Политика обеспечения информационной безопасности (ОИБ)

Версия 1.0

1 Определения и толкования

Определения, приведенные в данном разделе 2, применяются к настоящей Политике обеспечения информационной безопасности (ОИБ).

Term	Definition
Соглашение	Соглашение между flydubai и Третьей стороной, в связи с которым Третья сторона получает доступ к Данным flydubai.
Уполномоченные стороны	Все лица, являющиеся работниками Третьей стороны, а также агенты, представители Третьей стороны и любые другие стороны в каждом конкретном случае, чье привлечение и доступ к Данным flydubai строго необходимы для выполнения обязательств Третьей стороны по Соглашению.
Непрерывность бизнеса и аварийное восстановление	Совокупность процессов и методов, используемых для того, чтобы помочь организации восстановиться после бедствия и продолжить или возобновить работу в штатном режиме.
Конфиденциальная информация	Информация, раскрываемая стороной (или от ее имени) или ее представителями другой стороне в связи с Соглашением и помеченная как конфиденциальная или обоснованно расцениваемая как конфиденциальная при данных обстоятельствах.
Протокол динамической конфигурации хоста	Протокол управления сетью, используемый в сетях с доступом по межсетевому протоколу для автоматического присвоения IP-адресов и других параметров связи устройствам, подключенным к сети, с использованием архитектуры «Клиент — сервер».
flydubai	Дубайская авиационная корпорация (ведущая деятельность под коммерческим наименованием flydubai).

Данные flydubai	Вся информация в любой форме, относящаяся к flydubai, ее коммерческой деятельности или клиентам, которую flydubai предоставляет в связи с выполнением обязательств Третьей стороны по Соглашению, включая любую информацию, предоставляемую или генерируемую, собираемую, обрабатываемую, сохраняемую или передаваемую в связи с доступом компании flydubai к обязательствам Третьей стороны по Соглашению и/или использованием ею таких обязательств.
Процесс управления инцидентами	Совокупность процедур и действий, предпринимаемых в порядке реагирования и разрешения критически значимых инцидентов: методы обнаружения и оповещения об инцидентах, ответственные лица, используемые инструменты, а также шаги, предпринимаемые для разрешения инцидента.
Мобильные и портативные устройства	Вычислительные устройства малого форм-фактора, предназначенные для использования в руках и применяемые для выхода в Интернет и связи с другими людьми.
Персональная информация	Информация или мнение об идентифицированном физическом лице или физическом лице, которое можно с достаточными основаниями идентифицировать, независимо от того, являются ли такая информация или мнение верными или нет; и независимо от того, зафиксированы ли такая информация или мнение в материальной форме или нет, включая, помимо прочего, персональные данные для целей Общего регламента ЕС по защите персональных данных 2016/ 679.
Политика	Настоящая Политика обеспечения информационной безопасности.
Ограниченная, взаимная, наследуемая или копилефтная лицензия	Лицензия на программное обеспечение, требующая, чтобы информация, необходимая для воспроизведения и модификации такого программного обеспечения, была предоставлена в общем доступе получателям выполняемых версий такого программного обеспечения, включая, помимо прочего, универсальные

	общественные лицензии General Public Licence (GPL) и Affero General Public Licence (AGPL).
Шлюз безопасности	Совокупность управляющих механизмов между двумя или более сетями с различными уровнями доверия, фильтрующих и регистрирующих трафик, который проходит или пытается пройти между сетями, а также соответствующие административные и управляющие серверы.
Строгая аутентификация	Метод проверки пользователей, признанный достаточно надежным для того, чтобы противостоять атакам на систему, в которой пользователи проходят аутентификацию.
Криптостойкое шифрование	Использование технологий шифрования с минимальной длиной ключа 128 бит для симметричного шифрования и 1024 бит для асимметричного шифрования, устойчивость которых внушает разумную уверенность в том, что они защитят зашифрованную информацию от несанкционированного доступа и обеспечат достаточный уровень конфиденциальности и приватности зашифрованной информации, и которые воплощают в себе документированную политику управления ключами шифрования и соответствующие процессы, достаточные для защиты конфиденциальности и приватности ключей и паролей, используемых в качестве входных данных для алгоритма шифрования.
Технические и организационные меры безопасности	Функции, процессы, средства управления, системы, процедуры и меры, которые организации могут внедрять для обеспечения безопасной обработки и хранения персональных и конфиденциальных данных, предотвращения утечек данных и соблюдения соответствующих обязательств по защите данных.
Третья сторона	Третья сторона, получающая доступ к Данным flydubai в связи с настоящей политикой.

1. Организация информационной безопасности

Третья сторона должна по меньшей мере:

a. Обеспечить, чтобы доступ к Данным flydubai предоставлялся только Уполномоченным сторонам.

b. Применять Технические и организационные меры безопасности, не менее строгие, чем передовые методы обеспечения информационной безопасности, для защиты целостности, доступности и конфиденциальности Данных flydubai и другой непубличной информации и предотвращения несанкционированного доступа, получения, раскрытия, уничтожения, изменения, случайной потери, неправильного использования или повреждения Данных flydubai.

c. Разработать, внедрить и поддерживать в соответствии с передовыми отраслевыми методами, политикой и программой организационные, операционные, административные, физические, а также Технические и организационные меры безопасности, необходимые для (1) предотвращения любого доступа неуполномоченных сторон к Данным flydubai способом, не предусмотренным Соглашением или настоящей Политикой, и (2) соблюдения требований всех применимых законов и нормативных актов, а также применимых отраслевых стандартов.

d. Принимать разумные меры для предотвращения несанкционированного доступа к Данным flydubai и обязательствам Третьей стороны по Соглашению, системам, устройствам или носителям, содержащим эту информацию, а также для предотвращения потери вышеперечисленного.

e. Использовать процессы и процедуры оценки рисков для регулярной оценки систем, используемых для предоставления flydubai доступа к обязательствам или продуктам Третьей стороны. Третья сторона должна устранять такие риски в максимально короткие сроки и соразмерно уровню риска для Данных flydubai с учетом угроз, известных на момент идентификации. Организовать процесс, позволяющий сообщать о рисках или предполагаемых инцидентах в службу безопасности flydubai.

