Требования информационной безопасности

1. Введение

Поставщик и CWT заключили соглашение, в соответствии с которым Поставщик соглашается предоставлять услуги и/или продукты в соответствии с условиями этого соглашения (« **Соглашение** »). Поставщик соглашается с тем, что он должен соблюдать и обязывает Третьих лиц, действующих от его имени , соблюдать требования информационной безопасности, содержащиеся в настоящем документе (« **Требования информационной безопасности ») ,** и требуемые меры информационной безопасности (« **Технические и организационные меры безопасности** »). Требования информационной безопасности и Технические и организационные меры безопасности включены в Соглашение и являются его неотъемлемой частью.

2. Определения

2.1 Если иное не указано или не расширено в настоящем документе, определенные термины имеют то же значение, что и в Соглашении. К настоящим Требованиям информационной безопасности применяются следующие определенные термины . В случае противоречия между определениями, содержащимися в Соглашении, и определениями, содержащимися в настоящем документе, определение, содержащееся в настоящем документе, имеет преимущественную силу в отношении требований информационной безопасности.

«**Аффилированные лица**», если иное не определено в Соглашении, означает, применительно к стороне, любую компанию или другое юридическое лицо, которое на дату подписания Соглашения прямо или косвенно: (i) контролирует сторону; или (ii) контролируется стороной; или (iii) контролируется компанией или юридическим лицом, которое прямо или косвенно контролирует сторону. Для этих целей «контроль» означает право на осуществление более чем пятидесяти процентов (50%) голосов или аналогичное право собственности; но только до тех пор, пока такой контроль будет продолжать существовать.

«Уполномоченный сотрудник» означает сотрудников Поставщика, которым необходимо знать или иным образом получать доступ к Конфиденциальной информации и Личной информации, чтобы позволить Поставщику выполнять свои обязательства по Соглашению.

«**Уполномоченная сторона» или «Уполномоченные стороны**» означает (i) уполномоченных сотрудников Поставщика; и (ii) Третьи стороны, которым необходимо знать или иным образом получать доступ к Личной информации и Конфиденциальной информации, чтобы позволить Поставщику выполнять свои обязательства по Соглашению, и которые связаны письменными обязательствами в отношении конфиденциальности и другими обязательствами, достаточными для защиты Личной информации и Конфиденциальной информации. в соответствии с условиями Соглашения и настоящего документа.

«Конфиденциальная информация » означает любую коммерческую, частную или иную конфиденциальную информацию, относящуюся к (a) CWT, ее партнерам и ее аффилированным лицам; (b) клиент CWT и сотрудники, подрядчики, субподрядчики или поставщики клиента CWT; (c) персонал CWT; (d) его независимые партнеры и участники совместного предприятия; или (e) содержание и/или цель Соглашения, будь то устное, письменное или любым другим способом, которое может прямо или косвенно попасть во владение Продавца или во владение Уполномоченных сторон в результате или в связи с Соглашение. Во избежание сомнений, все Рабочие продукты должны представлять собой Конфиденциальную информацию.

«CWT» , если иное не определено в Соглашении, означает юридическое лицо CWT, указанное в Соглашении, а также его Аффилированные лица.

«**Демилитаризованная зона**» или « **DMZ** » — это сеть или подсеть, расположенная между доверенной внутренней сетью, такой как корпоративная частная локальная сеть (LAN), и ненадежной внешней сетью, такой как общедоступный Интернет. DMZ помогает предотвратить прямой доступ внешних пользователей к внутренним системам и другим ресурсам.

«Процесс управления инцидентами» — это разработанный Поставщиком, задокументированный процесс и процедура, которым необходимо следовать в случае фактического или предполагаемого нападения, вторжения, несанкционированного доступа, потери или другого нарушения, связанного с конфиденциальностью, доступностью или целостностью. личной информации и конфиденциальной информации CWT.

«Маскирование» — это процесс сокрытия информации, отображаемой на экране.

«Мобильные и портативные устройства» означают мобильные и/или портативные компьютеры, устройства, носители и системы, которые можно легко переносить, перемещать, транспортировать или передавать, которые используются в связи с Соглашением. Примеры таких устройств включают портативные компьютеры, планшеты, жесткие диски USB, карты памяти USB, персональные цифровые помощники (КПК), мобильные телефоны или телефоны с данными, а также любые другие беспроводные, периферийные или съемные устройства с возможностью хранения конфиденциальной информации и личной информации. .

«Личная информация», если иное не определено в Соглашении, означает , как определено в Регламенте (ЕС) 2016/679 и других применимых глобальных законах об информационной безопасности, защите данных и конфиденциальности, означает любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу, которое может быть прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один или несколько факторов, характерных для его или ее физической, физиологической, умственной, экономической, культурной или социальной идентичности. Личная информация принадлежит CWT, а не Поставщику.

«Шлюз безопасности» означает набор механизмов управления между двумя или более сетями с разными уровнями доверия, которые фильтруют и регистрируют трафик, проходящий или пытающийся пройти между сетями и соответствующими серверами администрирования и управления. Примеры шлюзов безопасности включают брандмауэры, серверы управления брандмауэрами, блоки переходов, пограничные контроллеры сеансов, прокси-серверы и устройства предотвращения вторжений.

«Строгая аутентификация» означает использование механизмов аутентификации и методологий аутентификации, требующих множественных факторов аутентификации, включая по крайней мере два из следующих: (1) Знание — что-то известное пользователю, например , пароль или личный идентификационный номер, (2) Владение — что-то у пользователя есть, например, жетон, смарт-карта, мобильный телефон и (3) неотъемлемая часть — то, чем является пользователь, например отпечаток пальца.

«Надежное шифрование» означает использование технологий шифрования с минимальной длиной ключа 256 бит для симметричного шифрования и 1024 бит для асимметричного шифрования, надежность которых обеспечивает разумную уверенность в том, что она защитит зашифрованную информацию от несанкционированного доступа и достаточна для защиты конфиденциальности. и конфиденциальность зашифрованной информации , и который включает в себя документированную политику управления ключами шифрования и связанными с ними процессами, достаточными для защиты конфиденциальности и конфиденциальности ключей и паролей, используемых в качестве входных данных для алгоритма шифрования. Сильное шифрование включает, но не ограничивается: SSL v3.0+/TLS v1.2, протокол туннелирования точка-точка (PPTP), AES 256, FIPS 140-2 (только для правительства США), RSA 1024 бит, SHA1/SHA2 /SHA3, безопасность интернет-протокола (IPSEC), SFTP, SSH, Vormetric v4 или WPA2.

«Технические и организационные меры безопасности» означает любые действия, требуемые в соответствии с настоящими Требованиями информационной безопасности. для доступа, управления, передачи, обработки, хранения, сохранения и уничтожения информации или данных; раскрывать и уведомлять затронутые стороны в соответствии с Соглашением и применимыми законами о конфиденциальности информации и защите данных; а также для защиты информации или данных, чтобы обеспечить доступность, целостность, конфиденциальность и неприкосновенность частной жизни, или уведомлять отдельных лиц о любой неспособности защитить такую информацию или данные. Меры включают, помимо прочего, те, которые требуются или интерпретируются как требуемые в соответствии с Общим регламентом ЕС по защите данных (GDPR), Директивой ЕС о платежных услугах, Законом штата Калифорния о конфиденциальности потребителей, NYS DFS 23 NYCRR 500 , Законом Грэмма-Лича Блайли США (GLBA), Закон США о переносимости и подотчетности медицинского страхования (HIPAA), требования ЕС/Швейцарии о конфиденциальности данных, а также любые другие международные законы и законы США, официальные юридические толкования или прецеденты , касающиеся информации или данных в соответствии с Соглашением .

