеттерін айқындау;

2.2.10. ақпараттық қауіпсіздік саласындағы бұзушылықтардан болатын ықтимал шығындар мен залалды азайту.

3. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы қызметтің негізгі қағидаттары

3.1. Серіктестікте ақпараттық қауіпсіздікті қамтамасыз ету мынадай негізгі қағидаттарға сәйкес жүзеге асырылады:

3.1.1. заңдылыққа;
3.1.2. процесс тәсіліне;
3.1.3. қорғау әдістерін, әдістері мен құралдарын кешенді пайдалануға;
3.1.4. үздік тәжірибелерді ұстануға;
3.1.5. ақылға қонымды жеткіліктілікке;
3.1.6. жеке жауапкершілікке.

4. Ақпараттық қауіпсіздікті басқару

4.1. Аталған мақсаттарға қол жеткізу үшін Қазақстан Республикасы заңнамасының талаптарына, Серіктестіктің нормативтік және шарттық міндеттемелеріне сәйкес келетін ақпараттық қауіпсіздікті басқару жүйесі пайдаланылады.

4.2. Серіктестіктің ақпараттық қауіпсіздігін басқару жүйесі осы Саясатта, ережелерде, рәсімдерде және Серіктестіктің барлық қызметкерлері орындауға міндетті болып табылатын жұмыс нұсқаулықтарында құжатталған. Осы жүйенің құжатталған талаптары Серіктестік қызметкерлерінің назарына жеткізіледі.

4.3. Серіктестіктің барлық ақпараттық активтері, соның ішінде бағдарламалық қамтамасыз ету, қағаз және электрондық жеткізгіштердегі ақпараттық ресурстар, персонал, олардың маңыздылығы мен қолжетімділік дәрежесіне сәйкес есепке алынуға және санатталуға жатады.

4.4. Белгіленген рәсімдерге сәйкес ақпараттық қауіпсіздікке төнетін қатерлерді тұрақты бағалау жүзеге асырылады. Оны жүргізу кезінде қауіптердің ықтималдығы және олардың бизнес-процестерге, Серіктестіктің қаржылық жағдайына және іскерлік беделіне әсер ету дәрежесі ескеріледі.

4.5. Ақпараттық қауіпсіздікке төнетін қатерлерді бағалау нәтижелері бойынша ұйымдастырушылық, физикалық, техникалық, бағдарламалық және бағдарламалық-аппараттық құралдарды қоса алғанда, ақпаратты қорғау үшін басқару құралдары таңдалады және қолданылады.

4.6. Серіктестіктің ақпараттық активтерін физикалық қорғауды қамтамасыз ету үшін ақпараттық қауіпсіздік жүйесінің әрекет ету шекараларында қауіпсіздік аймақтары белгіленеді және рұқсатсыз кіруді болғызбау жөнінде шаралар қабылданады.

4.7. Серіктестік белгіленген рәсімдерге сәйкес ақпараттық қауіпсіздік саласындағы оқиғаларды анықтауға, ескеруге және оларға ден қоюға ұмтылады.

4.8. Серіктестік қызметкерлері өздерінің функционалдық міндеттерін орындау үшін қажетті ақпаратқа қол жеткізе алады. Серіктестік ақпараттық қауіпсіздік саласындағы қызметкерлерді ақпараттандыруды, оқытуды және олардың біліктілігін арттыруды жүргізеді.

5. Жауапкершілік

5.1. Серіктестіктің басшылығы инормациялық қауіпсіздікті жалпы басқаруды жүзеге асырады және мыналар үшін қажетті жағдайларды қамтамасыз етеді:

5.1.1. инормациялық қауіпсіздік және ақпаратты қорғау қатерлерін бағалау жөніндегі іс-шараларды іске асыруды;

5.1.2. ақпараттық қауіпсіздікті басқару жүйесін қолдау, Бақылау, талдау және үздіксіз жетілдіруді;

5.1.3. Серіктестік қызметкерлерін ақпараттық қауіпсіздік саласында тұрақты оқытуды.

5.2. Серіктестік қызметкерлері ақпараттық қауіпсіздік құжаттары талаптарының сақталуына дербес жауапты болады және Серіктестік қауіпсіздік тобы басшысының ақпараттық қауіпсіздік саласындағы барлық бұзушылықтар туралы хабардар етуге міндетті.

5.3. Серіктестік қызметкерлерінің еңбек шарттары мен лауазымдық нұсқаулықтарында қызметтік құжаттаманың сақталуына және өз міндеттерін орындауға байланысты белгілі болған ақпараттың құпиялылығына жауапкершілік белгіленеді.

6. Қорытынды ережелер

6.1. Серіктестіктің ақпараттық қауіпсіздік саясаты барлық мүдделі тараптарға ұсынылуы және Серіктестіктің ресми веб-сайтында орналастырылуы мүмкін жалпыға қолжетімді құжат болып табылады.