f. Вести учет ресурсов Уполномоченных сторон и Третьих сторон, которые пользуются доступом к, передают, поддерживают, хранят или обрабатывают Данные flydubai.

g. Проводить комплексную проверку биографических данных всех Уполномоченных сторон до приема на работу в пределах, разрешенных законом. В рамках комплексной проверки биографических данных физических лиц должна рассматриваться по меньшей мере информация о предыдущих местах работы, сведения о судимости, кредитная история, рекомендательные письма и любые дополнительные сведения согласно требованиям отраслевых стандартов к проверке биографических данных.

h. Требовать от Уполномоченных сторон принятия договорных обязательств о неразглашении или сохранении конфиденциальности информации до предоставления им доступа к Данным flydubai.

i. Обеспечить, чтобы все Уполномоченные стороны, которые могут выполнять работу по Соглашению или иметь доступ к Данным flydubai, соблюдали эти Технические и организационные меры безопасности, что должно быть подтверждено письменным соглашением, предусматривающим не менее строгие ограничения, чем настоящая Политика.

2. Физическая безопасность и безопасность среды

Третья сторона должна по меньшей мере:

a. Обеспечить, чтобы все системы и другие ресурсы Третьей стороны, предназначенные для коллективного использования, располагались внутри защищенных физических объектов с ограниченным доступом только для уполномоченных лиц.

b. Контролировать и регистрировать в целях аудита доступ к физическим объектам, содержащим системы и другие ресурсы, предназначенные для коллективного использования и используемые в связи с выполнением Третьей стороной своих обязательств по Соглашению.

c. Ограничивать и контролировать физический доступ к своим объектам, предоставляя его только Уполномоченным сторонам.

d. Обеспечить физическую защиту оборудования, используемого для хранения, обработки или передачи Данных flydubai, включая точки беспроводного доступа, шлюзы, портативные устройства, сетевое/коммуникационное оборудование и телекоммуникационные линии.

e. Внедрить средства управления для минимизации риска возникновения физических угроз и защиты от них.

f. Защищать любые устройства, собирающие данные платежных карт посредством прямого физического взаимодействия, от взлома или подмены путем периодического осмотра поверхностей устройств для обнаружения взлома или подмены; проводить обучение персонала для обеспечения его осведомленности о попытках взлома или подмены устройств.

3. Управление доступом

Третья сторона должна по меньшей мере:

a. Отделять информацию flydubai от данных других клиентов Третьей стороны, а также собственных приложений и информации Третьей стороны либо с помощью

физического разделения серверов, либо с помощью механизмов логического управления доступом, если физическое разделение серверов не реализовано.

b. Идентифицировать соответствующих владельцев и обязать их проверять и одобрять доступ к системам, используемым для доступа, обработки, управления или хранения Данных flydubai, не реже одного раза в квартал, чтобы исключить несанкционированный доступ; а также осуществлять поддержку и мониторинг процессов одобрения доступа.

c. Отменять доступ к системам, управляющим Данными flydubai, в течение 24 часов после того, как Уполномоченная сторона расторгнет отношения с Третьей стороной; и соблюдать обоснованно необходимые процедуры для отмены доступа к таким системам в течение трех рабочих дней в случаях, когда такой доступ больше не нужен или не имеет отношения к выполнению обязанностей Третьей стороны. Все идентификаторы других пользователей должны быть аннулированы или удалены по истечении 90 календарных дней бездействия.

d. Ограничить доступ от имени системного администратора (также именуемого root, привилегированный или суперпользователь) к операционным системам, предназначенным для коллективного использования, предоставив его исключительно лицам, которым такой высокоуровневый доступ необходим для выполнения их работы. Использовать контрольные идентификаторы системного администратора с индивидуальными учетными данными пользователей и журналами регистрации действий для управления доступом высокого уровня безопасности и сокращения круга лиц, имеющих доступ высокого уровня, до крайне ограниченного числа пользователей. Требовать от администраторов приложений, баз данных, сетей и систем ограничивать доступ пользователей, предоставляя его только к командам, данным, системам и другим ресурсам, необходимым для выполнения разрешенных пользователям функций. Роли системных администраторов и списки доступа должны пересматриваться не реже одного раза в год.

e. Требовать прохождения Строгой аутентификации во всех случаях неконсольного административного доступа, удаленного доступа и административного доступа к облачным средам.

4. Идентификация и аутентификация

Третья сторона должна по меньшей мере:

a. Присвоить уникальные идентификаторы отдельным пользователям и установить механизмы аутентификации для каждой отдельной учетной записи.

b. Использовать документированный процесс управления жизненным циклом идентификатора пользователя, включая, помимо прочего, процедуры одобренного создания учетной записи, своевременного удаления и изменения учетной записи (например, изменения прав, степени доступа, функций/ролей), для всех случаев доступа к Данным flydubai во всех средах (производственная, тестовая, среда разработки и т.д.). Такой процесс должен включать проверку прав доступа и валидности учетных записей, которая должна проводиться не реже одного раза в квартал.

c. Ограничить доступ к Данным flydubai, предоставляя его только тем, кто использует действительный идентификатор пользователя и пароль, и требовать, чтобы для уникальных идентификаторов пользователя использовалось одно из следующих средств: пароль или кодовая фраза, двухфакторная аутентификация или биометрические данные.

d. Требовать использования сложных паролей и соблюдать следующие требования к структуре пароля согласно политике flydubai: минимум восемь (8) символов в длину для системных паролей и четыре (4) символа для кодов доступа на планшетах и смартфонах. Системные пароли должны содержать три (3) из следующих элементов: символы верхнего регистра, символы нижнего регистра, цифры или специальные символы.

e. Пароль также не должен совпадать с идентификатором пользователя, к которому он привязан, содержать слова из словаря, последовательные или повторяющиеся цифры, а также не должен совпадать с одним из последних пяти паролей.

f. Периодически требовать истечения срока действия пароля через промежутки времени, не превышающие девяноста (90) дней.