«**Третья сторона»** или «**Третья сторона**» означает Продавца субподрядчики , консультанты, временный персонал, подрядчики или дополнительные поставщики и/или агенты, действующие от имени Поставщика, и не включает какое-либо определение Третьей стороны в соответствии с применимым законодательством ЕС, США или другим международным законодательством.

«**Продавец**» означает организацию-заказчика, указанную в Соглашении, вместе с ее Аффилированными лицами и Третьими сторонами.

3 . Организация информационной безопасности

Поставщик должен , как минимум :

3.1 Убедитесь, что только Уполномоченные стороны имеют доступ к Личной информации и Конфиденциальной информации.

3.2 Внедрить технические и организационные меры безопасности, которые являются не менее строгими, чем лучшие практики информационной безопасности, для защиты целостности, доступности и конфиденциальности Конфиденциальной информации, Личной информации и другой непубличной информации и предотвращения несанкционированного доступа, приобретения, раскрытия, уничтожения, изменения. , случайная потеря, неправильное использование или повреждение Персональной информации или Конфиденциальной информации.

3.3 Установить, внедрить и поддерживать в соответствии с передовой отраслевой практикой , политикой и программой организационные, операционные, административные, физические, технические и организационные меры безопасности, необходимые для (1) предотвращения любого доступа неуполномоченных сторон к личной информации и конфиденциальной информации в способом, не разрешенным Соглашением или настоящими Требованиями информационной безопасности, и (2) соблюдать все применимые законы и правила, а также применимые отраслевые стандарты.

3.4 Предоставлять Уполномоченным сторонам, которые будут иметь доступ к Личной информации и Конфиденциальной информации , наблюдение, руководство и обучение по техническим и организационным мерам безопасности, включая обучение, которое включает практические упражнения, соответствующие текущим сценариям угроз, и дает обратную связь тем, кто проходит обучение . Поставщик должен обеспечить обучение техническим и организационным мерам безопасности после найма Уполномоченного сотрудника и до того, как Уполномоченное лицо получит доступ к Конфиденциальной информации и Личной информации. Повышение квалификации должно проводиться не реже одного раза в год и как можно скорее после любого существенного изменения технических и организационных мер безопасности Поставщика.

3.5 Обеспечить специализированное обучение специально для Уполномоченных сторон с важными обязанностями по обеспечению безопасности, включая, помимо прочего, функции управления персоналом или информационных технологий, а также любые функции администратора технологий. Как минимум, специализированное обучение должно включать, в зависимости от роли, процедуры информационной безопасности, приемлемое использование ресурсов информационной безопасности, текущие угрозы информационным системам, функции безопасности конкретных систем и процедуры безопасного доступа.

3.6 Принимать разумные меры для предотвращения несанкционированного доступа или потери Персональной информации и Конфиденциальной информации, а также служб, систем, устройств или носителей, содержащих эту информацию.

3.7 Используйте процессы и процедуры оценки рисков для регулярной оценки систем, используемых для предоставления услуг или продуктов для CWT. Поставщик должен устранить такие риски как можно скорее и соизмеримо с уровнем риска для Личной информации и Конфиденциальной информации с учетом угроз, известных на момент идентификации. Управляйте процессом, позволяющим сообщать о рисках или предполагаемых инцидентах группе безопасности Поставщика.

3.8 В той степени, в которой Поставщик оказывает услуги в соответствии с Соглашением на объектах CWT или с использованием услуг, систем, устройств или носителей, принадлежащих, эксплуатируемых или управляемых CWT, Поставщик должен обеспечить соблюдение всеми Уполномоченными сторонами всех политик CWT, предоставленных Поставщику , по его запрос, которые применимы к такому доступу. Поставщик должен незамедлительно уведомить CWT в письменной форме, когда Уполномоченной стороне больше не требуется доступ к Личной информации или Конфиденциальной информации , чтобы Поставщик мог предоставлять продукты или услуги CWT , в том числе, помимо прочего , когда Уполномоченная сторона прекращает свою деятельность или иным образом прекращает свою деятельность. услуги по договору.

3.9 Вести записи об Уполномоченных сторонах и ресурсах Поставщиков, которые получают доступ, передают, поддерживают, хранят или обрабатывают Личную информацию и Конфиденциальную информацию.

3.10 Проводить всесторонние проверки биографических данных всех Уполномоченных сторон перед приемом на работу, насколько это разрешено законом . Комплексная проверка биографических данных физических лиц должна включать , как минимум, предыдущую историю трудоустройства, судимость, кредитную историю, проверку рекомендаций и любые дополнительные стандартные требования к проверке биографических данных.

3.11 Назначить одного или нескольких квалифицированных сотрудников, отвечающих за поддержание его программы информационной безопасности, и он должен не реже одного раза в год отчитываться о своей программе информационной безопасности

перед советом директоров Поставщика или эквивалентным руководящим органом. Поставщик должен обеспечить, чтобы его сотрудники службы безопасности имели разумный и необходимый опыт и подготовку в области информационной безопасности, включая поддержание знаний об изменяющихся угрозах и мерах противодействия. По запросу Поставщик должен предоставить CWT контактное лицо по всем вопросам, связанным с информационной безопасностью.

3.12 Требовать от Уполномоченных сторон договорных обязательств о неразглашении или конфиденциальности до предоставления им доступа к Личной информации и Конфиденциальной информации.

3.13 Обеспечить, чтобы все Уполномоченные стороны, которые могут выполнять работу в соответствии с Соглашением или которые могут иметь доступ к Личной информации или Конфиденциальной информации , соблюдали настоящие Технические и организационные меры безопасности, что должно быть подтверждено письменным соглашением, не менее ограничительным, чем настоящие Требования информационной безопасности. .

4. Физическая и экологическая безопасность

Поставщик должен , как минимум :

4.1 Убедитесь, что все системы и другие ресурсы Поставщика, предназначенные для использования несколькими пользователями , расположены в безопасных физических помещениях с ограниченным доступом и доступом только для уполномоченных лиц.

4.2 Отслеживайте и записывайте в целях аудита доступ к физическим объектам, содержащим системы и другие ресурсы, предназначенные для использования несколькими пользователями, используемые в связи с выполнением Продавцом своих обязательств по Соглашению.

4.3 Требовать от всех Уполномоченных сторон соблюдения политики чистоты рабочего стола и блокировки экранов рабочих станций перед тем, как покинуть рабочее место.

4.4 Собрать все активы компании при увольнении или расторжении контракта.

4.5 Ограничивать и контролировать физический доступ к своим объектам в соответствии со следующими требованиями:

a. Доступ посетителей регистрируется в течение трех (3) месяцев, включая имя посетителя, компанию, которую он/она представляет, и имя сотрудника, разрешающего физический доступ. Посетители должны постоянно находиться в сопровождении сотрудника Продавца .
b. Доступ ограничен соответствующим персоналом на основе служебной необходимости.

c. Все сотрудники должны носить бейдж с именем, предоставленный компанией, а все посетители или третьи стороны должны носить бейдж гостя/посетителя, предоставленный компанией.
d. Доступ аннулируется немедленно после увольнения персонала Поставщика или Третьего лица , а все механизмы физического доступа, такие как ключи, карты доступа и т. д., возвращаются или отключаются.
e. Центр обработки данных или компьютерный зал запираются , и доступ к ним имеют только те, кому это необходимо для выполнения своих служебных обязанностей.
f. Там, где это разрешено законом, используйте видеокамеры для наблюдения за индивидуальным физическим доступом к уязвимым зонам и регулярно просматривайте такие данные. Видеозапись должна храниться не менее трех (3) месяцев.
g. Оборудование, используемое для хранения, обработки или передачи Личной информации и Конфиденциальной информации , должно быть физически защищено, включая точки беспроводного доступа, шлюзы, портативные устройства, сетевое/коммуникационное оборудование и телекоммуникационные линии.

