Утверждена решением Совета Директоров
ЧКОО «КМГ Кашаган Б.В.»
от «18» октября 2024г.

Политика информационной безопасности ЧКОО «КМГ Кашаган Б.В.»

Обеспечение информационной безопасности (ИБ) является одним из приоритетных направлений в рамках реализации Миссии, достижения Видения и стратегических целей ЧКОО «КМГ Кашаган Б.В.». В этих целях ЧКОО «КМГ Кашаган Б.В.» внедряет и поддерживает систему управления информационной безопасности (СУИБ).

1. ЦЕЛЬЮ настоящей Политики является всесторонняя защита интересов ЧКОО «КМГ Кашаган Б.В.», ее филиала в РК, его работников, а также контрагентов от угроз в области информационно-коммуникационных технологий, в том числе посредством обеспечения и постоянного поддержания следующего состояния корпоративной вычислительной сети:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование локально-вычислительной сети;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой на средствах вычислительной техники и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в локально-вычислительной сети и передаваемой по каналам связи.

2. ЗАДАЧАМИ настоящей Политики являются:

- защита от вмешательства посторонних лиц в процесс функционирования локально-вычислительной сети;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и при необходимости криптографическими средствами защиты, используемыми в локально-вычислительной сети;
- регистрация действий пользователей при использовании ресурсов локально-вычислительной сети в системных журналах;
- периодический контроль корректности действий пользователей системы путем анализа содержимого журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения, удаления;
- контроль целостности используемых программных средств, а также защита системы от внедрения вредоносных кодов, включая компьютерные вирусы;
- защита коммерческой тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче, в том числе по каналам связи;
- обеспечение аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз ИБ, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы ИБ и негативные тенденции;
- создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- а также иные задачи, определенные применимыми нормами Королевства Нидерландов, законодательства Республики Казахстан, включая Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации», постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения ИБ», стандартами СУИБ ISO/IEC 27001, СТ РК ISO/IEC 27001 и СТ РК ISO/IEC 27002, а также Корпоративным стандартом информационной безопасности АО «Самрук-Казына» (протокол 40/24 от 25.07.2024 г.).

ПРИНЦИПАМИ настоящей Политики являются:

- ❖ содействие достижению бизнес-целей Компании;
- ❖ предотвращение рисков и угроз в области ИБ Компании;
- ❖ обеспечение конфиденциальности, доступности и целостности информационных активов Компании;
- ❖ соответствие международным стандартам в области ИБ;
- ❖ обеспечение непрерывности функционирования СУИБ Компании.

Настоящая Политика служит основой для обеспечения режима и руководством при разработке правил, методик, регламентов и инструкций в области ИБ.

Руководство Компании берет на себя ответственность за организацию обеспечения ИБ в Компании, декларирует свою приверженность вышеуказанным целям, задачи и принципам.

Все Работники Компании обязаны выполнять требования настоящей Политики и обеспечивать ИБ в рамках своей деятельности. Работники Компании обязаны информировать своих непосредственных руководителей и представителей подразделения ИБ о нарушениях и отклонениях от требований настоящей Политики и других нормативных документов в области ИБ, утвержденных в Компании.