g. Маскировать все пароли при отображении.

h. Ограничить число неудачных попыток входа в систему до максимум пяти (5) в течение 24 часов и по достижении этого предела блокировать учетную запись пользователя в персистентном состоянии. Доступ к учетной записи пользователя может быть впоследствии восстановлен в ручном режиме при условии подтверждения личности пользователя.

i. Верифицировать личность пользователя и устанавливать для каждого пользователя уникальное значение одноразового и восстановленного пароля. Систематически предлагать сменить пароль после первого использования.

j. Использовать безопасный метод передачи учетных данных для аутентификации (например, паролей) и механизмов аутентификации (например, токенов или смарт-карт).

k. Установить длину паролей учетных записей служб и прокси не менее 12 символов, включая символы верхнего регистра, символы нижнего регистра и цифры, а также специальные символы. Менять пароли учетных записей служб и прокси не реже одного раза в год и после прекращения трудовых отношений со всеми, кому был известен пароль.

l. Завершать интерактивные сеансы или активировать защитную блокирующую экранную заставку, требующую аутентификации, после периода бездействия, не превышающего пятнадцати (15) минут.

m. Использовать метод аутентификации на основе уязвимости Данных flydubai. При хранении учетных данных для аутентификации Третья сторона должна защищать их с помощью Криптостойкого шифрования.

n. Настроить системы на автоматическое завершение работы после максимального периода бездействия следующим образом: сервер (15 минут), рабочая станция (15 минут), мобильное устройство (4 часа), протокол динамической конфигурации хоста (7 дней), виртуальная частная сеть (24 часа).

5. Приобретение, разработка и обслуживание информационных систем

Третья сторона должна по меньшей мере:

a. Использовать эффективную методологию управления приложениями, позволяющую включить Технические и организационные меры безопасности в процесс разработки программного обеспечения, и обеспечить своевременное внедрение Третьей стороной Технических и организационных мер безопасности в соответствии с передовым отраслевым опытом.

b. Соблюдать стандартные для отрасли процедуры разработки, включая разделение доступа и кода между непроизводственной и производственной средами и соответствующее разделение обязанностей между такими средами.

c. Обеспечить регулярную оценку внутренних средств управления информационной безопасностью при разработке программного обеспечения и их соответствие передовому отраслевому опыту, а также своевременно пересматривать и внедрять такие средства управления.

d. Управлять безопасностью процесса разработки и обеспечивать внедрение и использование методов безопасного программирования, включая соответствующие

криптографические средства управления, защиту от вредоносного кода и процедуру экспертной оценки.

e. Проводить тестирование на проникновение в функционально законченные приложения перед выпуском в производственную среду и в дальнейшем не менее одного раза в год и после любых значительных изменений исходного кода или конфигурации в соответствии с OWASP, CERT, SANS Top 25 и PCI-DSS. Устранять любые доступные для использования уязвимости до развертывания в производственной среде.

f. Использовать обезличенные или замаскированные данные в непроизводственных средах. Никогда не использовать производственные данные в виде открытого текста в любой непроизводственной среде и никогда не использовать Персональную информацию в непроизводственных средах по любой причине. Обеспечить удаление всех тестовых данных и учетных записей до выпуска в производственную среду.

g. Проверять открытый или свободный исходный код, одобренный flydubai, программное обеспечение, приложения или сервисы на наличие недостатков, ошибок, проблем безопасности или несоответствия условиям лицензирования открытого или свободного исходного кода. Третья сторона должна заблаговременно уведомлять flydubai об использовании любого открытого или свободного исходного кода и, в случае одобрения такого использования со стороны flydubai, предоставлять flydubai название, версию и URL открытого или свободного исходного кода. Третья сторона заявляет и гарантирует, что (i) любой открытый или свободный исходный код, который она использует в своих продуктах или сервисах, лицензируется по пермиссивным лицензиям на открытый или свободный исходный код, а не по ограниченным, взаимным, наследуемым или копилефтным лицензиям; (ii) Третья сторона имеет право свободно изменять, адаптировать и комбинировать открытый или свободный исходный код, а также включать его в проприетарный код без наложения ограничений на такие изменения, адаптации, комбинации или проприетарный код, содержащий открытый или свободный исходный код, и на порядок их последующего лицензирования (совместно именуемые «производные работы») и (iii) такие производные работы не будут подпадать под действие какой-либо лицензии на открытый или свободный исходный код, требующей лицензирования производной работы или ее бесплатного предоставления третьим сторонам в соответствии с условиями лицензии на открытый или свободный исходный код.

h. Третья сторона не будет размещать какие-либо коды, созданные в рамках Соглашения, независимо от стадии разработки, в каких-либо общих или не частных

средах, например в репозиториях кода с открытым доступом, независимо от защиты паролем.

6. **Целостность программного обеспечения и данных**

Третья сторона должна по меньшей мере:

a. В средах, где антивирусное программное обеспечение является коммерчески доступным, обеспечивать установку и запуск антивирусного программного обеспечения для сканирования и оперативного удаления или перемещения в карантин вирусов и другого вредоносного ПО из любой системы или устройства.

b. Отделять непроизводственную информацию и ресурсы от производственной информации и ресурсов.

c. Обеспечить, чтобы сотрудники использовали документированный процесс управления изменениями для всех изменений в системе, включая процедуры восстановления предыдущего состояния для всех производственных сред и процессы аварийных изменений. Предусмотреть тестирование, документирование и утверждение всех изменений в системе и требовать одобрения руководства в случае значительных изменений таких процессов.

d. Создать и поддерживать зону PCI, если Третья сторона обрабатывает или хранит данные держателей карт.

e. Для приложений, использующих базу данных, которая позволяет вносить изменения в Данные flydubai, иметь и поддерживать функции ведения журналов аудита транзакций базы данных и хранить такие журналы в течение как минимум одного (1) года, при этом информация за три месяца должна быть незамедлительно доступна для анализа.

f. Проверять программное обеспечение с целью поиска и устранения уязвимостей при первоначальном внедрении и при любых значительных изменениях и обновлениях.

g. Выполнять тестирование для обеспечения качества компонентов безопасности (например, тестирование функций идентификации, аутентификации и авторизации), а также любые другие действия, направленные на проверку архитектуры безопасности, при первоначальном внедрении и при любых значительных изменениях и обновлениях.