4.6 Внедрите средства контроля, чтобы свести к минимуму риск физических угроз и защититься от них.

4.7 Поддерживайте все аппаратные активы, обрабатывающие или обрабатывающие Персональную информацию и Конфиденциальную информацию, в соответствии с рекомендованными производителем требованиями к обслуживанию.

4.8 Ограничить конференц-зал и другие общедоступные сети и сетевые разъемы логически и физически от внутренней сети Поставщика и разрешить только пользователям, прошедшим проверку подлинности, или отключить по умолчанию.

4.9 Защитите любое устройство, которое захватывает данные платежной карты посредством прямого физического взаимодействия, от несанкционированного доступа и подмены, периодически проверяя поверхности устройства для обнаружения подделки или подмены; провести обучение персонала, чтобы он знал о попытках несанкционированного доступа или замены устройств.

4.10 Контролируйте и отделяйте точки доступа, такие как зоны доставки и погрузки, а также другие точки от всех центров доступа, управления, хранения или обработки личной информации и конфиденциальной информации.

4.11 Убедитесь, что в центрах обработки данных поставщика есть устройства обогрева, охлаждения, пожаротушения, обнаружения воды и обнаружения тепла/дыма. В центрах обработки данных и компьютерных залах поставщиков не должно быть горючих материалов (например , коробок, бумаги и т. д.) или они должны храниться в металлических шкафах.

5. Контроль доступа

Поставщик должен , как минимум :

5.1 Принимать все разумные меры, чтобы предотвратить доступ кого-либо, кроме Уполномоченных сторон, к Личной информации и Конфиденциальной информации любым способом или в любых целях, не разрешенных CWT и Соглашением.

5.2 Отделяйте информацию CWT от данных других клиентов Поставщика или собственных приложений и информации Поставщика либо с помощью физически отдельных серверов, либо с помощью логических средств управления доступом, когда физическое разделение серверов не реализовано.

5.3 Определить и потребовать от соответствующих владельцев проверять и утверждать доступ к системам, используемым для доступа, обработки, управления или хранения Личной информации и Конфиденциальной информации, по крайней мере, ежеквартально, чтобы исключить несанкционированный доступ ; поддерживать и отслеживать разрешения на доступ.

5.4 Удалить доступ к системам, управляющим Персональной информацией и Конфиденциальной информацией, в течение 24 часов с момента прекращения отношений Уполномоченной стороны с Поставщиком; и поддерживать разумные процедуры для прекращения доступа к таким системам в течение трех рабочих дней , когда это больше не требуется или не имеет отношения к выполнению их обязанностей . Все остальные идентификаторы пользователей должны быть отключены или удалены через 90 календарных дней бездействия.

5.5 Ограничить системному администратору (также известному как root, привилегированный или суперпользователь) доступ к операционным системам, предназначенным для использования несколькими пользователями, только теми лицами, которым требуется такой высокий уровень доступа при выполнении своей работы. Используйте идентификаторы системного администратора выписки с индивидуальными учетными данными пользователя и журналами действий, чтобы управлять доступом с высоким уровнем безопасности и сократить доступ высокого уровня до очень ограниченного числа пользователей. Требовать, чтобы администраторы приложений, баз данных, сети и системы ограничивали доступ пользователей только к командам, данным, системам и другим ресурсам, необходимым им для выполнения авторизованных функций. Системные административные роли и списки доступа должны пересматриваться не реже одного раза в год.

5.6 Применять правило наименьших привилегий (т . е. ограничение доступа только к командам, информации, системам и другим ресурсам, необходимым для выполнения авторизованных функций в соответствии с должностными обязанностями).

5.7 Требовать строгой аутентификации для всех видов административного доступа, не связанных с консолью , любого удаленного доступа и любого административного доступа в облачные среды .

5.8 Запрещать и применять технические и организационные меры безопасности для обеспечения того, чтобы Личная информация не могла копироваться, перемещаться или хранить Личную информацию на локальных жестких дисках, а также вырезать, вставлять или распечатывать Личную информацию.

5.9 Активируйте использование возможностей удаленного доступа только при необходимости, контролируйте их во время использования и немедленно деактивируйте после использования.

5.10 Требовать строгой аутентификации для подключения к внутренним ресурсам поставщика, содержащим личную информацию и конфиденциальную информацию.

6. Идентификация и аутентификация

Поставщик должен , как минимум :

6.1 Назначьте уникальные идентификаторы пользователей отдельным пользователям и назначьте механизмы аутентификации для каждой отдельной учетной записи.

6.2 Используйте задокументированный процесс управления жизненным циклом идентификатора пользователя, включая, помимо прочего, процедуры утвержденного создания учетной записи, своевременного удаления учетной записи и модификации учетной записи (например, изменения привилегий, диапазона доступа, функций/ролей) для любого доступа к Персональным данным и Конфиденциальная информация и во всех средах (например, производственная, тестовая, разработка и т. д.). Такой процесс должен включать проверку прав доступа и действительности учетной записи, которая должна выполняться не реже одного раза в квартал.

6.3 Ограничьте любой доступ к личной информации и конфиденциальной информации теми, кто использует действительный идентификатор пользователя и пароль, и требуйте, чтобы уникальные идентификаторы пользователей использовали одно из следующего: пароль или кодовую фразу, двухфакторную аутентификацию или биометрическое значение.

6.4 Требовать сложности пароля и соблюдать следующие требования к конструкции пароля: минимум двенадцать (12) символов для системных паролей и четыре (4) символа для паролей для планшетов и смартфонов. Системные пароли должны содержать три (3) из следующих символов: верхний регистр, нижний регистр, цифры или специальные символы. Пароли также не должны совпадать с идентификатором пользователя, с которым они связаны, содержать слово из словаря, последовательные или повторяющиеся числа и не должны быть одним из последних 24 паролей. Требовать

истечения срока действия пароля через регулярные промежутки времени, не превышающие девяносто (90) дней. Маскируйте все пароли при отображении.

6.5 Ограничьте число неудачных попыток входа в систему не более чем пятью (5) неудачными попытками входа в систему в течение 24 часов и заблокируйте учетную запись пользователя при достижении этого ограничения в постоянном состоянии. Доступ к учетной записи пользователя может быть повторно активирован впоследствии с помощью ручного процесса, требующего проверки личности пользователя.

6.6 Подтвердите личность пользователя и установите для одноразового использования и сброса пароли уникальные значения для каждого пользователя. Систематически предлагать замену после первого использования.

6.7 Используйте безопасный метод для передачи учетных данных аутентификации (например, паролей) и механизмов аутентификации (например, жетонов или смарт-карт).

6.8 Ограничьте пароли сервисных учетных записей и прокси-серверов минимум 20 символами , включая прописные и строчные буквы, цифры и специальные символы. Меняйте учетную запись службы и пароли прокси-сервера не реже одного раза в год и после увольнения любого, кто знает пароль.

6.9 Завершать интерактивные сеансы или активировать безопасную блокирующую заставку, требующую аутентификации, после периода бездействия, не превышающего пятнадцать (15) минут.

6.10 Используйте метод проверки подлинности, основанный на конфиденциальности личной информации и конфиденциальной информации. Всякий раз, когда учетные данные для аутентификации хранятся, Поставщик должен защищать их с помощью надежного шифрования.

