Russian

Требования по обеспечению информационной безопасности

1. Введение

Поставщик соглашается с тем, что третьи стороны, действующие от его лица в рамках предоставления продуктов и услуг CWT, обязаны соблюдать требования к обеспечению информационной безопасности, содержащиеся в настоящем документе («**Требования по обеспечению информационной безопасности**»), в котором определены необходимые меры по обеспечению информационной безопасности («**Технические и организационные меры безопасности**»).

2. Определения

Если в настоящем документе не указано и не предусмотрено иное, термины, определения которых приведены ниже, имеют то же значение, что и в основном Договоре. В настоящих Требованиях по обеспечению информационной безопасности используются следующие термины, определение которых приведено ниже:

«**Аффилированные лица**», если иное прямо не определено в настоящем документе, применительно к сторонам договора означают любую компанию или юридическое лицо, которые: (i) прямо или косвенно контролируют какую-либо из сторон; (ii) находятся под прямым или косвенным контролем какой-либо из сторон; или (iii) находятся под прямым или косвенным контролем компании или юридического лица, которое прямо или косвенно контролирует какую-либо из сторон. В данном контексте «контроль» означает право на реализацию более чем пятидесяти процентов (50%) прав голоса или аналогичных прав собственности, но лишь на протяжении срока осуществления такого контроля.

«Договор», если иное прямо не определено в настоящем документе, означает контракт или другой правовой документ, подписанный CWT и Поставщиком.

«Конфиденциальная информация» означает любую закрытую коммерческую, служебную и другую конфиденциальную информацию, относящуюся к (а) CWT и ее аффилированным лицам; (б) клиентам CWT; (в) персоналу CWT и (г) независимым партнерам и совместным предприятиям CWT или (д) содержанию и/или цели Договора, как в устном, так и в письменном виде, которая может любым образом, прямо или опосредованно, оказаться в распоряжении Поставщика или сотрудников Поставщика, а также его представителей, подрядчиков или субподрядчиков в связи с Договором или в результате его исполнения. Во избежание недоразумений вся информация, содержащаяся в рабочих документах, считается конфиденциальной информацией.

«CWT», если иное прямо не определено в настоящем Договоре, означает указанную в Договоре компанию CWT и ее аффилированных лиц.

«**Демилитаризованная зона**» или «**ДМЗ**» означает сеть или подсеть, находящуюся между защищенной внутренней сетью, например, закрытой корпоративной локальной сетью (LAN), и незащищенной внешней сетью, например, общедоступной сетью Интернет. ДМЗ помогает предотвратить прямой доступ посторонних пользователей к внутрикорпоративным системам и другим ресурсам.

«Регламент реагирования на инциденты» означает разработанный Поставщиком и документально оформленный процедурный регламент, которому нужно следовать в случае фактической или предполагаемой атаки, проникновения, несанкционированного доступа или другого нарушения безопасности, затрагивающего конфиденциальность, доступность или целостность конфиденциальной информации и персональных данных.

«Маскировка» означает процесс скрытия отображаемой на экране информации.
«Мобильные и портативные устройства» означают мобильные и/или портативные компьютеры, устройства, носители информации или системы, которые можно легко переносить, перемещать, транспортировать или передавать, используемые в связи с Договором. Примерами таких устройств могут служить ноутбуки, планшеты, внешние жесткие диски с USB-интерфейсом, карты памяти USB, карманные персональные компьютеры (КПК), мобильные телефоны и смартфоны, а также любые другие беспроводные или периферийные устройства, на которых можно хранить конфиденциальную информацию и персональные данные.

«Персональные данные», если иное прямо не определено в настоящем Договоре, согласно определению Регламента ЕС 2016/679 и других применимых международных законов в сфере информационной безопасности, защиты данных и личной жизни означают любую информацию, относящуюся к физическому лицу, личность которого установлена или может быть прямо или косвенно установлена, в частности, с помощью идентификационного номера или одного и более факторов, характеризующих конкретно его физическую, физиологическую, умственную, экономическую, культурную или социальную идентичность.

«Шлюз безопасности» означает ряд механизмов контроля, расположенных между двумя или более сетями с различными уровнями защиты, которые фильтруют и регистрируют трафик, проходящий (или пытающийся пройти) между сетями и связанными с ними административными серверами, а также серверами управления. Примеры шлюзов безопасности: брандмауэры, серверы управления брандмауэрами, системы Hopbox, пограничные контроллеры сессий, прокси-серверы и устройства предотвращения вторжения.

«Строгая аутентификация» означает использование более сложных механизмов и техник аутентификации, нежели простая защита паролем. Примеры механизмов и техник строгой аутентификации: цифровые сертификаты, двухфакторная аутентификация и одноразовые пароли.

«Криптостойкое шифрование» означает использование технологий шифрования, длина ключа в которых составляет не менее 256 битов при симметричном шифровании и не менее 1024 битов — при ассиметричном шифровании. Такая длина дает разумно обоснованную гарантию того, что ключ защитит зашифрованную информацию от несанкционированного доступа и обеспечит надлежащую защиту ее конфиденциальности и анонимности. Криптостойкое шифрование сопровождается документально оформленной политикой управления ключами шифрования и связанными процессами, достаточными для защиты конфиденциальности и анонимности ключей и паролей, используемых для ввода в алгоритме шифрования. К криптостойкому шифрованию относятся, помимо прочего: протокол SSLv3.0+/TLSv1.0+, протокол PPTP (туннельный протокол типа «точка-точка»), алгоритм AES 256, алгоритм FIPS 140-2 (только для правительства США), алгоритм RSA (1024 бита), алгоритм SHA1/SHA2/SHA3, протоколы IPSEC, SFTP, SSH, Vormetricv4 или WPA2.