7. **Безопасность системы**

Третья сторона должна по меньшей мере:

a. Регулярно создавать и обновлять последние версии схем потоков данных и системы, используемых для доступа, обработки, управления или хранения Данных flydubai.

b. Вести активный мониторинг отраслевых ресурсов (например, www.cert.org, www.cert.org и соответствующих списков почтовой рассылки и веб-сайтов поставщиков программного обеспечения) для своевременного уведомления обо всех применимых предупреждениях об опасности, относящихся к системам и другим информационным ресурсам Третьей стороны.

c. Эффективно управлять криптографическими ключами путем ограничения доступа к ним до минимально необходимого числа хранителей, хранения секретных и приватных криптографических ключей путем шифрования ключом как минимум такого же уровня надежности, что и ключ шифрования данных, а также хранения отдельно от ключа шифрования данных в защищенном криптографическом устройстве, в минимально возможном количестве мест. Менять криптографические ключи, используемые по умолчанию, при установке и не реже одного раза в два года, и надежно уничтожать старые ключи.

d. Сканировать доступные извне и внутренние системы и другие информационные ресурсы, включая, помимо прочего, сети, серверы, приложения и базы данных, с помощью соответствующего отраслевому стандарту программного обеспечения для сканирования уязвимостей с целью выявить уязвимости, обеспечить надлежащую защиту таких систем и других ресурсов и выявить любые несанкционированные беспроводные сети, не реже одного раза в квартал и до выпуска приложений, значительных изменений и обновлений в сроки, установленные по результатам анализа рисков на основе оправданных и общепринятых в сфере ИТ политик и стандартов.

e. Обеспечить, чтобы все системы и другие ресурсы Третьей стороны были и оставались защищенными, что включает, помимо прочего, удаление или отключение неиспользуемых сетевых и других служб и продуктов (например, finger, rlogin, ftp и простых служб и продуктов Transmission Control Protocol/Internet Protocol (TCP/IP), а также установку системного брандмауэра, программ Transmission Control Protocol (TCP) Wrappers или аналогичных технологических барьеров.

f. Развернуть одну или несколько систем обнаружения вторжений (IDS), систем предотвращения вторжений (IPS) или систем обнаружения и предотвращения вторжений (IDP) в активном режиме работы с целью контроля всего трафика, входящего и выходящего из систем и других ресурсов в связи с Соглашением, в средах, где такая технология коммерчески доступна, и в той мере, в какой это практически осуществимо.

g. Поддерживать процесс оценки риска для выявления уязвимостей в соответствии с передовым отраслевым опытом для устранения уязвимостей в любой системе или другом ресурсе, включая, помимо прочего, уязвимости, отмеченные в отраслевых публикациях и обнаруженные при сканировании на уязвимости, сканировании на вирусы и просмотре журналов безопасности, и оперативно осуществлять обновление системы безопасности с учетом вероятности того, что такая уязвимость может быть использована или находится в процессе использования. Если по результатам оценки были обнаружены критические уязвимости, корректирующие меры должны быть приняты при первой же возможности и ни в коем случае не позднее 7 дней после получения результатов оценки и выпуска обновления системы безопасности. При обнаружении уязвимостей высокого уровня риска корректирующие меры должны быть приняты в течение 30 дней после получения результатов оценки и выпуска обновления системы безопасности. При обнаружении уязвимостей среднего и низкого уровня риска корректирующие меры должны быть приняты в течение 70 календарных дней после получения результатов оценки и выпуска обновления системы безопасности.

h. Проводить обобщенное внутреннее и внешнее тестирование на проникновение не реже одного раза в год и после любого значительного обновления или модификации инфраструктуры или приложений.

i. Удалять или отключать несанкционированное программное обеспечение, обнаруженное в системах Третьих сторон, и использовать стандартные для отрасли средства борьбы с вредоносным ПО, включая установку, регулярное обновление и постоянное использование программных продуктов для борьбы с вредоносным ПО во всех сервисах, системах и устройствах, которые могут использоваться для доступа к Данным flydubai. Использовать надежное и, по возможности, лучшее в отрасли антивирусное программное обеспечение и обеспечивать обновление антивирусных баз.

j. Поддерживать в актуальном состоянии программное обеспечение во всех сервисах, системах и устройствах, которые могут быть использованы для доступа к Данным flydubai, что включает соответствующее обслуживание операционной системы (систем) и успешное обновление системы безопасности до приемлемого актуального состояния.

k. Возложить обязанности по управлению системой безопасности при настройке операционных систем хоста на конкретных лиц.

l. Изменять все заданные по умолчанию имена учетных записей и/или пароли.

8. Контроль

Третья сторона должна по меньшей мере:

a. Сохранять данные журналов событий для flydubai. Журналы событий должны предназначаться для обнаружения и реагирования на инциденты и включать, помимо прочего:

   i. Все случаи доступа отдельных пользователей к Данным flydubai

   ii. Все действия, предпринимаемые лицами с административными или root-правами

   iii. Все случаи доступа пользователей к журналам аудита

   iv. Неудачные попытки логического доступа

   v. Использование механизмов идентификации и аутентификации и изменения в них

b. Регистрировать основные действия Третьих сторон в системах, содержащих любые Данные flydubai.

c. Ограничить доступ к журналам безопасности до круга Уполномоченных лиц и защитить журналы безопасности от внесения несанкционированных изменений.

d. Внедрить механизм обнаружения изменений (например, контроль целостности файлов) для предупреждения персонала о несанкционированном изменении критических системных файлов, файлов конфигурации или файлов контента; настроить программное обеспечение для еженедельного сравнения критических файлов.

e. Не реже одного раза в неделю просматривать все журналы аудита безопасности и связанные с безопасностью журналы аудита систем, содержащих Данные flydubai, на предмет аномалий, а также своевременно документировать и устранять все зарегистрированные ошибки безопасности.

f. Ежедневно просматривать все события безопасности, журналы системных компонентов, хранящих, обрабатывающих или передающих данные держателей карт, журналы критических компонентов системы, а также журналы серверов и компонентов системы, выполняющих функции обеспечения безопасности.