6.11 Настройте системы для автоматического тайм-аута 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).

7. Приобретение, разработка и обслуживание информационных систем .

Поставщик должен , как минимум :

7.1 Отображать предупреждающий баннер на экранах или страницах входа в систему, как указано CWT в письменной форме для продуктов или услуг под торговой маркой CWT или для продуктов и программного обеспечения, разработанных для CWT.

7.2 Верните все устройства доступа, принадлежащие или предоставленные CWT, как можно скорее, но ни в коем случае не позднее, чем через пятнадцать (15) дней после ближайшего из следующих событий:

a. истечение срока действия или расторжение Соглашения;
b. требование CWT о возврате такого имущества; или же
c. дата, когда Продавцу больше не нужны такие устройства.

7.3 Применять эффективную методологию управления приложениями, которая включает технические и организационные меры безопасности в процесс разработки программного обеспечения, и обеспечивать своевременное внедрение технических и организационных мер безопасности, представленных передовым отраслевым опытом.

7.4 Следуйте стандартным отраслевым процедурам разработки, включая разделение доступа и кода между непроизводственной и производственной средами и связанное с этим разделение обязанностей между такими средами.

7.5 Обеспечить регулярную оценку внутренних средств контроля информационной безопасности для разработки программного обеспечения и отражение лучших отраслевых практик, а также своевременно пересматривать и внедрять эти средства контроля.

7.6 Управляйте безопасностью процесса разработки и обеспечьте внедрение и соблюдение методов безопасного кодирования, включая соответствующие средства криптографического контроля, защиту от вредоносного кода и процесс экспертной оценки.

7.7 Проводите тестирование на проникновение функционально завершенных приложений перед выпуском в рабочую среду и после этого не реже одного раза в год и после любых значительных изменений исходного кода или конфигурации, которые соответствуют OWASP, CERT, SANS Top 25 и PCI-DSS. Устраните все уязвимости, которые можно использовать, до развертывания в производственной среде.

7.8 Используйте анонимные или запутанные данные в непроизводственных средах. Никогда не используйте производственные данные в виде обычного текста в любой непроизводственной среде и никогда не используйте личную информацию в непроизводственной среде по какой-либо причине. Убедитесь, что все тестовые данные и учетные записи удалены до выпуска рабочей версии.

7.9 Проверяйте открытый или бесплатный исходный код, одобренный CWT, программное обеспечение, приложения или услуги на наличие недостатков, ошибок, проблем безопасности или несоблюдения условий лицензирования открытого или бесплатного исходного кода. Поставщик должен заблаговременно уведомить CWT об использовании любого открытого или бесплатного исходного кода и, в случае одобрения использования CWT, предоставить CWT название, версию и URL-адрес открытого или бесплатного исходного кода. Поставщик заявляет и гарантирует, что (a)

любой открытый или свободный исходный код, который он использует в своих продуктах или услугах, должен быть лицензирован в соответствии с «разрешительными» лицензиями на открытый или свободный исходный код, а не в соответствии с ограничительными, взаимными, наследственными лицензиями или лицензиями с авторским левом; (b) Поставщик имеет право свободно изменять, адаптировать открытый или свободный исходный код и комбинировать открытый или свободный исходный код или содержать открытый или свободный исходный код с проприетарным кодом, не накладывая ограничений на такие изменения, адаптации или комбинации или проприетарный код, который содержит открытый или свободный исходный код и как они могут быть лицензированы в дальнейшем (совместно « **производные работы** ») и (c) такие производные работы не будут подпадать под какую-либо лицензию на открытый или свободный исходный код, требующую лицензирования производной работы или предоставления ее бесплатного доступа третьим лицам в соответствии с условиями лицензии на открытый или свободный исходный код.

7.10 Не передавать какой-либо код, созданный в соответствии с Соглашением, независимо от стадии разработки, в какой-либо общей или не частной среде, такой как репозиторий кода с открытым доступом, независимо от защиты паролем.

8. Целостность программного обеспечения и данных

Поставщик должен , как минимум :

8.1 В средах, где антивирусное программное обеспечение имеется в продаже, установите и запустите актуальное антивирусное программное обеспечение для сканирования и быстрого удаления или помещения в карантин вирусов и других вредоносных программ из любой системы или устройства.

8.2 Отделите непроизводственную информацию и ресурсы от производственной информации и ресурсов.

8.3 Убедитесь, что команды используют задокументированный процесс контроля изменений для всех системных изменений, включая процедуры возврата для всех производственных сред и процессы внесения экстренных изменений. Включите тестирование, документацию и утверждения для всех системных изменений и требуйте одобрения руководства для значительных изменений в таких процессах.

8.4 Создайте и поддерживайте зону PCI, если поставщик обрабатывает или хранит данные о держателях карт.

8.5 Для приложений, использующих базу данных, позволяющую вносить изменения в Личную информацию и Конфиденциальную информацию, включите и поддерживайте функции ведения журнала аудита транзакций базы данных, которые сохраняют журналы аудита транзакций базы данных в течение как минимум одного (1) года с немедленным доступом к трем месяцам для анализа.

8.6 Проверяйте программное обеспечение, чтобы найти и устранить уязвимости в системе безопасности во время первоначального внедрения, а также после любых существенных модификаций и обновлений.

8.7 Выполнять тестирование обеспечения качества для компонентов безопасности (например, тестирование функций идентификации, аутентификации и авторизации), а также любые другие действия, предназначенные для проверки архитектуры безопасности, во время начальной реализации и после любых значительных модификаций и обновлений.

9. Безопасность системы

Поставщик должен , как минимум :

9.1 Регулярно создавайте и обновляйте самые последние версии потоков данных и системных диаграмм, используемых для доступа, обработки, управления или хранения личной информации и конфиденциальной информации.

9.2 Активно отслеживайте отраслевые ресурсы (например , , www.cert.org и списки рассылки и веб-сайты соответствующих поставщиков программного обеспечения) для своевременного уведомления обо всех применимых предупреждениях о безопасности, относящихся к системам Поставщика и другим информационным ресурсам.

9.3 Эффективно управлять криптографическими ключами, сокращая доступ к ключам за счет наименьшего числа необходимых хранителей, храня секретные и частные криптографические ключи путем шифрования ключом не менее надежного, чем ключ шифрования данных, и храня отдельно от ключа шифрования данных в безопасном криптографическое устройство в наименьшем количестве возможных мест. Изменяйте криптографические ключи по умолчанию при установке и не реже одного раза в два года, а также безопасно утилизируйте старые ключи.

9.4 Сканировать внешние и внутренние системы и другие информационные ресурсы, включая, помимо прочего, сети, серверы, приложения и базы данных, с помощью соответствующего стандартного программного обеспечения для сканирования уязвимостей безопасности, чтобы обнаружить уязвимости безопасности, убедиться, что такие системы и другие ресурсы должным образом защищены, и выявляйте любые несанкционированные беспроводные сети не реже одного раза в квартал и перед выпуском приложений, а также значительных изменений и обновлений в сроки, полученные в результате анализа рисков на основе разумных и общепринятых ИТ-политик и стандартов.

9.5 Убедитесь, что все системы и другие ресурсы Поставщика защищены и остаются защищенными, включая, помимо прочего, удаление или отключение неиспользуемых сетевых и других служб и продуктов (например, finger, rlogin, ftp и простой протокол управления передачей/протокол Интернета (TCP/ IP) услуги и продукты) и установка

системного брандмауэра, оболочек протокола управления передачей (TCP) или аналогичной технологии.