«Технические и организационные меры безопасности» означают любые мероприятия, необходимые в соответствии с настоящими Требованиями по обеспечению информационной безопасности для получения доступа, управления, передачи, обработки, хранения, в том числе долгосрочного, или уничтожения информации, или данных; для информирования и оповещения заинтересованных сторон в соответствии с Договором и применимыми законами в области обеспечения конфиденциальности информации и защиты данных, а также для защиты информации или данных с целью обеспечения их доступности, целостности, конфиденциальности и анонимности или уведомления физических лиц о неспособности защитить такую информацию или данные. К таковым, в частности, относятся меры, необходимые или признанные необходимыми в соответствии с Директивами Европейского парламента 94/46/ЕС и 2006/24/ЕС, принятыми в странах-членах ЕС, американским законом Грэмма — Лича — Блайли (GLBA), законом США «О перемещаемости и подотчетности страхования здоровья» (HIPAA), требованиями к защите конфиденциальности данных ЕС/Швейцарии или любыми другими

международными или американскими законами, официальным юридическим толкованием или судебным прецедентом, относящимся к информации или данным, на которые распространяется Договор.

«**Третья сторона»,** если иное прямо не определено в настоящем Договоре, означает любых субподрядчиков, а также всех временных сотрудников Поставщика, его подрядчиков или дополнительных поставщиков и/или представителей, действующих от имени Поставщика, и распространяется на любые третьи стороны согласно применимым законам ЕС, США и другим международным законам.

«**Поставщик**» означает указанную в Договоре подрядную организацию, ее аффилированных лиц и сторонних партнеров

2.2. Поставщик гарантирует и подтверждает, что обязуется соблюдать приведенные ниже технические и организационные меры безопасности в той степени, в какой они применимы к предоставлению указанных в Договоре услуг.

3. Организация информационной безопасности

Поставщик обязуется:

3.1 разработать, внедрить и обеспечивать соблюдение соответствующих отраслевым стандартам, по меньшей мере разумно обоснованных политик и программ организационных, оперативных, административных и физических технических и организационных мер безопасности, необходимых для (1) предотвращения доступа к конфиденциальной информации и персональным данным любым образом, не разрешенным в Договоре или настоящих Требованиях по обеспечению информационной безопасности, и гарантии (2) соответствия всем действующим отраслевым стандартам. Поставщик также обязуется гарантировать, что весь персонал, связанный с обеспечением безопасности, имеет достаточный и необходимый опыт в области обеспечения информационной безопасности;

3.2 обеспечить персоналу Поставщика, которому требуется доступ к конфиденциальной информации и персональным данным, надлежащий уровень контроля, руководства и подготовки в сфере технических и организационных мер безопасности. Поставщик также обязуется обеспечивать подготовку в сфере технических и организационных мер безопасности после найма сотрудников на работу и до предоставления им доступа к конфиденциальной информации и персональным данным. Переподготовку необходимо проводить не менее одного раза в год и как можно скорее после любого существенного изменения технических и организационных мер безопасности Поставщика;

3.3 Персонал Поставщика, выполняющий важные обязанности в сфере обеспечения безопасности, помимо прочего, служебные обязанности в сфере кадровой политики или информационных технологий и любые обязанности по администрированию технологий, также должен пройти специальную подготовку в соответствии с должностными обязанностями. В рамках специализированной подготовки необходимо обеспечить, в зависимости от должностных обязанностей, ознакомление с процедурами обеспечения информационной безопасности, допустимым использованием ресурсов в области информационной безопасности, актуальными угрозами безопасности информационных систем, функциями обеспечения безопасности конкретных систем и процедурами безопасного доступа;

3.4 принимать необходимые меры для предотвращения несанкционированного доступа к конфиденциальной информации и персональным данным и услугам, системам, устройствам

или средам, содержащим такую информацию, а также потери такой информации, услуг, систем, устройств или сред;

3.5 использовать регламент и процедуры оценки рисков для регулярной оценки систем, используемых для предоставления CWT продуктов или услуг. Поставщик также обязуется устранять такие риски в кратчайшие сроки и в соответствии с уровнем риска, установленного для конфиденциальной информации и персональных данных с учетом угроз, о которых стало известных на момент определения рисков. Поставщик обязуется внедрить регламент, который позволит персоналу Поставщика сообщать о рисках или предполагаемых инцидентах в службу безопасности Поставщика.

3.6 В тех случаях, когда Поставщик предоставляет услуги в соответствии с Договором на объекте CWT или с использованием услуг, систем, устройств или носителей информации, которые принадлежат, находятся в эксплуатации или под управлением CWT, соблюдать все предоставленные ему политики CWT, применимые к такому доступу. Поставщик также обязуется незамедлительно уведомлять CWT в письменной форме, если такой доступ больше не требуется, в том числе когда сотрудник, подрядчик, субподрядчик или третья сторона Поставщика больше не предоставляют услуги в соответствии с Договором, или когда им больше не требуется доступ к конфиденциальной информации и персональным данным;

3.7 вести учет своих ресурсов, которые имеют доступ к конфиденциальной информации и песрональным данным, а также задействованы в их передаче, актуализации, хранении или обработке.

3.8 выполнять требования CWT к проведению комплексной проверки в степени, необходимой и допустимой по закону, как определено в соответствующем техническом задании/заказе-наряде/заказе на покупку.