9. Шлюзы безопасности

Третья сторона должна по меньшей мере:

a. Требовать строгой аутентификации для административного и/или управленческого доступа к Шлюзам безопасности, включая, помимо прочего, любой доступ с целью просмотра файлов журналов.

b. Иметь и использовать документированные средства управления, политики, процессы и процедуры, обеспечивающие отсутствие у неуполномоченных пользователей административного и/или управленческого доступа к Шлюзам безопасности и адекватность уровней авторизации пользователей для администрирования и управления Шлюзами безопасности.

c. Не реже одного раза в шесть (6) месяцев проверять защиту конфигурации Шлюзов безопасности, выбирая образец Шлюза безопасности и проверяя, обеспечивает ли каждый набор стандартных правил и набор параметров конфигурации следующее:

    i. Маршрутизация от источников Интернет-протокола (IP) отключена,

    ii. На кольцевой адрес наложен запрет на вход во внутреннюю сеть,

    iii. Установлены фильтры для защиты от спуфинга,

    iv. Широковещательные пакеты не допускаются в сеть,

    v. Перенаправления протокола Internet Control Message Protocol (ICMP) отключены,

    vi. Все наборы правил заканчиваются предписанием «DENY ALL» и

    vii. Каждое правило имеет прослеживаемую связь с конкретным бизнес-запросом.

d. Обеспечить использование инструментов контроля для подтверждения того, что все аспекты Шлюзов безопасности (например, аппаратное, программно-аппаратное и программное обеспечение) постоянно находятся в рабочем состоянии.

e. Обеспечить настройку и внедрение всех Шлюзов безопасности таким образом, чтобы все неработающие Шлюзы безопасности запрещали любой доступ.

f. Входящие пакеты из недоверенной внешней сети должны отсекаться в демилитаризованной зоне («ДМЗ») и не должны пропускаться напрямую в доверенную внутреннюю сеть. Все входящие пакеты, направляемые в доверенную внутреннюю сеть, должны исходить только из ДМЗ. ДМЗ должна быть отделена от недоверенной внешней сети с помощью Шлюза безопасности, а от доверенной внутренней сети с помощью:

i. другого Шлюза безопасности или

ii. того же Шлюза безопасности, который используется для отделения ДМЗ от недоверенной внешней сети. В этом случае Шлюз безопасности должен обеспечить, чтобы пакеты, получаемые из недоверенной внешней сети немедленно удалялись либо, если они не удалены, направлялись только в ДМЗ без какой-либо обработки за исключением, возможно, их регистрации в журнале.

g. Перечисленное далее должно находиться только в пределах доверенной внутренней сети:

i. Любые Данные flydubai, хранящиеся без использования Криптостойкого шифрования,

ii. Официальная регистрационная копия информации

iii. Серверы баз данных,

iv. Все экспортированные журналы и

v. Все среды, используемые для разработки, тестирования, безопасного исполнения программ («песочницы»), производства и любые другие подобные среды; а также все версии исходного кода.

h. Учетные данные для аутентификации, не защищенные с помощью Криптостойкого шифрования, не должны находиться в ДМЗ.

10. Безопасность сети

Третья сторона должна по меньшей мере:

a. По запросу flydubai предоставить flydubai логическую схему сети, отображающую системы и соединения с другими ресурсами, включая маршрутизаторы, коммутаторы, брандмауэры, системы IDS, топологию сети, внешние точки подключения, шлюзы, беспроводные сети и любые другие устройства, которые должны поддерживать flydubai.

b. Соблюдать формальную процедуру утверждения, тестирования и документирования всех сетевых соединений и изменений в конфигурации брандмауэра и маршрутизатора. Настроить брандмауэры так, чтобы они отсекали и регистрировали подозрительные пакеты, а также пропускали только надлежащий и санкционированный трафик, запрещая прохождение через брандмауэр всего остального трафика. Пересматривать правила брандмауэра каждые шесть месяцев.

c. Установить брандмауэры в каждой точке подключения к Интернету и между любой ДМЗ и зоной внутренней сети. Любая система, содержащая Персональную информацию, должна находиться в зоне внутренней сети, отделенной от ДМЗ и других недоверенных сетей

d. Контролировать брандмауэр на границе и внутри периметра для регулировки и защиты потока сетевого трафика, входящего или выходящего за границу, по мере необходимости.

e. Использовать документированный процесс и средства управления для обнаружения и пресечения несанкционированных попыток доступа к Данным flydubai.

f. При предоставлении flydubai услуг и продуктов через Интернет защищать Данные flydubai путем внедрения сетевой ДМЗ. Веб-серверы, предоставляющие услуги flydubai, должны находиться в ДМЗ. Любая система или информационный ресурс, где хранятся Данные flydubai (например, серверы приложений и баз данных), должны находиться в доверенной внутренней сети. Третья сторона должна использовать ДМЗ для предоставления Интернет-услуг и продуктов.

g. Ограничить несанкционированный исходящий трафик от приложений, обрабатывающих, хранящих или передающих Данные flydubai, IP-адресами в пределах ДМЗ и Интернета.

h. При использовании технологий беспроводных сетей на основе радиочастот (RF) для выполнения или поддержки услуг и продуктов, предоставляемых flydubai, Третья сторона должна обеспечить, чтобы все передаваемые Данные flydubai были защищены с помощью соответствующих технологий шифрования, достаточных для защиты конфиденциальности Данных flydubai; однако при условии, что в любом случае длина ключа, используемого для такого шифрования, должна составлять не менее 256 бит для симметричного шифрования и 2048 бит для асимметричного шифрования. Регулярно сканировать, выявлять и отключать несанкционированные точки беспроводного доступа.