9.6 Развернуть одну или несколько систем обнаружения вторжений (IDS), систем предотвращения вторжений (IPS) или систем обнаружения и предотвращения вторжений (IDP) в активном режиме работы, который отслеживает весь входящий и исходящий трафик систем и других ресурсов в соответствии с Соглашением в средах, где такая технология коммерчески доступна и насколько это практически осуществимо.

9.7 Поддерживать процесс оценки рисков для результатов оценки уязвимостей в соответствии с передовыми отраслевыми практиками для устранения уязвимостей безопасности в любой системе или другом ресурсе, включая, помимо прочего, обнаруженные с помощью отраслевых публикаций, сканирования уязвимостей, сканирования вирусов и просмотра журналов безопасности. , и своевременно применяйте соответствующие исправления безопасности с учетом вероятности того, что такая уязвимость может быть использована или находится в процессе эксплуатации. Выводы и исправления, связанные с оценкой критических уязвимостей, должны быть исправлены сразу после их выпуска и ни в коем случае не позднее, чем через 7 дней после выпуска. Результаты оценки высокой уязвимости и исправления должны быть исправлены в течение 30 дней после выпуска. Результаты оценки уязвимостей и исправления средней степени должны быть исправлены в течение 90 календарных дней. Результаты оценки низкой уязвимости и исправления должны быть исправлены в течение 120 календарных дней.

9.8 Проводите внутреннее и внешнее тестирование сети и сегментации на проникновение не реже одного раза в год и после любого значительного обновления или модификации инфраструктуры или приложений.

9.9 Удаляйте или отключайте неавторизованное программное обеспечение, обнаруженное в системах Поставщика, и применяйте стандартные средства контроля вредоносного ПО, включая установку, регулярное обновление и рутинное использование программных продуктов для защиты от вредоносных программ во всех службах, системах и устройствах, которые могут использоваться для доступа к Персональным данным и CWT. Конфиденциальная информация. По возможности используйте надежное и передовое в отрасли антивирусное программное обеспечение и следите за тем, чтобы такие определения вирусов постоянно обновлялись.

9.10 Поддерживать актуальное программное обеспечение во всех службах, системах и устройствах, которые могут использоваться для доступа к Персональным данным и Конфиденциальной информации CWT, включая надлежащее обслуживание операционных систем и успешную установку достаточно современных исправлений безопасности.

9.11 Назначьте обязанности по администрированию безопасности для настройки хост-операционных систем конкретным лицам.

9.12 Измените все имена учетных записей по умолчанию и/или пароли по умолчанию.

10. Мониторинг

Поставщик должен , как минимум :

10.1 Хранить данные журнала для Личной информации и Конфиденциальной информации в течение не менее 12 месяцев с даты создания данных журнала и предоставлять журнал и такие данные CWT в разумные сроки и по запросу, если иное не указано в Соглашении. Журналы должны быть предназначены для обнаружения инцидентов и реагирования на них и включать, но не ограничиваться:

a. Доступ отдельных пользователей к личной информации и конфиденциальной информации
b. Все действия, предпринятые лицами с административными или корневыми привилегиями
c. Доступ всех пользователей к журналам аудита
d. Неверные попытки логического доступа
e. Использование и изменения механизмов идентификации и аутентификации

10.2 Записывать основные системные действия третьих лиц поставщика для систем, содержащих любую личную информацию и конфиденциальную информацию, и иметь официальную стороннюю программу обеспечения гарантии того, что третьи лица или субподрядчики поставщика имеют соответствующие средства контроля безопасности и сертификаты на месте. провести оценку безопасности облачных вычислений, если CWT данные находятся в облачной среде.

10.3 Ограничьте доступ к журналам безопасности уполномоченными лицами и защитите журналы безопасности от несанкционированного изменения.

10.4 Внедрить механизм обнаружения изменений (например , мониторинг целостности файлов) для оповещения персонала о несанкционированных изменениях важных системных файлов, файлов конфигурации или файлов содержимого; настроить программное обеспечение для еженедельного сравнения важных файлов.

10.5 Не реже одного раза в неделю просматривайте все журналы аудита безопасности и связанных с безопасностью систем, содержащих Персональную информацию и Конфиденциальную информацию, на наличие аномалий, документируйте и своевременно устраняйте все зарегистрированные проблемы безопасности.

10.6 Ежедневно просматривайте все события безопасности, журналы компонентов системы, хранящих, обрабатывающих или передающих данные о держателях карт, журналы критических компонентов системы и журналы серверов и компонентов системы, выполняющих функции безопасности.

11. Шлюзы безопасности

Поставщик должен , как минимум :

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

11.2 Иметь и использовать документированные элементы управления, политики, процессы и процедуры, чтобы гарантировать, что неавторизованные пользователи не имеют административного и/или управленческого доступа к шлюзам безопасности, и что уровни авторизации пользователей для администрирования и управления шлюзами безопасности являются подходящими.

11.3 Имейте строгие средства контроля безопасности электронной почты, такие как настройка протоколов аутентификации DKIM и SPF, которые помогают проверить, что сообщение электронной почты получено из надежного и проверенного источника. Реализация DMARC на принимающих почтовых серверах.

11.4 Не реже одного раза в шесть (6) месяцев проверяйте усиление безопасности конфигураций шлюзов безопасности, выбирая выборку шлюзов безопасности и проверяя, что каждый набор правил по умолчанию и набор параметров конфигурации обеспечивают следующее:

a. Исходная маршрутизация интернет-протокола (IP) отключена,
б. Закольцованному адресу запрещен вход во внутреннюю сеть,
в. Реализованы антиспуфинговые фильтры,
д. Широковещательные пакеты не могут попасть в сеть,
е. Перенаправления протокола управляющих сообщений Интернета (ICMP) отключены,
ф. Все наборы правил заканчиваются оператором «DENY ALL», и
грамм. Каждое правило прослеживается до конкретного бизнес-запроса.

11.5 Убедитесь, что инструменты мониторинга используются для проверки того, что все аспекты шлюзов безопасности (например, аппаратное обеспечение, микропрограммное обеспечение и программное обеспечение) непрерывно работают.

Убедитесь, что все шлюзы безопасности сконфигурированы и внедрены таким образом, что все нерабочие шлюзы безопасности должны запрещать любой доступ.

11.6 Входящие пакеты из ненадежной внешней сети должны заканчиваться в демилитаризованной зоне (« **DMZ** »), и им не должно быть позволено проходить напрямую в доверенную внутреннюю сеть. Все входящие пакеты, направляемые в доверенную внутреннюю сеть, должны исходить только из демилитаризованной зоны. DMZ должна быть отделена от ненадежной внешней сети с помощью шлюза безопасности и должна быть отделена от доверенной внутренней сети с помощью:

a. другой шлюз безопасности или
б. тот же шлюз безопасности, который используется для отделения DMZ от ненадежной внешней сети, и в этом случае шлюз безопасности должен гарантировать, что пакеты, полученные из ненадежной внешней сети, либо немедленно удаляются, либо, если они не удаляются, направляются только в DMZ без какой-либо другой обработки такие входящие пакеты выполняются иначе, чем, возможно, запись пакетов в журнал.

Следующее должно находиться только в доверенной внутренней сети:

a. Любая личная информация и конфиденциальная информация CWT, хранящаяся без использования сильного шифрования,
б. Официальная копия информации
в. серверы баз данных,
д. Все экспортированные журналы и
е. Все среды, используемые для разработки, тестирования, песочницы, производства и любых других подобных сред; и все версии исходного кода.

11.7 Учетные данные аутентификации, не защищенные с помощью сильного шифрования, не должны находиться в демилитаризованной зоне.