4. Физическая и экологическая безопасность

Поставщик обязуется:

4.1 обеспечить размещение всех систем и других ресурсов Поставщика, предназначенных для использования несколькими пользователями, на территории защищенных физических объектов с ограниченным доступом только для уполномоченных лиц;

4.2 контролировать и регистрировать, в целях проверки, доступ к физическим объектам, на территории которых размещены системы и другие ресурсы, предназначенные для использования несколькими пользователями, которые используются в связи с выполнением Поставщиком своих обязательств в соответствии с Договором;

4.3 обеспечить подписание персоналом Поставщика соглашения о неразглашении или соглашения о конфиденциальности с Поставщиком до получения доступа к конфиденциальной информации и персональным данным;

4.4 требовать от всех своих сотрудников соблюдения политики «чистого стола» и блокирования экранов рабочих станций перед уходом из рабочей зоны;

4.5 забирать все принадлежащее компании имущество в случае прекращения трудовых отношений или расторжения договора;

4.6 ограничивать и контролировать физический доступ на территорию своих объектов в соответствии со следующими требованиями.

а. Все посетители регистрируются, а журнал посещений хранится в течение трех (3) месяцев; в журнале указываются имя и фамилия посетителя, компания, которую он/она представляет, а также имя и фамилия сотрудника, разрешившего физический доступ.
б. Доступ предоставляется только соответствующему персоналу, в зависимости от служебных обязанностей.
в. Все сотрудники должны носить предоставленный компанией именной бейдж.
г. В случае прекращения трудовых отношений сотрудник немедленно лишается права доступа, а все физические механизмы доступа, такие как ключи, карты доступа и т. д., должны быть возвращены или деактивированы.
д. Центр обработки данных или компьютерный зал должен закрываться на ключ, доступ к нему предоставляется только тем лицам, которым он необходим для выполнения служебных обязанностей.
е. Когда это разрешено законом, необходимо использовать видеокамеры для контроля физического доступа в важные помещения и регулярно анализировать данные видеонаблюдения. Записи видеонаблюдения должны храниться в течение не менее трех (3) месяцев.
ж. Оборудование, используемое для хранения, обработки или передачи конфиденциальной информации и персональных данных, например, беспроводные точки доступа, шлюзы, портативные устройства, сетевые/коммуникационные аппаратные средства и линии телекоммуникаций, должно быть защищено с помощью физических средств.

4.7 внедрить меры и системы контроля с целью уменьшения риска и защиты от физических угроз;

4.8 содержать все аппаратные активы, используемые для обработки или передачи конфиденциальной информации и персональных данных, в соответствии с рекомендуемыми требованиями к техническому обслуживанию стороннего поставщика услуг;

4.9 логически отделить сетевые розетки в конференц-залах и других общедоступных зонах от сети Поставщика и предоставить доступ к ним только уполномоченному персоналу или по умолчанию отключить их;

4.10 защищать от несанкционированного доступа и замены любое устройство, которое фиксирует данные платежной карты посредством прямого физического взаимодействия, периодической проверки поверхностей устройства с целью обнаружения признаков несанкционированного доступа или замены; обеспечить подготовку персонала и научить его распознавать несанкционированный доступ или замену устройств;

4.11 контролировать и физически отделять точки доступа, такие как пункты приема и погрузки, а также другие точки, от всех центров обработки данных, которые связаны с доступом, управлением, хранением или обработкой конфиденциальной информации и персональных данных;

4.12 оборудовать центры обработки данных обогревательными и охлаждающими устройствами, а также средствами пожаротушения, обнаружения воды и тепла/дыма.

5. <u>Контроль доступа</u>

Поставщик обязуется:

5.1 принимать все разумно обоснованные меры для предотвращения доступа к конфиденциальной информации и персональным данным любым образом и с любой целью, которые не предусмотрены CWT и Договором. Поставщик также обязуется ограничить доступ к конфиденциальной информации и персональным данным сотрудниками Поставщика, которые (1) имеют обоснованную потребность в доступе к конфиденциальной информации и персональным данным с целью предоставления услуг в соответствии с Договором и (2) в письменной форме согласились обеспечивать защиту целостности, доступности и конфиденциальности конфиденциальной информации и персональных данных;

5.2 внедрить и обеспечить соблюдение процедур, необходимых для прекращения доступа к конфиденциальной информации и персональным данным, предоставленного персоналу Поставщика, в том случае, если он больше не нужен или не требуется для выполнения служебныхобязанностей, и до прекращения трудовых отношений с Поставщиком или сотрудничества с CWT;

5.3 отделять информацию CWT от информации любых других клиентов и собственных приложений и информации Поставщика либо с помощью физического отделения серверов, либо, в тех случаях, когда физического отделение серверов не реализовано, с помощью логических элементов управления доступом;

5.4 определять и требовать от соответствующих владельцев рассмотрения и разрешения доступа к системам, используемым для получения доступа к конфиденциальной информации и персональным данным, а также их обработки, управления или хранения; вести учет и отслеживать случаи разрешения доступа;

5.5 отменить право доступа к системам, управляющим конфиденциальной информацией и персональными данными, в течение 24 часов после прекращения трудовых отношений сотрудника, подрядчика, субподрядчика или третьей стороны с Поставщиком; отменить право доступа к таким системам в течение трех (3) рабочих дней в тех случаях, когда должностные обязанности сотрудника, подрядчика, субподрядчика или третьей стороны в компании были изменены; в остальных случаях идентификаторы пользователей должны быть деактивированы или аннулированы, если не используются в течение 90 календарных дней;