11. Требования к подключению

В случае, если Третья сторона имеет или должна получить возможность подключения к ресурсам Данных flydubai в связи с Соглашением, то в дополнение к вышеизложенному, если Третья сторона имеет или получает возможность подключения к среде flydubai, Третья сторона должна по меньшей мере:

a. Использовать только взаимно согласованные средства и методики подключения для соединения среды flydubai с ресурсами Третьей стороны.

b. НЕ устанавливать соединение со средой flydubai без предварительного письменного согласия flydubai.

c. Предоставлять flydubai доступ к любым соответствующим объектам инфраструктуры Третьей стороны в обычное рабочее время для обслуживания и поддержки любого оборудования (например, маршрутизатора), предоставленного flydubai в рамках Соглашения для подключения к ресурсам Данных flydubai.

d. Использовать любое оборудование, предоставленное flydubai в рамках Соглашения для подключения к среде flydubai, только для предоставления тех услуг и продуктов или выполнения тех функций, которые в явной форме указаны в Соглашении.

e. Если согласованная методика подключения требует, чтобы Третья сторона внедрила Шлюз безопасности, вести журналы всех сеансов с использованием такого Шлюза безопасности. Эти журналы сеансов должны содержать достаточно подробную информацию для идентификации конечного пользователя или приложения, IP-адрес отправителя, IP-адрес получателя, используемые порты/протоколы сетевого обслуживания и продолжительность доступа. Журналы сеансов должны храниться на протяжении не менее шести (6) месяцев с момента создания сеанса.

f. Немедленно прерывать или разрывать любое соединение со средой flydubai в том случае, если Третья сторона считает, что имело место нарушение или несанкционированный доступ, или по указанию flydubai, если flydubai, по своему усмотрению, считает, что имело место нарушение безопасности или несанкционированный доступ или неправомерное использование средств передачи Данных flydubai или любой информации, систем и других ресурсов flydubai.

12. Мобильные и портативные устройства

Третья сторона должна по меньшей мере:

a. Использовать Криптостойкое шифрование для защиты Данных flydubai, передаваемых или доступных в удаленном режиме через Мобильные и портативные устройства с функциями сетевой осведомленности.

b. В случае использования Мобильных и портативных устройств с функциями сетевой осведомленности, не являющихся ноутбуками, для доступа к Данным flydubai и/или их хранения, такие устройства должны быть наделены функцией удаления всех сохраненных копий Данных flydubai при получении по сети должным образом аутентифицированной команды. (Примечание: такая функция часто называется функцией «удаленного стирания»).

c. Внедрить документированные политики, процедуры и стандарты, обеспечивающие, чтобы Уполномоченная сторона, под чьим физическим управлением должно находиться Мобильное и портативное устройство с функциями сетевой осведомленности, не являющееся ноутбуком и хранящее Данные flydubai, незамедлительно инициировала удаление всех Данных flydubai в случае утери или кражи устройства.

d. Внедрить документированные политики, процедуры и стандарты, обеспечивающие, чтобы Мобильные и портативные устройства, не являющиеся ноутбуками и не наделенные функциями сетевой осведомленности, автоматически удаляли все сохраненные копии Данных flydubai после ряда последовательных неудачных попыток входа в систему.

e. Иметь документированные политики, процедуры и стандарты, обеспечивающие, чтобы любые Мобильные и портативные устройства, используемые для доступа к Данным flydubai и/или их хранения:

    i. Находились в физическом владении Уполномоченных сторон;

    ii. Были физически защищены в тех случаях, когда они не находятся в физическом владении Уполномоченных сторон; или

    iii. Обеспечивали быстрое и надежное удаление их хранилища данных в тех случаях, когда они не находятся в физическом владении Уполномоченной стороны или не имеют физической защиты либо после 10 неудачных попыток доступа.

f. Перед предоставлением доступа к Данным flydubai, хранящимся на Мобильных и портативных устройствах или доступным с их помощью, Третья сторона должна внедрить и использовать процесс, обеспечивающий соблюдение следующих условий:

    i. Пользователь является Уполномоченной стороной, обладающей соответствующим правом доступа; и

    ii. Личность пользователя была подтверждена.

g. Внедрить политику, запрещающую использование любых Мобильных и портативных устройств, которые не администрируются и/или не управляются Третьей стороной или flydubai, для доступа к Данным flydubai и/или их хранения.

h. Не менее одного раза в год проверять характер использования и средства управления для всех Мобильных и портативных устройств, администрируемых или управляемых Третьей стороной, чтобы убедиться, что Мобильные и портативные

устройства соответствуют применимым Техническим и организационным мерам безопасности.

13. Безопасность при транспортировке

Третья сторона должна по меньшей мере:

a. Использовать Криптостойкое шифрование для передачи Данных flydubai за пределы сетей, управляемых flydubai или Третьей стороной, или при передаче Данных flydubai по любой недоверенной сети.

b. Если записи, содержащие Данные flydubai, в бумажном формате, на микрофишах или электронных носителях, подлежат физической передаче, транспортировать их с помощью безопасной курьерской службы или другим отслеживаемым способом доставки, в надежной упаковке, в соответствии со спецификациями изготовителя. Любые Данные flydubai должны перевозиться в запертых контейнерах.

14. Безопасность при хранении

Третья сторона должна по меньшей мере:

a. Использовать Криптостойкое шифрование для защиты Данных flydubai при хранении.

b. Не хранить Данные flydubai в электронном виде за пределами сетевой среды Третьей стороны (или собственной защищенной компьютерной сети flydubai), если устройство хранения (например, резервная магнитная лента, ноутбук, карта памяти, компьютерный диск и т.д.) не защищено Криптостойким шифрованием.

c. Не хранить Данные flydubai на съемных носителях (например, USB-накопителях, флеш-картах, картах памяти, магнитных лентах, компакт-дисках или внешних жестких дисках), кроме как: для резервного копирования, обеспечения непрерывности бизнеса, аварийного восстановления и обмена данными, как это разрешено и требуется по договору между Третьей стороной и flydubai. Если съемные носители используются для хранения Персональной информации или Конфиденциальной информации в соответствии с исключениями, указанными в данном подразделе, информация должна быть защищена с помощью Криптостойкого шифрования. Для съемных носителей и устройств хранения данных функция автозапуска должна быть отключена.

d. Надлежащим образом хранить и защищать записи, содержащие Данные flydubai, в бумажном формате или на микрофишах, в местах, доступ к которым разрешен только уполномоченному персоналу.

e. При отсутствии иных письменных указаний со стороны flydubai, при сборе, генерации или создании Данных flydubai в бумажном формате и на резервных носителях для, через, от имени или под брендом flydubai убедиться, что такая информация является Персональной информацией или Конфиденциальной информацией, и, при наличии возможности, снабдить такую информацию flydubai пометкой «Конфиденциально». Третья сторона признает, что Данные flydubai являются и будут оставаться собственностью flydubai независимо от наличия или отсутствия пометки.

