УТВЕРЖДАЮ

Генеральный директор

ТОО «Вериграм»

Дата: «5» января 2026 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОО «ВЕРИГРАМ»

1. Назначение и область применения

Настоящая Политика является основным документом Системы управления информационной безопасностью (СУИБ) ТОО «Вериграм». Действие Политики распространяется на все бизнес-процессы, активы, сотрудников и подрядчиков компании, задействованных в процессах разработки, внедрения и технической поддержки сервисов биометрической верификации и онлайн-подписания, а также на инфраструктуру разработки в офисе и серверные мощности, арендуемые в сертифицированном ЦОД.

Главная цель СУИБ ТОО «Вериграм» — обеспечение конфиденциальности, целостности и доступности обрабатываемых данных (включая биометрические персональные данные пользователей и исходный код разрабатываемых продуктов), обеспечение непрерывности бизнеса и укрепление доверия клиентов.

2. Принципы обеспечения информационной безопасности

Для достижения главной цели руководство ТОО «Вериграм» обязуется следовать следующим принципам:

- **Защита данных по умолчанию (Security by Design):** Требования информационной безопасности интегрируются на всех этапах жизненного цикла разработки ПО.
- **Контроль инфраструктуры:** Обеспечение надежного и безопасного функционирования сервисов посредством строгого управления доступом, резервного копирования и контроля SLA с внешними поставщиками услуг (ЦОД).
- **Осведомленность:** Каждый сотрудник осознает свою ответственность за безопасность данных и регулярно проходит обучение по противодействию актуальным угрозам (в т.ч. социальной инженерии).

3. Структура постановки целей информационной безопасности

Высшее руководство гарантирует, что цели информационной безопасности устанавливаются, измеряются, анализируются и актуализируются. Для оценки результативности СУИБ применяются:

- **Стратегические цели:** Устанавливаются руководством ежегодно (в виде Плана достижения целей) и направлены на внедрение новых процессов и технологий защиты (например, интеграция SAST, проведение регулярных тестирований на проникновение).
- **Операционные показатели (KPI):** Измеряются на регулярной основе (ежемесячно/ежеквартально) для контроля текущих процессов (такие как время реакции на инциденты MTTD/MTTR, показатели блокировки презентационных атак на биометрические алгоритмы).

4. Обязательства руководства

Высшее руководство ТОО «Вериграм» принимает на себя следующие обязательства:

1. **Выполнять применимые требования:** Неукоснительно соблюдать законодательные и нормативные требования Республики Казахстан (в сфере защиты персональных данных и информатизации), договорные обязательства перед клиентами и партнерами, а также требования международного стандарта ISO/IEC 27001:2022.
2. **Обеспечивать ресурсами:** Выделять необходимые финансовые, технические и кадровые ресурсы для функционирования, мониторинга и поддержки СУИБ.
3. **Постоянно улучшать СУИБ:** Регулярно анализировать результаты мониторинга метрик, результаты внутренних и внешних аудитов, а также инциденты ИБ для непрерывного совершенствования системы управления информационной безопасностью.

5. Ответственность

- **Генеральный директор** несет общую ответственность за утверждение настоящей Политики и функционирование СУИБ.
- **Технический директор** несет ответственность за разработку, внедрение, контроль и организацию аудитов СУИБ, а также информирование руководства о ее результативности.
- **Каждый сотрудник и подрядчик** ТОО «Вериграм» несет персональную ответственность за соблюдение требований настоящей Политики и связанных с ней внутренних нормативных документов СУИБ.

6. Пересмотр документа

Настоящая Политика пересматривается не реже одного раза в год в рамках процедуры анализа со стороны руководства, а также при существенных изменениях в бизнес-процессах, инфраструктуре или законодательстве.