5.6 регулярно, не реже одного раза в квартал, пересматривать и утверждать доступ к системам, управляющими конфиденциальной информацией и персональными данными, чтобы предотвратить несанкционированный доступ;

5.7 предоставлять доступ системного администратора (также известного как «root-пользователь», «привилегированный пользователь» или «суперпользователь») к операционным системам, предназначенным для использования несколькими пользователями, только лицам, которым такой высокоуровневый доступ необходим для выполнении их должностных обязанностей; по возможности использовать для управления высокоуровневым доступом идентификацию при завершении работы, с учетными данными и журналами событий; в противном случае ограничить высокоуровневый доступ крайне малым числом пользователей;

5.8 требовать от администраторов приложений, баз данных, сетей и систем ограничивать доступ пользователей только командами, данными, системами и другими ресурсами, которые необходимы для выполнения их утвержденных служебных обязанностей;

5.9 требовать проведения строгой аутентификации в случае любого удаленного доступа;

5.10 запретить персоналу Поставщика, имеющему доступ к персональным данным, копировать, перемещать или хранить конфиденциальную информацию и персональные данные на локальных жестких дисках или вырезать и вставлять, или распечатывать конфиденциальную информацию и персональные данные, а также использовать технические и организационные меры безопасности для обеспечения выполнения этого правила;

5.11 активировать возможность удаленного доступа только при необходимости, контролировать доступ во время использования и отключить его сразу после завершения использования;

5.12 требовать по меньшей мере двухфакторной аутентификации при подключении к внутренним ресурсам Поставщика, содержащим конфиденциальную информацию и персональные данные.

6. Идентификация и аутентификация

Поставщик обязуется:

6.1 присваивать каждому пользователю уникальный идентификатор и определять механизмы аутентификации для каждого отдельного пользователя (то есть учетной записи);

6.2 использовать документально оформленный регламент управления жизненным циклом идентификаторов пользователей, который включает, помимо прочего, процедуры создания утвержденных учетных записей, своевременного удаления учетных записей и изменения учетных записей (например, изменения привилегий, уровня доступа, функций/служебных обязанностей) для доступа к любой конфиденциальной информации и персональным данным во всех рабочих средах (например, среде разработки, тестирования, создания и т. д.); такой регламент должен предусматривать пересмотр прав доступа и действительности учетных записей, который должен выполняться не реже одного раза в квартал;

6.3 обеспечивать соблюдение принципа наименьших привилегий, согласно которому доступ ограничивается только командами, информацией, системами и другими ресурсами, необходимыми для выполнения рабочих функций, разрешенных в соответствии со служебными обязанностями;

6.4 ограничить доступ к конфиденциальной информации и персональным данным лицами, использующими действительный идентификатор пользователя и пароль, а также требовать использования в уникальном идентификаторе пользователя одного из следующих средств защиты: пароля или ключевой фразы, двухфакторной или биометрической аутентификации;

6.5 требовать использования сложных паролей, соответствующих следующим требованиям: системные пароли должны содержать не менее восьми (8) символов, а коды для входа с планшетных ПК и смартфонов — не менее четырех (4) символов; системные пароли должны содержать три следующих элемента: буквенные символы в верхнем регистре, буквенные символы в нижнем регистре, числовые или специальные символы; пароли не должны совпадать с идентификатором пользователя, с которым они связаны, или пятью последними паролями и не должны содержать словарные слова, последовательность чисел или повторяющиеся числа; требовать прекращения действия пароля с регулярным интервалом, не превышающим девяносто (90) дней; скрывать отображаемые на экране пароли;

6.6 разрешать не более пяти (5) неудачных попыток входа в систему в течение 24 часов и блокировать учетную запись пользователя при регулярном достижении этого предельного

значения; доступ к учетной записи пользователя может быть впоследствии возобновлен вручную после подтверждения личности пользователя;

6.7 проверять личность пользователя и создавать для каждого пользователя уникальные пароли для однократного использования или восстановления доступа к учетной записи; систематически предлагать изменить пароль после первого использования;

6.8 использовать безопасный метод для передачи учетных данных для аутентификации (например, паролей) и механизмов аутентификации (например, токенов или смарт-карт);

6.9 ограничивать длину паролей к учетным записям служб и паролей прокси не менее чем 12 символами; такие пароли должны содержать символы верхнего регистра, символы нижнего регистра, числовые и специальные символы; изменять пароли к учетным записям служб и пароли прокси не реже одного раза в год;

6.10 принудительно завершать интерактивную сессию или активировать безопасную блокирующую заставку с требованием аутентификации после определенного периода бездействия, который не должен превышать пятнадцать (15) минут;

6.11 использовать метод аутентификации, соответствующий степени важности конфиденциальной информации и персональных данных; при сохранении учетных данных для аутентификации использовать для их защиты криптостойкое шифрование;

6.12 настроить системы на выполнение автоматического тайм-аута по истечении максимального периода бездействия: для сервера — 15 минут, для рабочей станции — 15 минут, для мобильного устройства — 4 часа, для протокола DHCP — 7 дней, для виртуальной частной сети — 24 часа.

