ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Общие положения

Настоящая Политика информационной безопасности и защиты персональных данных устанавливает основные принципы и обязательства ТОО «Global Service Asia» в части защиты информации, персональных данных и иных сведений ограниченного доступа, используемых в деятельности Компании, и разработана в соответствии с законодательством Республики Казахстан, включая Закон Республики Казахстан «О персональных данных и их защите».

Политика распространяется на работников Компании, а также учитывается при взаимодействии с подрядчиками, поставщиками, консультантами, арендодателями, клиентами и иными деловыми партнерами в той мере, в которой это применимо к деятельности Компании.

Настоящая Политика носит рамочный характер и применяется совместно с иными внутренними и договорными документами Компании, регулирующими вопросы конфиденциальности, коммерческой тайны, защиты персональных данных, использования информационных ресурсов и обязательств работников, подрядчиков и контрагентов.

2 Цель Политики

Целью настоящей Политики является установление для Компании понятных и применимых правил защиты информации, персональных данных и иных сведений ограниченного доступа, направленных на соблюдение требований законодательства Республики Казахстан, предупреждение утраты, искажения, несанкционированного раскрытия и неправомерного использования информации, а также применение соразмерных организационных и технических мер защиты.

Компания исходит из того, что даже при небольшом масштабе деятельности надлежащая защита информации и персональных данных является обязательным элементом добросовестного ведения бизнеса, договорной дисциплины и доверия со стороны работников, клиентов и деловых партнеров.

3 Основные принципы

Компания руководствуется следующими принципами при работе с информацией:

- законность обработки - персональные данные и иная информация обрабатываются на законных основаниях и для определенных, правомерных и ограниченных целей в соответствии с законодательством Республики Казахстан;
- минимально необходимый объем - сбор, хранение, использование и передача информации осуществляются только в объеме, необходимом для исполнения трудовых, договорных, расчетных, административных, клиентских и иных законных бизнес-задач Компании;
- ограничение доступа - доступ к сведениям ограниченного доступа предоставляется только лицам, которым такая информация необходима для выполнения служебных или договорных функций;
- точность и актуальность - Компания принимает разумные меры по поддержанию достоверности обрабатываемой информации и ее актуализации при необходимости;
- безопасное хранение и удаление - информация хранится и уничтожается способом, соразмерным ее характеру, срокам хранения и уровню риска.

4 Основные обязательства Компании

4.1 Защита персональных данных и коммерческой информации

Компания обеспечивает защиту персональных данных работников, клиентов, контрагентов и иных лиц, чьи данные обрабатываются в связи с деятельностью Компании, а также защиту коммерческой, договорной и иной конфиденциальной информации.

Компания стремится ограничивать объем собираемой и хранимой информации теми сведениями, которые действительно необходимы для исполнения трудовых, договорных, административных, расчетных и иных законных задач Компании.

4.2 Порядок доступа, хранения и передачи

Хранение. Бумажные носители, содержащие сведения ограниченного доступа, хранятся в запираемых шкафах или иных местах с ограниченным доступом. Электронные данные защищаются паролями, разграничением доступа и иными соразмерными мерами защиты. Для критически важных сервисов может применяться двухфакторная аутентификация при наличии технической возможности.

Передача. Передача информации третьим лицам допускается только при наличии законных оснований, в рамках исполнения договоров, требований законодательства либо иных правомерных целей, при условии соблюдения применимого режима конфиденциальности.

Каналы связи. Работники обязаны использовать для служебного обмена информацией корпоративную почту и иные каналы связи, согласованные Компанией. Использование

личных аккаунтов и несанкционированных каналов для передачи сведений ограниченного доступа не допускается.

4.3 Безопасное использование ресурсов и инциденты

Работники несут персональную ответственность за сохранность выданного оборудования, учетных данных и иных средств доступа, используемых в служебных целях.

Запрещается установка несанкционированного программного обеспечения, передача паролей третьим лицам и использование ресурсов Компании в личных или неправомерных целях.

В случае утери устройства, обнаружения подозрительной активности, ошибочной отправки данных, несанкционированного доступа или иного инцидента информационной безопасности работник обязан незамедлительно уведомить непосредственного руководителя, Генерального директора либо направить сообщение на адрес compliance@globalservice-asia.com.

4.4 Работа с подрядчиками и внешними сервисами

При передаче персональных данных, конфиденциальных документов или иной чувствительной информации подрядчикам, консультантам, сервисным организациям или внешним исполнителям Компания доводит до них применимые требования по конфиденциальности, защите информации и персональных данных через договоры, заказы, технические задания, сопроводительную переписку и иные документы, используемые в конкретной модели взаимодействия.

Если Компания действует в качестве подрядчика или исполнителя для клиента и получает доступ к его документам, переписке, заявкам, персональным данным, коммерческой информации, внутренним системам либо иным сведениям ограниченного доступа, Работники и, при необходимости, привлеченные Компанией контрагенты обязаны соблюдать применимые требования клиента по защите информации и обращению с данными наряду с внутренними требованиями Компании.

В применимых случаях Компания вправе запрашивать у партнеров сведения о применяемых ими мерах защиты информации и принимать меры по ограничению доступа или пересмотру взаимодействия при выявлении существенных угроз безопасности.

4.5 Инструктаж и контроль

Ознакомление с настоящей Политикой является обязательным при приеме на работу и при ее существенном обновлении.

Компания вправе выборочно проверять соблюдение базовых правил хранения документов, использования учетных данных и обращения со сведениями ограниченного доступа, а при выявлении уязвимостей или нарушений принимать соразмерные корректирующие меры.

5 Ответственность

Генеральный директор осуществляет общее руководство и контроль реализации Политики.

Работники несут ответственность за нарушение требований настоящей Политики, несанкционированное разглашение сведений ограниченного доступа и несоблюдение базовых правил информационной безопасности в соответствии с законодательством Республики Казахстан, трудовым договором и локальными актами Компании в области конфиденциальности и защиты информации.

В случаях, предусмотренных законодательством Республики Казахстан, виновные лица могут быть привлечены к административной или уголовной ответственности за нарушение тайны персональных данных или разглашение коммерческой информации.

6 Мониторинг и пересмотр

Компания осуществляет периодический пересмотр настоящей Политики с учетом изменений законодательства, требований клиентов, структуры деятельности Компании, используемых информационных ресурсов и накопленной практики ее применения.

7 Заключительные положения

Настоящая Политика вступает в силу с даты утверждения.

Политика подлежит доведению до работников Компании и, при необходимости, до подрядчиков, поставщиков и иных заинтересованных сторон в части, относящейся к их взаимодействию с Компанией.

Утверждено:

Генеральный директор

ТОО «Global Service Asia»

_____ /Р.С. Шадыжев/

«___» _____ 2026 г.