15. Возврат, хранение, уничтожение и удаление

Третья сторона должна по меньшей мере:

a. Без дополнительной оплаты со стороны flydubai, по запросу flydubai или после прекращения действия Соглашения предоставить flydubai копии любых Данных flydubai в течение тридцати (30) календарных дней после такого запроса или прекращения действия Соглашения. Третья сторона должна вернуть или, по выбору flydubai, уничтожить все Данные flydubai, включая электронные, бумажные и защищенные резервные копии в сроки, предусмотренные Соглашением, или, если это не предусмотрено Соглашением, в течение девяноста календарных (90) дней после наиболее раннего из следующих событий: (i) истечения срока действия или расторжения Соглашения, (ii) запроса flydubai о возврате Данных flydubai, или (iii) даты, когда Третья сторона перестает нуждаться в Данных flydubai для выполнения своих обязательств и предоставления продуктов по Соглашению.

b. В случае, если flydubai одобрит уничтожение Данных flydubai в качестве альтернативы их возврату, подтвердить в письменном виде за подписью должностного лица Третьей стороны, что в результате уничтожения Данные flydubai становятся невосстановимыми и не подлежащими восстановлению. Третья сторона должна полностью уничтожить все копии Данных flydubai на всех носителях и во всех системах, где хранятся Данные flydubai, включая, помимо прочего, носители и системы ранее одобренных Уполномоченных сторон. Такая информация должна быть уничтожена согласно стандартной отраслевой процедуре полного уничтожения, такой как DOD 5220.22M или NIST Special Publication 800-88, или с использованием рекомендованного производителем размагничивающего устройства для соответствующей системы. До такого уничтожения Третья сторона должна соблюдать все применимые Технические и организационные меры безопасности для защиты безопасности, приватности и конфиденциальности Данных flydubai.

c. Удалять Персональную информацию и Конфиденциальную информацию flydubai таким образом, чтобы ее невозможно было восстановить в пригодном для использования формате. Бумаги, слайды, микрофильмы, микрофиши и фотографии должны уничтожаться путем перекрестного измельчения или сжигания. Материалы, которые содержат Данные flydubai, подлежащие уничтожению, следует хранить в защищенных контейнерах и транспортировать с помощью надежной третьей стороны.

16. Реагирование на инциденты и уведомление об инцидентах

Третья сторона должна по меньшей мере:

a. Внедрить и использовать Процесс управления инцидентами и соответствующие процедуры, а также обеспечить такой Процесс управления инцидентами и процедуры специализированными кадровыми ресурсами. Незамедлительно и ни в коем случае не позднее чем за двадцать четыре (24) часа уведомлять flydubai о любых предполагаемых или подтвержденных атаках, вторжениях, несанкционированном доступе, потере или других инцидентах, касающихся информации, систем или других ресурсов flydubai.

b. После уведомления flydubai регулярно сообщать flydubai об обновлениях статуса, которые включают, помимо прочего, действия, предпринятые для разрешения такого инцидента, через взаимно согласованные промежутки времени или во взаимно согласованные сроки в течение всего периода инцидента и в разумно возможные кратчайшие сроки после закрытия инцидента; предоставлять flydubai письменный отчет с описанием инцидента, действий, предпринятых Третьей стороной в рамках реагирования, и планов Третьей стороны относительно будущих действий по предотвращению повторения подобного инцидента.

c. Не сообщать и не разглашать публично сведения о любом таком нарушении безопасности информации, систем или других ресурсов flydubai до предварительного уведомления flydubai и принятия совместно с flydubai мер по уведомлению соответствующих региональных, государственных или местных правительственных органов или служб кредитного мониторинга, а также лиц, пострадавших от такого нарушения, и любых соответствующих средств массовой информации, определенных законом.

d. Внедрить процесс, позволяющий оперативно выявлять нарушения в отношении средств управления безопасностью, в том числе изложенные в настоящей Политике, со стороны Третьих сторон. Выявленные нарушители должны быть подвергнуты соответствующим дисциплинарным взысканиям в соответствии с применимым

законодательством. Несмотря на вышесказанное, нарушители остаются под управлением Третьих сторон. flydubai не считается работодателем Третьей стороны.

17. Управление непрерывностью бизнеса и аварийное восстановление

Третья сторона должна по меньшей мере:

a. Разработать, исполнять, контролировать и пересматривать планы обеспечения непрерывности бизнеса для каждого территориального подразделения и планы аварийного восстановления для каждой основной технологии с целью минимизации воздействия на flydubai, связанного с выполнением Третьей стороной своих обязательств по Соглашению. Такие планы должны включать: перечень ресурсов, предназначенных для обеспечения непрерывности бизнеса и аварийного восстановления, установленное целевое время восстановления и целевые точки восстановления, ежедневное резервное копирование данных и систем, хранение резервных носителей и записей за пределами производственного объекта, защиту записей и планы на случай непредвиденных обстоятельств, соответствующие требованиям Соглашения. Обеспечить надежное хранение таких планов за пределами производственного объекта и их доступность Третьей стороне по мере необходимости.