12. Сетевая безопасность

Поставщик должен , как минимум :

12.1 По запросу CWT предоставить CWT логическую схему сети, документирующую системы и подключения к другим ресурсам, включая маршрутизаторы, коммутаторы, брандмауэры, системы IDS, топологию сети, внешние точки подключения, шлюзы, беспроводные сети и любые другие устройства, которые должны поддерживать CWT.

12.2 Поддерживать формальный процесс утверждения, тестирования и документирования всех сетевых подключений и изменений в конфигурациях брандмауэра и маршрутизатора. Настройте брандмауэры так, чтобы они блокировали и регистрировали подозрительные пакеты, а также разрешайте только соответствующий и авторизованный трафик, запрещая весь другой трафик через брандмауэр. Пересматривайте правила брандмауэра каждые шесть месяцев.

12.3 Установите брандмауэр при каждом подключении к Интернету и между любой DMZ и внутренней сетевой зоной. Любая система, хранящая личную информацию, должна находиться во внутренней сетевой зоне, отделенной от демилитаризованной зоны и других ненадежных сетей.

12.4 Мониторинг брандмауэра по периметру и внутри для контроля и защиты потока сетевого трафика, входящего или исходящего за границу или границу, по мере необходимости.

12.5 Установите технологии обнаружения угроз, такие как сетевое обнаружение и реагирование (NDR), обнаружение и реагирование на конечных точках (EDR) и расширенное обнаружение и реагирование (XDR), которые предлагают комплексное решение для обнаружения и реагирования на различные кибератаки или атаки программ-вымогателей.

12.6 Поддерживайте документированный процесс и средства контроля для обнаружения и обработки несанкционированных попыток доступа к Персональным данным и Конфиденциальной информации CWT.

12.7 Предоставляя CWT интернет-услуги и продукты, защищать Личную информацию и Конфиденциальную информацию путем создания сети DMZ. Веб-серверы, предоставляющие услуги CWT, должны находиться в демилитаризованной зоне. Любая система или информационный ресурс, хранящий Личную информацию и Конфиденциальную информацию (например, серверы приложений и баз данных), должны находиться в доверенной внутренней сети. Поставщик должен использовать демилитаризованную зону для Интернет-услуг и продуктов .

12.8 Ограничить несанкционированный исходящий трафик от приложений, обрабатывающих, хранящих или передающих личную информацию и конфиденциальную информацию, на IP-адреса в демилитаризованной зоне и в Интернете.

12.9 При использовании беспроводных сетевых технологий на основе радиочастот (РЧ) для предоставления или поддержки услуг и продуктов для CWT Поставщик должен обеспечить защиту всей передаваемой Личной информации и Конфиденциальной информации с помощью соответствующих технологий шифрования, достаточных для защиты конфиденциальности Личной информации. и Конфиденциальная информация; при условии, однако, что в любом случае такое шифрование должно использовать ключи длиной не менее 256 битов для симметричного шифрования и 2048 битов для асимметричного шифрования. Регулярно сканируйте, идентифицируйте и отключайте неавторизованные точки беспроводного доступа.

12.10 Облачная безопасность — когда данные CWT находятся в облаке или поставщик использует стороннюю облачную среду, включая, помимо прочего, инфраструктуру как услугу (IaaS), программное обеспечение как услугу (Saas) и платформу как услугу (PaaS), поставщик должен внедрите или оцените управление состоянием безопасности в облаке, чтобы обнаруживать и автоматически устранять угрозы, неправильные конфигурации, неправомерное использование и нарушения нормативных требований в общедоступных облаках.

13. Требования к подключению

13.1 В случае, если Поставщик имеет или должен быть обеспечен доступом к Персональным данным и ресурсам Конфиденциальной информации CWT в связи с Соглашением, то в дополнение к вышеизложенному, если Поставщик имеет или ему предоставляется возможность подключения к среде CWT, Поставщик должен в минимум:

а. Используйте только взаимно согласованные средства и методы подключения для соединения среды CWT с ресурсами Поставщика.
б. НЕ устанавливать соединение со средой CWT без предварительного письменного согласия CWT.
в. Предоставлять CWT доступ к любым применимым объектам Поставщика в обычные рабочие часы для обслуживания и поддержки любого оборудования (например, маршрутизатора), предоставленного CWT в соответствии с Соглашением , для подключения к ресурсам Персональной информации и Конфиденциальной информации.
д. Использовать любое оборудование, предоставленное CWT в соответствии с Соглашением для подключения к среде CWT, только для предоставления тех услуг и продуктов или функций, которые явно разрешены в Соглашении.
е. Если согласованная методология подключения требует, чтобы Поставщик реализовал шлюз безопасности, ведите журналы всех сеансов с использованием такого шлюза безопасности. Эти журналы сеансов должны содержать достаточно подробную информацию для идентификации конечного пользователя или приложения, исходного IP-адреса, конечного IP-адреса, используемых портов/сервисных протоколов и продолжительности доступа. Эти журналы сеансов должны храниться не менее шести (6) месяцев с момента создания сеанса.
ф. Разрешить CWT собирать информацию, касающуюся доступа, включая доступ Поставщика, к среде CWT. Эта информация может быть собрана, сохранена и проанализирована CWT для выявления потенциальных угроз безопасности без дополнительного уведомления. Эта информация может включать в себя файлы трассировки, статистику, сетевые адреса и фактические данные или экраны, к которым осуществляется доступ или которые передаются.
грамм. Немедленно приостановить или прекратить любое присоединение к среде CWT, если Поставщики посчитают, что имело место нарушение или несанкционированный доступ, или по указанию CWT, если CWT, по своему собственному усмотрению, полагает, что имело место нарушение безопасности, несанкционированный доступ или неправомерное использование средств обработки данных CWT. или любую информацию, системы или другие ресурсы CWT.

14. Мобильные и портативные устройства

Поставщик должен , как минимум :

14.1 Не хранить Личную информацию и Конфиденциальную информацию на мобильных и портативных устройствах, если они полностью не зашифрованы с помощью надежного шифрования.

14.2 Используйте надежное шифрование для защиты личной информации и конфиденциальной информации, передаваемой, используемой или удаленно доступной мобильными и портативными устройствами с поддержкой сети.

а. При использовании мобильных и портативных устройств с поддержкой сети , которые не являются портативными компьютерами, для доступа и/или хранения личной информации и конфиденциальной информации, такие устройства должны быть способны удалять все сохраненные копии личной информации и конфиденциальной информации после получения по сети должным образом аутентифицированного команда. (Примечание. Такая возможность часто называется возможностью «удаленной очистки».)

б. Наличие задокументированных политик, процедур и стандартов для обеспечения того, чтобы Уполномоченная сторона , которая должна физически контролировать сетевое мобильное и портативное устройство, которое не является портативным компьютером и на котором хранится Личная информация и Конфиденциальная информация, незамедлительно инициировала удаление всех Личная информация и Конфиденциальная информация в случае утери или кражи устройства.

в. Наличие задокументированных политик, процедур и стандартов, гарантирующих, что Мобильные и Портативные Устройства, не являющиеся ноутбуками и не поддерживающие работу в сети, будут автоматически удалять все сохраненные копии Личной информации и Конфиденциальной информации после последовательных неудачных попыток входа в систему.

14.3 Наличие задокументированных политик, процедур и стандартов, гарантирующих, что любые Мобильные и Портативные Устройства, используемые для доступа и/или хранения Личной информации и Конфиденциальной информации:

а. Находятся в физическом владении Уполномоченных сторон ;

б. Физически защищены, когда не находятся в физическом владении Уполномоченных сторон ; или же

в. Незамедлительно и безопасно удалять хранилище своих данных, если они не находятся в физическом владении Уполномоченной стороны, или физически не защищены, или после 10 неудачных попыток доступа.