6.2. Саясат бизнесті дамытуда, сондай-ақ Қазақстан Республикасы заңнамасының немесе реттеуші органдардың талаптарында елеулі өзгерістер болған жағдайда қайта қаралады. Саясат, сондай-ақ ондағы барлық өзгерістер Серіктестіктің Бас директорының бұйрығымен бекітіледі.

Утверждена
приказом Генерального директора
ТОО «КазМунайГаз-Аэро»
от «27» февраля 2024 года
№ 18-OD

Политика информационной безопасности в ТОО «КазМунайГаз–Аэро»

г. Астана

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая Политика информационной безопасности ТОО «КазМунайГаз–Аэро» (далее - Политика) устанавливает цели, задачи и подходы в сфере обеспечения защищенности информации, которым ТОО «КазМунайГаз–Аэро» (далее – Товарищество) руководствуется в процессе повседневной деятельности.

1.2. Политика является основополагающим документом, отражающим видение Генерального директора Товарищества касательно обеспечения информационной безопасности.

2. Основные цели и задачи

2.1. Политика направлена на достижение следующих целей:

2.1.1. защита информации от реальных и потенциальных угроз;

2.1.2. минимизация и локализация последствий при воздействии угроз;

2.1.3. развитие культуры в области обеспечения информационной безопасности;

2.2. Основными задачами Политики являются:

2.2.1. выявление, предупреждение и нейтрализация реальных и потенциальных угроз информационной безопасности, а также установление причин и условий их возникновения;

2.2.2. совершенствование механизмов оперативного реагирования на угрозы информационной безопасности;

2.2.3. эффективное управление рисками информационной безопасности;

2.2.4. информирование, обучение, контроль знаний работников Товарищества по вопросам информационной безопасности;

2.2.5. сохранение конфиденциальности критичных информационных ресурсов;

2.2.6. обеспечение непрерывности доступа к информационным ресурсам Товарищества для поддержки бизнес-деятельности;

2.2.7. защита целостности деловой информации, с целью поддержания возможностей Товарищества по оказанию услуг высокого качества и принятию эффективных управленческих решений;

2.2.8. повышение осведомленности пользователей в области угроз, связанных с информационными ресурсами Товарищества;

2.2.9. определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в Товариществе;

2.2.10. минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

3. Основные принципы деятельности в сфере обеспечения информационной безопасности

3.1. Обеспечения информационной безопасности в Товариществе осуществляется в соответствии со следующими основными принципами:

3.1.1. законности;

3.1.2. процессного подхода;

3.1.3. комплексного использования способов, методов и средств защиты;

3.1.4. следования лучшим практикам;

3.1.5. разумной достаточности;

3.1.6. персональной ответственности.

4. Управление информационной безопасностью

4.1. Для достижения указанных целей используется система управления информационной безопасностью, соответствующая требованиям законодательства Республики Казахстан, нормативным и договорным обязательствам Товарищества.

4.2. Система управления информационной безопасностью Товарищества документирована в настоящей Политике, правилах, процедурах и рабочих инструкциях, которые являются обязательными для исполнения всеми работниками Товарищества. Документированные требования данной системы доводятся до сведения работников Товарищества.

4.3. Все информационные активы Товарищества, включая программное обеспечение, информационные ресурсы на бумажных и электронных носителях, персонал, подлежат учету и категорированию в соответствии с их важностью и степенью доступа.

4.4. В соответствии с установленными процедурами, осуществляется регулярная оценка угроз информационной безопасности. При ее проведении учитывается вероятность угроз и степень их влияния на бизнес-процессы, финансовое состояние и деловую репутацию Товарищества.

4.5. По результатам оценки угроз информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения.

4.6. Для обеспечения физической защиты информационных активов Товарищества, в границах действия системы информационной безопасности, устанавливаются зоны безопасности и принимаются меры по предотвращению неавторизированного доступа.

4.7. Товарищество стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

4.8. Работники Товарищества получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей. Товарищество проводит

информирование, обучение и повышение квалификации работников в сфере информационной безопасности.

5. Ответственность

5.1. Руководство Товарищества осуществляет общее управление инормационной безопасностью и обеспечивает необходиимые условия для:

5.1.1. реализации мероприятий по оценке угроз инормационной безопасностти и защиты информации;

5.1.2. поддержания, мониторинга, анализа и непрерывного улучшения сиистемы управления информационной безопасности;

5.1.3. регулярного обучения работников Товарищества в сфере иинформационной безопасности.

5.2. Работники Товарищества несут персональную ответственность за соблюдение требований документов информационной безопасности и обязаны информировать обо всех вывленных нарушениях в области информационной безопасности руководителя группы безопасности Товарищества.

5.3. В трудовых договорах и должностных инструкциях работников Товарищества устанавливается ответственность за сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения своих обязанностей.

6. Заключительные положения

6.1. Политика информационной безопасности Товарищества является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещаться на официальном веб-сайте Товарищества.

6.2. Политика пересматривается в случае существенных изменений в развитии бизнеса, а также требований законодательства Республики Казахстан или регулирующих органов. Политика, а также все изменения в ней утверждаются приказом Генерального директора Товарищества.