ТОО «Интернет-компания PS»

Политика информационной безопасности

Версия от 18.03.2025

1. Общие положения

Настоящая Политика информационной безопасности ТОО «Интернет-компания PS» (далее — Политика) описывает подход в организации и управлении информационной безопасностью.

Компания внедрила систему управления информационной безопасностью (далее — СУИБ) по требованиям стандартов ISO/IEC 27001:2022 и СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности — Системы управления информационной безопасностью — Требования», а также требованиям стандарта PCI DSS 4.0 в качестве инструмента по обеспечению конфиденциальности, целости и доступности информации.

СУИБ соответствует требованиям законов и нормативных правовых актов Республики Казахстан.

Обеспечение информационной безопасностью ТОО «Интернет-компания PS» (далее — Компания) осуществляется в рамках циклической модели системы менеджмента: «планирование — реализация — проверка — совершенствование».

Политика является методологической основой для:

1. формирования и соблюдения единых политик в области обеспечения безопасности информации в Компании;
2. принятия управленческих решений и разработки практических мер по воплощению Политики.

Политика направлена на достижение основных целей:

1. защиту целостности информации, используемой и обрабатываемой в рамках области сертификации;
2. сохранение конфиденциальности критичных информационных ресурсов;
3. обеспечение доступности обрабатываемой информации;
4. обеспечение непрерывности основных бизнес-процессов, функционирующих в рамках области сертификации;
5. сокращение времени реагирования на инциденты информационной безопасности;
6. повышение качества оказываемых услуг.

Компания обязуется:

- постоянно совершенствовать свою СУИБ, соблюдать применимые юридические и другие обязательства, и удовлетворять применимые ожидания заинтересованных сторон;
- контролировать или ограничивать доступ, чтобы только уполномоченные лица имели возможность просматривать и использовать конфиденциальную информацию;
- предоставлять доступ к информации о клиентах только тем лицам, у которых есть необходимость в просмотре или использовании этой информации;
- не предоставлять информацию третьим лицам без письменного согласия владельцев информации;
- выполнять все требования информационной безопасности клиентов и предоставлять необходимые ресурсы для достижения этой цели;
- регулярно пересматривать данную Политику.

Требования настоящей Политики распространяются на все структурные подразделения Компании.

Сотрудники Компании осведомлены об обязательствах и содержании настоящей политики и несут персональную ответственность за соблюдение требований документов СУИБ, а также обязуются сообщать обо всех выявленных нарушениях в области информационной безопасности.

Руководство принимает непосредственное участие в решении вопросов, связанных с СУИБ.

Настоящая Политика является общедоступным документом, который предоставляется без ограничений всем клиентам и заинтересованным лицам.

Политика, а также вся документация по СУИБ Компании, регулярно пересматривается и корректируется не реже одного раза в два года.

Внеплановый пересмотр документации СУИБ проводится в случае:

1. внесения существенных изменений в организационную структуру Компании;
2. изменений в законодательстве Республики Казахстан;
3. возникновения инцидентов информационной безопасности (далее — ИБ).

При внесении изменений учитываются следующие входные данные:

1. результаты аудита ИБ, а также результаты предыдущих аудитов;
2. рекомендации независимых экспертов по ИБ;
3. угрозы и уязвимости информационных систем;
4. отчеты об инцидентах в области ИБ;
5. рекомендации органов государственной власти;
6. обращения заинтересованных лиц;
7. статус превентивных и корректирующих действий;
8. результаты протоколов руководства по ИБ;
9. оценка рисков ИБ;
10. изменения, которые могут затронуть область действия СУИБ, включая изменения организационной сферы, бизнес обстоятельств, доступности ресурсов, контрактные, регуляторные требования и техническое оснащение;
11. тренды, относящиеся к угрозам и уязвимостям;
12. сообщенные инциденты ИБ.

Пересмотр документации СУИБ осуществляется специалистами, ответственными за ее разработку и внедрение, а также включает в себя оценку возможности улучшения СУИБ в соответствии с изменениями.

Пересмотренная документация СУИБ утверждается руководством Компании.