7. Приобретение, разработка и обслуживание информационных систем

Поставщик обязуется:

7.1 при использовании фирменных продуктов и услуг CWT или продуктов и программного обеспечения, разработанного для CWT, отображать баннер с предупреждением на экранах или страницах входа в систему, как это определено CWT в письменном виде;

7.2 обеспечивать соблюдение персоналом, выполняющим работу в соответствии с Договором, настоящих технических и организационных мер безопасности, что подтверждается письменным соглашением, не менее строгим, чем настоящие Требования по обеспечению информационной безопасности;

7.3 вернуть все устройства обеспечения доступа, принадлежащие или предоставленные CWT, в кратчайшие сроки, но не позднее, чем через пятнадцать (15) дней после наступления первого из следующих событий:

(а) окончания срока действия или прекращения действия Договора;
(б) получения запроса CWT о возврате такого имущества; или
(в) даты, когда Поставщику больше не требуются такие устройства;

7.4 использовать эффективную методику управления приложениями, которая предусматривает включение технических и организационных мер безопасности в процесс разработки программного обеспечения, а также обеспечивать своевременное внедрение Поставщиком технических и организационных мер безопасности, описанных в политиках, стандартах и

процедурах CWT в области обеспечения информационной безопасности и жизненного цикла разработки программного обеспечения;

7.5 следовать стандартным процедурам разработки, в том числе разделять доступ и код непроизводственной и производственной среды, и в этой связи распределять обязанности между такими средами;

7.6 обеспечить регулярную оценку внутренних средств управления информационной безопасностью для разработки программного обеспечения, призванную гарантировать соответствие лучшим отраслевым практикам, а также своевременно пересматривать и внедрять эти средства управления

7.7 управлять безопасностью процесса разработки, а также обеспечивать внедрение и соблюдение безопасных методов кодирования, в том числе соответствующих криптографических средств управления, средств защиты от вредоносного кода, а также регламента независимой технической экспертизы;

7.8 проводить тестирование функционально законченных приложений на проникновение до запуска в производство и в дальнейшем, не реже одного раза в год и после любых существенных изменений исходного кода или конфигурации в соответствии со стандартами OWASP, CERT, SANS Top 25, and PCI-DSS; устранять любые уязвимости, которые могут быть использованы, до развертывания в производственной среде;

7.9 использовать в непроизводственных средах анонимизированные или намеренно измененные данные; никогда не использовать незашифрованные производственные данные (в текстовом формате) в непроизводственной среде и ни при каких обстоятельствах не использовать в непроизводственной среде конфиденциальную информацию и персональные данные; обеспечить удаление всех данных тестирования и учетных записей до выпуска продукции;

7.10 обеспечить соблюдение Поставщиком, использующим открытый исходный код, программное обеспечение, приложения или услуги, надлежащих мер предосторожности при проверке полученного кода с целью выявления дефектов, ошибок и проблем безопасности, которые могут повлиять на целостность, доступность или конфиденциальность данных CWT или клиентов CWT. Поставщик также обязуется уведомлять CWT об использовании открытого кода и предоставлять CWT название и версию такого открытого кода

7.11 гарантировать, что Поставщик ни при каких обстоятельствах не будет размещать коды, созданные в соответствии с Договором, независимо от стадии разработки, в любой общей или не частной среде, например, в открытом репозитории исходного кода, вне независимости от наличия защиты паролем.

8. Целостность программного обеспечения и данных

Поставщик обязуется:

8.1 установить и использовать в тех средах, в которых на рынке доступно антивирусное программное обеспечение, современное антивирусное программное обеспечение, предназначенное для сканирования и быстрого удаления или перемещения в карантин вирусов и других вредоносных программ из любых систем или устройств;

8.2 отделять информацию и ресурсы непроизводственного характера от производственной информации и ресурсов;

8.3 обеспечить использование рабочими группами документально оформленного регламента управления всеми системными изменениями, который включает в себя процедуры резервного копирования для всех производственных сред и регламенты экстренного изменения; включить в такие регламенты тестирование, документирование и согласование всех системных изменений, и требовать утверждения любых существенных изменений руководством;

8.4 создать и обеспечить функционирование PCI-зоны в тех случаях, когда Поставщик обрабатывает или хранит данные владельцев карт;

8.5 включить и использовать функции ведения контрольного журнала транзакций базы данных в приложениях, использующих базы данных, которые позволяют вносить изменения в конфиденциальную информацию и персональные данные, и сохранять контрольные журналы транзакций базы данных в течение не менее чем шести (6) месяцев;

8.6 проверять все программное обеспечение с целью выявления и устранения уязвимостей безопасности в ходе первоначальной реализации, а также после любого существенного изменения и обновления;

8.7 выполнять проверку качества компонентов обеспечения безопасности (например, функций идентификации, аутентификации и авторизации), а также любые другие действия, направленные на проверку архитектуры системы безопасности, в ходе первоначальной реализации, а также после любого существенного изменения и обновления.

9. <u>Безопасность систем</u>

Поставщик обязуется:

9.1 регулярно создавать и обновлять новейшие версии потока данных и диаграмм системы, используемых для получения доступа к конфиденциальной информации и персональным данным, их обработки, управления или хранения;

9.2 активно следить за отраслевыми ресурсами (например, , www.cert.org и соответствующими рассылками и веб-сайтами поставщиков программного обеспечения) для получения своевременного оповещения обо всех потенциальных угрозах, касающихся систем и других информационных ресурсов Поставщика;

9.3 организовать эффективное управление криптографическими ключами путем ограничения доступа к ключам минимальным необходимым числом хранителей, использования при хранении секретных и частных криптографических ключей ключа не менее криптостойкого, чем ключ шифрования данных, и хранения таких ключей отдельно от ключа шифрования данных на защищенном криптографическом устройстве в минимальном необходимом количестве мест; изменять используемые по умолчанию криптографические ключи при установке и не реже одного раза в два года, а также надежно ликвидировать старые ключи;

