ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСНОСТИ ООО «ДСТ ГЛОБАЛ»

1. Общие положения

1.1. Настоящая Политика определяет общие принципы и организационные подходы ООО «ДСТ ГЛОБАЛ» (далее — «Компания») к защите конфиденциальной информации Компании, а также конфиденциальной информации Заказчиков, полученной в рамках исполнения договоров.

1.2. Компания реализует **гибкий и проектный подход** к информационной безопасности. Конкретный перечень технических и организационных мер защиты по каждому проекту определяется его масштабом, спецификой и **прямо согласовывается с Заказчиком** в Техническом задании, Спецификации или ином документе, являющемся неотъемлемой частью договора.

2. Базовые (универсальные) принципы и меры защиты

Независимо от проекта, Компания гарантирует соблюдение следующих базовых принципов:

2.1. **Конфиденциальность персональных и коммерческих данных:**

- Все сотрудники и привлекаемые подрядчики привлекаются к работе только после подписания Соглашения о конфиденциальности (NDA).
- Любая информация, полученная от Заказчика, считается конфиденциальной по умолчанию.

2.2. **Принцип минимального доступа и проверки полномочий:**

- Доступы к системам, исходному коду, базам данных и иной инфраструктуре Заказчика предоставляются **исключительно сотрудникам, официально назначенным на проект**.
- **Строгий запрет:** Никому, кроме официальных представителей Заказчика, указанных в договоре или прямо назначенных ими в письменной форме (например, через официальный чат проекта), **не предоставляются доступы, пароли, ключи или иная конфиденциальная информация**.
- Любой запрос на предоставление доступов проверяется на соответствие контактам и полномочиям, указанным в договоре.

2.3. **Принцип документирования требований:**

- Все специальные требования Заказчика к информационной безопасности (например, использование конкретного хостинга, настроек шифрования, систем резервного копирования, репозиториев кода) подлежат обязательному включению в Техническое задание или иной договорной документ.

3. Гибкие (проектные) меры защиты

3.1. Компания готова реализовать по требованию Заказчика и за его счет любой комплекс мер защиты, в том числе:

3.2. **Для проектов любого масштаба:**

- Использование систем контроля версий (GitLab, GitHub, Bitbucket и др.) с настройкой прав доступа.
- Организация процедур ручного или автоматического резервного копирования.
- Настройка систем мониторинга и логирования доступа.

3.3. **Для средних и крупных проектов:**

- Внедрение двухфакторной аутентификации (2FA).
- Использование выделенных защищенных серверов (VPS/VDS) с настройкой межсетевых экранов.
- Регулярное проведение аудита безопасности кода и инфраструктуры.
- Шифрование каналов связи и данных на rest.

4. Реагирование на инциденты

4.1. В случае возникновения подозрений на утечку информации или иного инцидента безопасности Компания обязуется:

- Немедленно уведомить Заказчика.
- Начать внутреннее расследование.
- Действовать в соответствии с инструкциями Заказчика и в рамках действующего законодательства.

Генеральный директор / Президент
ООО «ДСТ ГЛОБАЛ»

/ Морган А.А. /