14.4 Перед предоставлением доступа к Личной информации и Конфиденциальной информации, хранящейся на мобильных и портативных устройствах или посредством их использования , Поставщик должен иметь и использовать процесс, обеспечивающий следующее:

а. Пользователь является Уполномоченным лицом , уполномоченным на такой доступ; а также

б. Личность пользователя подтверждена.

14.5 Внедрить политику, запрещающую использование любых мобильных и портативных устройств, которые не администрируются и/или не управляются Поставщиком или CWT, для доступа и/или хранения Личной информации и Конфиденциальной информации.

14.6 Не реже одного раза в год проверять использование и средства контроля всех Мобильных и Портативных Устройств, находящихся под управлением или управлением Поставщика, чтобы убедиться, что Мобильные и Портативные Устройства соответствуют применимым Техническим и Организационным Мерам Безопасности.

15. Безопасность в пути

Поставщик должен , как минимум :

15.1 Используйте Сильное шифрование для передачи Личной информации и Конфиденциальной информации за пределы сетей, контролируемых CWT или Поставщиком, или при передаче Личной информации и Конфиденциальной информации по любой ненадежной сети.

15.2 Для физической передачи записей, содержащих Личную информацию и Конфиденциальную информацию в бумажном формате, на микрофишах или на электронных носителях, транспортируйте их защищенной курьерской службой или другим способом доставки, который можно отследить, надежно упаковать и в соответствии со спецификациями производителя. Любая личная информация и конфиденциальная информация должны перевозиться в закрытых контейнерах.

16. Безопасность в состоянии покоя

Поставщик должен , как минимум :

16.1 Используйте надежное шифрование для защиты личной информации и конфиденциальной информации при ее хранении.

16.2 Не хранить Личную информацию или Конфиденциальную информацию в электронном виде за пределами сетевой среды Поставщика (или собственной защищенной компьютерной сети CWT), если только устройство хранения (например, резервная лента, ноутбук, карта памяти, компьютерный диск и т . д.) не защищено надежным шифрованием.

16.3 Не хранить Личную информацию или Конфиденциальную информацию на съемных носителях (например, на USB-накопителях, флэш-накопителях, картах памяти, лентах, компакт-дисках или внешних жестких дисках), за исключением: резервного копирования, обеспечения непрерывности бизнеса, аварийного восстановления и обмена данными, если это разрешено и требуется по контракту между Поставщиком и CWT. Если съемные носители используются для хранения личной информации или конфиденциальной информации в соответствии с исключениями, указанными в этом подразделе, информация должна быть защищена с помощью надежного шифрования. Автозапуск должен быть отключен для съемных носителей и запоминающих устройств .

16.4 Надлежащим образом храните и защищайте записи, содержащие Личную информацию или Конфиденциальную информацию в бумажном формате или на микрофишах, в местах, доступ к которым разрешен только уполномоченному персоналу.

16.5 Если иное не указано CWT в письменной форме, при сборе, создании или создании Личной информации или Конфиденциальной информации в бумажной форме и на резервных носителях для, через или от имени CWT или под торговой маркой CWT убедитесь, что такая информация является Личной информацией или Конфиденциальной информацией . и, когда это возможно, пометить такую информацию CWT как «Конфиденциально». Поставщик признает, что Личная информация и Конфиденциальная информация являются и остаются собственностью CWT, независимо от маркировки или ее отсутствия.

17. Возврат, хранение, уничтожение и утилизация

Поставщик должен , как минимум :

17.1 Без дополнительной оплаты со стороны CWT , по запросу CWT или после расторжения Соглашения , предоставить CWT копии любой Личной информации и Конфиденциальной информации в течение тридцати (30) календарных дней с момента такого запроса или прекращения действия Соглашения . Поставщик должен вернуть или, по усмотрению CWT, уничтожить всю Конфиденциальную информацию и Личную информацию CWT, включая электронные , бумажные и защищенные резервные копии, как это предусмотрено Соглашением или, если это не предусмотрено Соглашением, в течение 90 (девяноста) календарных дней . дней после наибольшего из следующих событий: (а) истечения срока действия или расторжения Соглашения, (б) запроса CWT о возврате Личной информации и Конфиденциальной информации или (в) даты, когда Поставщику больше не нужны Личная информация и Конфиденциальная информация для оказания услуг. и продукции по Соглашению.

17.2 В случае, если CWT одобряет уничтожение в качестве альтернативы возврату Личной информации и Конфиденциальной информации, подтвердите в письменной форме должностным лицом Поставщика, что уничтожение делает Личную информацию и Конфиденциальную информацию неизвлекаемой и невозвратной. Поставщик должен полностью уничтожить все копии Личной информации и Конфиденциальной информации во всех местах и во всех системах, где хранится Личная информация и Конфиденциальная информация , включая, помимо прочего, ранее утвержденные Уполномоченные стороны. Такая информация должна быть уничтожена в соответствии со стандартной процедурой полного уничтожения, такой как DOD 5220.22M или NIST Special Publication 800-88, или с использованием размагничивающего продукта, рекомендованного производителем для затронутой системы. До такого уничтожения Поставщик должен соблюдать все применимые технические и организационные меры безопасности для защиты безопасности, конфиденциальности и конфиденциальности личной информации и конфиденциальной информации.

17.3 Утилизировать Личную информацию и Конфиденциальную информацию CWT таким образом, чтобы гарантировать, что информация не может быть преобразована в пригодный для использования формат. Бумаги, слайды, микрофильмы, микрофиши и фотографии должны быть уничтожены путем перекрестного измельчения или сжигания. Материалы, содержащие Личную информацию и Конфиденциальную информацию CWT, ожидающие уничтожения, должны храниться в защищенных контейнерах и транспортироваться с использованием надежной третьей стороны.

18. Реагирование на инцидент и уведомление

Поставщик должен , как минимум :

18.1 Иметь и использовать процесс управления инцидентами и связанные с ним процедуры, а также укомплектовать такие процессы и процедуры управления инцидентами специальными ресурсами. Немедленно и ни в коем случае не позднее , чем за двадцать четыре (24) часа, уведомлять CWT по адресу iRespond@mycwt.com о любом предполагаемом или подтвержденном нападении, вторжении, несанкционированном доступе, потере или другом инциденте, касающемся информации CWT. , системы или другие ресурсы.

18.2 После уведомления CWT предоставлять CWT регулярные обновления статуса, включая, помимо прочего, действия, предпринятые для разрешения такого инцидента, через взаимно согласованные интервалы или время в течение всего инцидента и как можно скорее после закрытия инцидента. , предоставить CWT письменный отчет с описанием инцидента, действий, предпринятых Поставщиком во время реагирования, и планов Поставщика на будущие действия по предотвращению повторения подобного инцидента.

18.3 Не сообщать и не раскрывать публично о любом таком нарушении информации, систем или других ресурсов CWT без предварительного уведомления CWT и непосредственного взаимодействия с CWT для уведомления соответствующих региональных, национальных, государственных или местных органов власти или служб кредитного мониторинга, лиц, затронутых таким нарушением, и любые применимые средства массовой информации, как того требует закон.

18.4 Внедрите процесс для оперативного выявления нарушений средств контроля безопасности, включая нарушения, изложенные в настоящих Требованиях информационной безопасности , персоналом Поставщика или Третьими сторонами. Выявленные нарушители подлежат соответствующему дисциплинарному взысканию в соответствии с действующим законодательством. Несмотря на вышеизложенное, нарушители остаются в ведении Продавца или его Третьих лиц. CWT не считается работодателем Продавца или персонала его Третьих сторон .