9.4 сканировать внешне ориентированные системы и другие информационные ресурсы, в том числе сети, серверы и приложения, с помощью применимого сканирующего программного обеспечения, соответствующего отраслевым стандартам, с целью обнаружения уязвимостей в системе безопасности, не реже одного раза в квартал и перед выходом приложений, существенными изменениями и любыми обновлениями в сроки, определенные на основании

анализа рисков в соответствии с разумно обоснованными и общепринятыми политиками, а также стандартами в области ИТ;

9.5 сканировать внутренние системы и другие информационные ресурсы, в том числе, помимо прочего, сети, серверы, приложения и базы данных, с помощью применимого сканирующего программного обеспечения, соответствующего отраслевым стандартам, с целью обнаружения уязвимостей в системе безопасности, обеспечения надлежащей защиты таких систем и других ресурсов и выявления любых несанкционированных беспроводных сетей, не реже одного раза в квартал и перед выходом приложений, существенными изменениями и любыми обновлениями в сроки, определенные на основании анализа рисков в соответствии с разумно обоснованными и общепринятыми политиками и стандартами в области ИТ;

9.6 внедрить и обеспечить соблюдение регламента категоризации рисков для обнаруженных уязвимостей, основанного на передовых практиках и серьезности потенциального воздействия; для устранения всех обнаруженных уязвимостей, которым была присвоена категория «4» или выше по шкале CVSS, необходимо использовать формализованный метод с целью обеспечения непрерывности оценки рисков;

9.7 обеспечить повышенную защиту всех систем и других ресурсов Поставщика, включая, помимо прочего, удаление или отключение неиспользуемых сетевых и других продуктов и услуг (например, продуктов и услуг, связанных с программой finger, сервисом rlogin, протоколом FTP и протоколом TCP/IP), и установку системного брандмауэра, программ-«оболочек» TCP-Wrapper или аналогичной технологии;

9.8 использовать одну или несколько систем обнаружения вторжений (IDS), систем предотвращения вторжений (IPS) или систем обнаружения и предотвращения вторжений (IDP) в активном режиме работы, в котором осуществляется мониторинг всего трафика на входе и выходе систем, и других ресурсов, связанных с Договором, в средах, где такая технология коммерчески доступна, и насколько это практически осуществимо;

9.9 внедрить и использовать регламент классификации рисков с целью устранения уязвимостей безопасности в любых системах или других ресурсах, к которым относятся, помимо прочих, уязвимости, обнаруженные с помощью отраслевых сообщений, сканирования на наличие уязвимостей, сканирования на наличие вирусов, а также в результате анализа журналов безопасности, и незамедлительно применять соответствующие патчи безопасности с учетом вероятности того, что такая уязвимость может использоваться или уже используется; критически важные патчи, имеющие оценку 7,5 или более баллов по шкале CVSS, должны быть установлены при первой возможности и ни в коем случае не позднее чем через месяц после выхода; патчи, имеющие оценку 4 или более баллов по шкале CVSS, должны быть установлены в течение 90 дней после выхода;

9.10 выполнять общее внутреннее и внешнее тестирование на проникновение не реже одного раза в год и после любого существенного обновления или изменения инфраструктуры, или приложения;

9.11 удалять или отключать неразрешенное программное обеспечение, обнаруженное в системах Поставщика, и использовать принятые в отрасли меры защиты от вредоносного программного обеспечения, включающие установку, регулярное обновление и использование антивредоносных программных продуктов на всех службах, системах и устройствах, которые могут быть использованы для доступа к конфиденциальной информации и персональным данным; в тех случаях, когда это практически осуществимо, использовать надежное

антивирусное программное обеспечение, соответствующее передовым отраслевым стандартам, и обеспечивать непрерывное обновление определений вирусов;

9.12 применять на всех службах, системах и устройствах, которые могут быть использованы для доступа к конфиденциальной информации и персональным данным, актуальное программное обеспечение и поддерживать его в работоспособном состоянии, что включает надлежащее техническое обслуживание операционной системы (систем) и успешную установку актуальных патчей безопасности;

9.13 поручить исполнение обязанностей по администрированию систем безопасности, связанных с настройкой хостовых операционных систем, конкретным лицам;

9.14 изменять все установленные по умолчанию имена учетных записей и/или пароли.

10. Контрольно-учетная деятельность

Поставщик обязуется:

10.1 хранить данные журналов событий, связанных с конфиденциальной информацией и персональным данными, на протяжении не менее чем 12 месяцев и обеспечивать доступность таких данных CWT в разумные сроки и по запросу, за исключением случаев, предусмотренных в других положениях Договора;

10.2 регистрировать первичные системные действия в системах, содержащих любые персональные данные и конфиденциальные данные;

10.3 предоставлять доступ к журналам событий безопасности только уполномоченному персоналу, а также защищать журналы событий безопасности от несанкционированных изменений;

10.4 внедрить механизм обнаружения изменений (например, контроль целостности файлов) для оповещения персонала о несанкционированных изменениях критически важных системных файлов, файлов конфигурации или содержимого; настроить в программном обеспечении выполнение еженедельного сопоставления критически важных файлов;

10.5 не реже одного раза в неделю проверять все журналы событий безопасности и контрольные журналы, связанные с безопасностью, в системах, содержащих персональные данные и конфиденциальную информацию, с целью обнаружения отклонений от нормы, документально фиксировать и своевременно устранять все обнаруженные проблемы безопасности;

10.6 ежедневно проверять все события и журналы событий безопасности системных компонентов, которые используются для хранения, обработки или передачи данных владельцев карт, журналы критически важных системных компонентов, а также журналы серверов и системных компонентов, выполняющих функции безопасности.

