**Компания «АБС»**

Политика информационной безопасности для обеспечения аутентификации доступа в личный кабинет «Партнёр-API» (в соответствии с требованиями стандарта ГОСТ 57580 и PCI DSS 4.0)

**1. Введение**

1.1 Настоящая Политика информационной безопасности устанавливает принципы и руководящие принципы для обеспечения безопасности доступа в личный кабинет «Партнёр-API»;

1.2 Целью данной политики является обеспечение аутентификации и защиты данных клиентов компании в соответствии с требованиями стандарта ГОСТ 57580 и PCI DSS 4.0.;

1.3 Политика создана и применяется к доступу в личный кабинет «Партнёр-API» и всем связанным с ним процессам и системам.

**2. Определения**

2.1 API (Интерфейс программирования приложений) - набор функций и процедур, которые используются для взаимодействия между различными программами;

2.2 Личный кабинет «Партнёр-API» - веб-интерфейс, предоставляющий доступ к функциональности и информации, связанной с партнерской интеграцией через API.

**3. Основные принципы**

3.1 Соблюдение требований стандарта ГОСТ 57580 и PCI DSS 4.0

* Все процессы, связанные с аутентификацией доступа в личный кабинет "Партнёр-API", должны соответствовать требованиям и рекомендациям стандарта ГОСТ 57580 и PCI DSS 4.0.;
* Ответственным за реализацию программы вменяется в обязанность проводить аудиты и проверки на соблюдении требований стандартов ГОСТ 57580 и PCI DSS 4.0 не реже 1 раза в год

3.2 Аутентификация

* Аутентификация пользователей в личном кабинете «Партнёр-API» должна быть обязательной и основываться на достоверных и проверяемых учетных данных;
* Применение двухфакторной аутентификации для доступа пользователей в личный кабинет «Партнёр-API» является обязательным;
* Блокировка учетной записи пользователя после 5 неудачных попыток ввода пароля на 24 часа является обязательной;
* Установить требования к паролям:
  + Длина пароля должна быть не менее 10 символов;
  + Пароль должен содержать как минимум одну заглавную букву, одну строчную букву, одну цифру и один специальный символ;
  + Пароль должен быть изменен не реже, чем раз в 90 дней;
* Определить требования к множественной аутентификации:
  + Не допускается подключения к личному кабинету "Партнёр-API" более чем с одного устройства за одну сессию

3.3 Защита учетных данных

* Учетные данные (такие как пароли и ключи API) должны быть защищены от несанкционированного доступа и доступны лишь ограниченному числу сотрудников компании, несущих личную ответственность за сохранность вышеупомянутых данных;
* Использование безопасных методов передачи и хранения учетных данных, такие как шифрование и хэширование является необходимым и обязательным

3.4 Разграничение доступа

* Разграничение доступа, предоставляющие клиентам минимально необходимые привилегии для выполнения операций в личном кабинете «Партнёр-API» является обязательным;

3.5 Мониторинг и регистрация событий

* Ведение мониторинга и регистрация всех событий, связанных с доступом в личный кабинет «Партнёр-API», для обеспечения выявления и реагирования на потенциальные инциденты безопасности является обязательным и непрерывным на весь период функционирования личного кабинета «Партнёр-API»;

3.6 Обучение и осведомленность

* Обеспечить проведение регулярных обучающих программы для сотрудников, связанных с личным кабинетом «Партнёр-API», с акцентом на безопасности данных и правилах аутентификации не реже 1 раза в 6 месяцев;
* Повышать осведомленность о безопасности среди пользователей личного кабинета «Партнёр-API» и предоставлять рекомендации по безопасной аутентификации не реже 1 раза в квартал.

**4. Реагирование на инциденты**

4.1 Определить процедуры реагирования на инциденты безопасности, связанные с доступом в личный кабинет «Партнёр-API», включая компрометацию учетных данных, несанкционированный доступ или утечку информации;

4.2 Назначить команду реагирования на инциденты и определить их обязанности, ответственность и сроки развертывания мероприятий по реагированию на инциденты;

4.3 Обеспечить проведение учений команды по реагированию на инциденты для проверки и улучшения готовности к инцидентам не реже 1 раза в квартал.

**5. Заключительные положения**

5.1 Политика информационной безопасности является обязательной для всех сотрудников компании «АБС» связанных с созданием и функционированием процессов и систем личного кабинета «Партнёр-API»;

5.2 Политика информационной безопасности является обязательной для всех пользователей личного кабинета «Партнёр-API»;

5.3 Политика должна регулярно обновляться и приводиться в соответствие с актуальными требованиями стандартов ГОСТ 57580 и PCI DSS 4.0.;

5.4 Ответственность за подготовку технической и административной документации, разработанной в целях реализации настоящей Политики, а также неукоснительное выполнение всех технических и административных мероприятий, направленных на выполнение Политики возложить на начальника службы информационной безопасности Петрова Б.В.;

5.5 Контроль за исполнением положений настоящей политики оставляю за собой.

Генеральный директор Иванов А.Г.