19. Управление непрерывностью бизнеса и аварийное восстановление

Поставщик должен , как минимум :

19.1 Разрабатывайте , эксплуатируйте, управляйте и пересматривайте планы обеспечения непрерывности бизнеса для каждого местоположения и планы аварийного восстановления для каждой базовой технологии , чтобы свести к минимуму влияние CWT на услуги или продукты Поставщика. Такие планы должны включать: названные ресурсы, относящиеся к функциям обеспечения непрерывности бизнеса и аварийного восстановления, установленные целевые показатели времени восстановления и целевые точки восстановления, как минимум ежедневное резервное копирование данных и систем, внешнее хранение резервных копий данных и систем и записей, запись планы защиты и действия в непредвиденных обстоятельствах, соответствующие требованиям Соглашения, хранить такие записи и планы в безопасном месте за пределами объекта и обеспечивать доступность таких планов для Поставщика по мере необходимости.

19.2 По запросу CWT предоставить CWT задокументированный план обеспечения непрерывности бизнеса, который обеспечит выполнение Поставщиком своих договорных обязательств по Соглашению и настоящему документу , включая требования любого применимого технического задания или соглашения об уровне обслуживания. Такие планы должны осуществлять восстановление, защищая целостность и конфиденциальность Личной информации и Конфиденциальной информации.

19.3 Иметь документированные процедуры безопасного резервного копирования и восстановления Личной информации и Конфиденциальной информации, которые должны включать, как минимум, процедуры транспортировки, хранения и уничтожения резервных копий Личной информации и Конфиденциальной информации, и по запросу CWT предоставлять такие документированные процедуры CWT.

19.4 Обеспечьте создание резервных копий всей Личной и Конфиденциальной информации, а также программного обеспечения и конфигураций для систем, используемых CWT, не реже одного раза в неделю.

19.5 Планы обеспечения непрерывности бизнеса и аварийного восстановления должны обновляться не реже одного раза в год или так часто, как это необходимо в связи со значительными изменениями в бизнес-среде и/или технологической среде.

19.6 Эти планы также должны выполняться не реже одного раза в год или после любых существенных изменений в планах обеспечения непрерывности бизнеса или аварийного восстановления за счет Поставщика. Такие учения должны обеспечивать надлежащее функционирование затронутых технологий и внутреннюю осведомленность о таких планах.

19.7 по запросу предоставьте CWT сводную информацию о планах и тестировании в разумные сроки.

19.8 Обеспечьте круглосуточный мониторинг всех объектов Поставщика или подрядчиков Поставщика, где хранятся или обрабатываются Персональные данные и

Конфиденциальная информация CWT, на предмет вторжений, огня, воды и других опасностей окружающей среды.

20. Соответствие и аккредитация

Поставщик должен , как минимум :

20.1 Хранить полные и точные записи, касающиеся выполнения им своих обязательств, вытекающих из настоящих Требований информационной безопасности, и соблюдения Поставщиком настоящих Правил в формате, позволяющем проводить оценку или аудит в течение не менее трех (3) лет или дольше, в зависимости от необходимости. в соответствии с постановлением суда или гражданским или нормативным производством. Несмотря на вышеизложенное, Поставщик обязан вести журналы безопасности не менее одного (1) года после любого продолжающегося выполнения Соглашения.

20.2 Разрешить CWT, без каких-либо дополнительных затрат для CWT, после разумного предварительного уведомления проводить периодические оценки безопасности или аудиты технических и организационных мер безопасности, используемых Поставщиком, в ходе которых CWT должна предоставить Поставщику письменные анкеты и запросы на документацию. На все запросы Поставщик должен предоставить письменный ответ и доказательства, если это применимо, немедленно или по взаимному согласию. По запросу CWT о проведении аудита со стороны CWT Поставщик должен запланировать проведение аудита безопасности в течение десяти (10) рабочих дней с момента такого запроса. CWT может потребоваться доступ к объектам, системам, процессам или процедурам для оценки среды контроля безопасности Поставщика.

20.3 По запросу CWT подтвердите, что он соответствует этому документу, а также подтверждающие сертификаты для самых последних версий PCI-DSS, ISO 27001/27002, SOC 2, Cyber Essentials или аналогичную оценку для Поставщика и любого субподрядчика или третьей стороны . обработка, доступ, хранение или управление от имени Продавца. Если Поставщик не может подтвердить соответствие, он должен предоставить письменный отчет с подробным описанием случаев несоблюдения и своего плана исправления для обеспечения соответствия.

20.4 В случае, если CWT по своему собственному усмотрению сочтет, что произошло нарушение безопасности, о котором не было сообщено CWT в соответствии с настоящим Соглашением и Процессом управления инцидентами Поставщика, запланируйте начало аудита или оценки в течение двадцати четырех (24) часов. уведомления CWT о необходимости проведения оценки или аудита.

20.5 В течение тридцати (30) календарных дней после получения результатов оценки или аудиторского отчета предоставить CWT письменный отчет с изложением корректирующих действий, которые Поставщик реализовал или предлагает осуществить, с указанием графика и текущего состояния каждого корректирующего действия. Поставщик должен обновлять этот отчет для CWT каждые тридцать (30)

календарных дней, сообщая о состоянии всех корректирующих действий до даты их реализации. Поставщик должен осуществить все корректирующие действия в течение девяноста (90) дней с момента получения Поставщиком отчета об оценке или аудите или в течение альтернативного периода времени, если такой альтернативный срок был взаимно согласован сторонами в письменной форме в течение не более тридцати (30) дней. дней с момента получения Поставщиком отчета об оценке или аудите.

20.6 Соответствие стандарту PCI DSS. В той мере, в какой Поставщик обрабатывает номера платежных счетов или любую другую связанную платежную информацию, Поставщик в настоящее время должен соответствовать самой последней версии индустрии платежных карт (PCI-DSS) для всего объема систем, обрабатывающих эту информацию, и продолжать такое соответствие. Если какой-либо субподрядчик или третье лицо обрабатывает, получает доступ, хранит или управляет данными кредитной карты от имени Поставщика, поставщик должен получить PCI AOC от такого субподрядчика или третьего лица и предоставить его CWT по запросу. В случае, если Поставщик не соответствует или более не соответствует стандарту PCI-DSS для какой-либо части полного набора систем, обрабатывающих применимые к PCI данные, Поставщик незамедлительно уведомит об этом CWT, немедленно приступит к устранению такого несоответствия и предоставит регулярный статус такого исправления CWT по запросу.

21. Стандарты, лучшие практики, правила и законы

В случае, если Поставщик обрабатывает, получает доступ, просматривает, хранит или управляет Персональными данными или Конфиденциальной информацией, относящейся к персоналу CWT, партнерам, Аффилированным лицам , клиентам CWT; или сотрудники, подрядчики, субподрядчики или поставщики клиентов CWT ; Поставщик должен применять технические и организационные меры безопасности не менее строгие, чем это требуется применимыми международными, региональными, национальными, государственными и местными руководствами, положениями, директивами и законами.

22. Модификация

CWT оставляет за собой право время от времени обновлять или изменять настоящие Требования информационной безопасности , публикуя последнюю версию на веб-сайте CWT. Если Поставщик не предоставит письменное уведомление о возражении против таких обновлений или изменений в течение тридцати (30) дней с момента публикации, считается, что Поставщик принял их.

Версия 6 .1
Дата: апрель 2024 г.