11. Шлюзы безопасности

Поставщик обязуется:

11.1 требовать строгой аутентификации при предоставлении административного и/или управленческого доступа к шлюзам безопасности, что включает, помимо прочего, любой доступ с целью просмотра файлов журналов;

11.2 внедрить и использовать документально оформленные средства управления, политики, регламенты и процедуры, гарантирующие, что неавторизованные пользователи не имеют административных и/или управленческих прав доступа к шлюзам безопасности, а также что используются надлежащие уровни авторизации пользователей, установленные для администрирования и управления шлюзами безопасности;

11.3 не реже одного раза в шесть (6) месяцев проверять защиту конфигурации шлюзов безопасности, выбрав один из шлюзов безопасности и убедившись в том, что каждый стандартный набор правил и параметров конфигурации обеспечивает следующее:

а) маршрутизация интернет-протокола (IP) от источника отключена;
б) адрес обратной связи не может проникнуть во внутреннюю сеть;
в) используются антиспуфинговые фильтры;
г) широковещательные пакеты не могут проникнуть в сеть;
д) переадресация по ICMP-протоколу отключена;
е) все наборы правил заканчиваются предписанием «DENYALL» (заблокировать все) и
ж) каждое правило можно соотнести с конкретным бизнес-запросу;

11.4 обеспечить использование средств контроля и учета для подтверждения бесперебойной работы всех элементов шлюзов безопасности (например, аппаратного обеспечения, программно-аппаратного и программного обеспечения);

11.5 обеспечить настройку и эксплуатацию всех шлюзов безопасности таким образом, чтобы блокировать всем доступ ко всем нерабочим шлюзам безопасности.

11.6 гарантировать перехват входящих пакетов из незащищенной внешней сети в демилитаризованной зоне («ДМЗ»); их прямая передача в защищенную внутреннюю сеть недопустима. В защищенную внутреннюю сеть должны поступать только входящие пакеты, созданные в ДМЗ. ДМЗ должна быть отделена от незащищенной внешней сети шлюзом безопасности, а от защищенной внутренней сети ее должен отделять один из следующих элементов:

а) еще один шлюз безопасности, или
б) шлюз безопасности, который используется для отделения ДМЗ от незащищенной внешней сети; в этом случае шлюз безопасности должен гарантировать, что пакеты, полученные из незащищенной внешней сети, немедленно удаляются, либо, если они не удаляются, передаются только в ДМЗ, и никакая другая обработка таких входящих пакетов не производится, за исключением регистрации пакетов в журнале.

Следующие элементы должны размещаться исключительно в защищенной внутренней сети:

а) любая конфиденциальная информация и персональные данные, которые хранятся без использования криптостойкого шифрования;
б) официальный зарегистрированный экземпляр информации, доступ к которому можно получить по запросу из незащищенной внешней сети;
в) официальный зарегистрированный экземпляр информации, который может быть изменен в результате запросов из незащищенной внешней сети;
г) серверы баз данных;
д) все экспортированные журналы событий, а также
е) любые рабочие среды, используемые для разработки, тестирования, экспериментальной проверки и создания программных продуктов, а также любые подобные среды и все версии исходного кода.

11.7 Учетные данные для аутентификации, не защищенные криптостойким шифрованием, не должны храниться в ДМЗ.

12. Сетевая безопасность

Поставщик обязуется:

12.1 по запросу CWT предоставить CWT логическую схему сети, в которой указаны системы и подключения к другим ресурсам, в том числе маршрутизаторам, коммутаторам, межсетевым экранам, системам IDS, топологии сети, внешним точкам подключения, шлюзам, беспроводным сетям, а также любым другим устройствам, поддерживающим CWT;

12.2 внедрить и обеспечивать соблюдение официального регламента утверждения, тестирования и регистрации всех сетевых соединений и изменений конфигурации брандмауэра и маршрутизатора; настроить в брандмауэрах блокирование и регистрацию любых подозрительных пакетов и пропуск только релевантного и разрешенного трафика; весь остальной трафик через брандмауэры должен быть заблокирован; проверять правила пропуска трафика брандмауэрами каждые шесть месяцев;

12.3 установить брандмауэр на каждом подключенном к интернету устройстве, а также между ДМЗ и зоной внутренней сети; любая система, в которой хранятся персональные данные и конфиденциальная информация, должна находиться во внутренней сети, отделенной от ДМЗ и других незащищенных сетей;

12.4 контролировать брандмауэр по сетевому периметру и изнутри с целью контроля и защиты сетевого трафика, проходящего через границу сетей, по необходимости;

12.5 внедрить документально оформленный регламент и средства контроля для обнаружения и нейтрализации попыток несанкционированного доступа к конфиденциальной информации и персональным данным;

12.6 в случае предоставления CWT интернет-продуктов и услуг обеспечивать защиту конфиденциальной информации и персональных данных посредством внедрения сетевой ДМЗ; веб-серверы, используемые для предоставления услуг CWT, должны быть размещены в ДМЗ; любая система или информационный ресурс, используемые для хранения конфиденциальной информации и персональных данных (например, приложения и серверы баз данных), должны находиться в защищенной внутренней сети (для предоставления интернет-продуктов и услуг необходимо использовать ДМЗ);

12.7 ограничить неразрешенный исходящий трафик от приложений, используемых для обработки, хранения или передачи конфиденциальной информации и персональных данных на IP-адреса в пределах ДМЗ и Интернета;

12.8 при использовании радиочастотных (РЧ) технологий беспроводных сетей для реализации или поддержки услуг и продуктов для CWT обеспечивать защиту всей переданной конфиденциальной информации и персональных данных посредством использования надежных технологий шифрования, достаточных для защиты конфиденциальности персональных данных и конфиденциальной информации; регулярно выполнять сканирующие проверки, обнаруживать и отключать точки несанкционированного беспроводного доступа.