b. По запросу flydubai предоставить flydubai документированный план обеспечения непрерывности бизнеса, гарантирующий, что Третья сторона в состоянии выполнить свои договорные обязательства по Соглашению и настоящему документу, включая требования любого применимого технического задания или соглашения об уровне обслуживания. Такие планы должны обеспечивать восстановление и вместе с тем защиту целостности и конфиденциальности Данных flydubai.

c. Использовать документированные процедуры безопасного резервного копирования и восстановления Данных flydubai, которые должны включать как минимум процедуры транспортировки, хранения и удаления резервных копий Данных flydubai и, по запросу flydubai, предъявлять такие документированные процедуры flydubai.

d. Обеспечить создание резервных копий всех хранящихся Данных flydubai или программного обеспечения и конфигураций систем, используемых flydubai, не реже одного раза в неделю.

e. Регулярно, но не реже одного раза в год или после любого существенного изменения в планах обеспечения непрерывности бизнеса или аварийного восстановления, проводить всестороннее тестирование таких планов исключительно за счет Третьей стороны. Такое тестирование должно обеспечивать надлежащее функционирование технологий, подвергшихся воздействию, и внутреннюю осведомленность о таких планах. Планы обеспечения непрерывности бизнеса и аварийного восстановления должны обновляться как минимум один раз в год или так часто, как это необходимо в связи со значительными изменениями в бизнесе и/или технологической среде.

f. Оперативно пересматривать свой план обеспечения непрерывности бизнеса для учета дополнительных или возникающих источников или сценариев угроз и в разумные сроки по запросу предоставлять flydubai высокоуровневую сводку по планам и тестированию.

g. Обеспечить круглосуточное наблюдение за всеми местами размещения или обработки Данных flydubai, принадлежащими Третьей стороне или используемыми по договору Третьей стороной, на предмет проникновения, пожара, затопления и других угроз со стороны окружающей среды.

18. Нормативно-правовое соответствие и аккредитации

Третья сторона должна по меньшей мере:

a. Сохранять полные и точные записи, относящиеся к выполнению ее обязательств, вытекающих из настоящей Политики, и к соблюдению Третьей стороной настоящей Политики, в формате, позволяющем проводить оценку или аудит, на протяжении не менее трех (3) лет или дольше, если это может потребоваться в соответствии с постановлением суда или гражданским либо регуляторным разбирательством. Несмотря на вышесказанное, Третья сторона обязана вести журналы безопасности в течение как минимум одного (1) года после любого непрерывного периода выполнения Соглашения.

b. Разрешить flydubai, без дополнительных для нее затрат, после заблаговременного уведомления, проводить периодические оценки безопасности или аудиты Технических и организационных мер безопасности, принимаемых Третьей стороной, в ходе которых flydubai должна направлять Третьей стороне опросные листы и письменные запросы на документацию. На все запросы Третья сторона должна немедленно или по взаимному соглашению предоставлять письменные ответы и свидетельства, если это применимо. По запросу flydubai на проведение ею аудита, Третья сторона должна запланировать аудит безопасности, который должен начаться в течение десяти (10) рабочих дней после такого запроса. flydubai может потребовать доступ к объектам, системам, процессам и процедурам для оценки среды управления безопасностью Третьей стороны.

c. По запросу flydubai подтверждать соответствие настоящему документу и подтверждающим сертификатам PCI-DSS, ISO 27001/27002, SOC 2 последних версий или аналогичным критериям оценки Третьей стороны и любого субподрядчика или третьей стороны, осуществляющей обработку, доступ, хранение или управление от имени Третьей стороны. Если Третья сторона не может подтвердить соответствие, она должна предоставить письменный отчет с подробным описанием того, в чем она не соответствует требованиям, и план корректирующих действий для достижения соответствия требованиям.

d. В случае, если flydubai по своему усмотрению считает, что имело место нарушение безопасности, о котором flydubai не было сообщено в соответствии с настоящим Соглашением и Процессом управления инцидентами Третьей стороны, запланировать аудит или оценку, которые должны начаться в течение двадцати четырех (24) часов после уведомления flydubai о необходимости проведения оценки или аудита.

e. В течение тридцати (30) календарных дней после получения результатов оценки или отчета об аудите предоставить flydubai письменный отчет с описанием корректирующих действий, которые Третья сторона осуществила или предлагает осуществить, с указанием сроков и текущего статуса каждого корректирующего действия. Третья сторона должна обновлять этот отчет flydubai каждые тридцать (30) календарных дней, сообщая о статусе всех корректирующих действий вплоть до даты их реализации. Третья сторона должна выполнить все корректирующие действия в течение девяноста (90) дней с момента получения Третьей стороной результатов оценки или отчета об аудите или в течение иного периода времени, если такой период времени был взаимно согласован сторонами в письменном виде в течение не более чем тридцати (30) дней с момента получения Третьей стороной результатов оценки или отчета об аудите.

f. Соответствовать в настоящее время и продолжать соответствовать любым применимым государственным стандартам информационной безопасности и требованиям к отчетности, а также ISO 27001/27002. В той степени, в которой Третья сторона обрабатывает номера платежных счетов или любую другую связанную с ними платежную информацию, Третья сторона должна соответствовать самой последней версии стандарта Payment Card Industry (PCI-DSS) в рамках всего комплекса систем, обрабатывающих эту информацию, и продолжать поддерживать это соответствие. Если Третья сторона больше не соответствует стандарту PCI-DSS в рамках любой части комплекса систем обработки данных, относящихся к PCI, она должна незамедлительно уведомить об этом flydubai, немедленно и без неоправданных задержек приступить к устранению такого несоответствия и по запросу регулярно предоставлять flydubai информацию о статусе корректирующих действий по устранению несоответствия.

19. Стандарты, передовые методы, правила и законы

В случае, если Третья сторона обрабатывает, получает доступ, просматривает, хранит или управляет Данными flydubai, относящимися к персоналу, партнерам, филиалам, клиентам flydubai; или сотрудникам клиентов flydubai, подрядчикам, субподрядчикам или поставщикам; Третья сторона должна соблюдать Технические и организационные меры безопасности, не менее строгие, чем те, которых требуют применимые международные, региональные, государственные и местные руководства, нормы, директивы и законы.