13. Требования к сетевым подключениям

Поставщик обязуется:

13.1 в случае наличия или предоставления Поставщику в связи с Договором возможности подключения к ресурсам конфиденциальной информации и персональных данных:

а) использовать для подключения ресурсов конфиденциальной информации и персональных данных к ресурсам Поставщика только взаимно согласованные материально-технические средства и методики;
б) не подключаться к ресурсам конфиденциальной информации и персональных данных без предварительного согласия CWT;
в) обеспечить CWT доступ к любым задействованным материально-техническим средствам Поставщика в течение нормального рабочего дня с целью выполнения технического обслуживания и поддержки любого оборудования (например, маршрутизатора), предоставленного CWT в соответствии с Договором для подключения к ресурсам конфиденциальной информации и персональных данных;
г) использовать любое оборудование, предоставленное CWT в соответствии с Договором для подключения к ресурсам конфиденциальной информации и персональных данных, исключительно для предоставления услуг, продуктов или функций, прямо разрешенных в Договоре;
д) если согласованные методики подключения предусматривают внедрение Поставщиком шлюза безопасности, вести журналы всех сеансов, использующих такой шлюз безопасности. Такие журналы сеансов должны содержать достаточно подробную информацию для определения конечного пользователя или приложения, исходного IP-адреса, целевого IP-адреса, используемых протоколов портов/служб и продолжительности доступа. Журналы сеансов необходимо хранить в течение не менее чем шести (6) месяцев с момента начала сеанса.

13.2 В случае наличия или предоставления Поставщику в связи с Договором возможности подключения к ресурсам конфиденциальной информации и персональных данных в дополнение к прочим правам, предусмотренным настоящим документом, разрешать CWT следующее:

а) собирать информацию, связанную с доступом, в том числе доступом Поставщика, к ресурсам конфиденциальной информации и персональных данных; CWT имеет право без дополнительного уведомления собирать, сохранять и анализировать такую информацию с целью выявления потенциальных угроз безопасности; такая информация может включать данные файлов трассировки, статистические данные, сетевые адреса, а также просмотренные или переданные фактические данные или страницы (экраны);
б) незамедлительно приостанавливать или прерывать подключение к ресурсам конфиденциальной информации и персональных данных, если CWT по своему единоличному усмотрению считает, что имело место нарушение безопасности, несанкционированный доступ или неправомерное использование информационных объектов CWT или какой-либо информации, систем или других ресурсов CWT.

14. Мобильные и портативные устройства

Поставщик обязуется:

14.1 использовать криптостойкое шифрование для защиты всей конфиденциальной информации и персональных данных, которые хранятся на мобильных и портативных устройствах;

14.2 не хранить конфиденциальную информацию и персональные данные на мобильных устройствах или ноутбуках, а также не хранить конфиденциальную информацию и персональные данные на съемных носителях без использования криптостойкого шифрования;

14.3 использовать криптостойкое шифрование для защиты конфиденциальной информации и персональных данных, передача или удаленный доступ к которым осуществляется с помощью мобильных и портативных устройств, поддерживающих аутентификацию в сети;

а) при использовании мобильных и портативных устройств, поддерживающих аутентификацию в сети, за исключением ноутбуков, используемых для получения доступа и/или хранения конфиденциальной информации и персональных данных, такие устройства должны иметь функцию удаления всех сохраненных копий конфиденциальной информации и персональных данных после получения по сети команды с надлежащей аутентификацией (примечание: такую функцию часто называют функцией «удаленной очистки»);

б) внедрить документально оформленные политики, процедуры и стандарты в целях обеспечения незамедлительного инициирования уполномоченным лицом, физически контролирующим мобильные и портативные устройства, поддерживающие аутентификацию в сети, за исключением ноутбуков и устройств, используемых для хранения конфиденциальной информации и персональных данных, удаления всей конфиденциальной информации и персональных данных в случае потери или кражи устройства;

в) внедрить документально оформленные политики, процедуры и стандарты в целях обеспечения автоматического удаления всех сохраненных копий конфиденциальной информации и персональных данных после нескольких последовательных неудачных попыток входа с мобильных и портативных устройств, за исключением ноутбуков и устройств, поддерживающих аутентификацию в сети;

14.4 внедрить документально оформленные политики, процедуры и стандарты в целях обеспечения того, что любые мобильные и портативные устройства, используемые для получения доступа к конфиденциальной информации и персональных данных и/или их хранения:

а) физически находятся в распоряжении уполномоченного персонала;
б) физически изолированы, когда не находятся в распоряжении уполномоченного персонала, или
в) быстро и надежно очищаются от содержащихся на них данных, когда не находятся в распоряжении уполномоченного персонала, не изолированы или после 10 неудачных попыток получения доступа;

14.5 прежде чем предоставить доступ к конфиденциальной информации и персональным данным, которые хранятся на мобильных и портативных устройствах или с их помощью, разработать и использовать регламент для обеспечения следующего:

а) пользователю разрешен такой доступ и
б) пользователь успешно прошел аутентификацию;

14.6 внедрить политику, запрещающую использование для получения доступа к конфиденциальной информации и персональных данных или их хранения любых мобильных и портативных устройств, администрирование и/или управление которыми осуществляется не Поставщиком или CWT;

14.7 не реже одного раза в год проверять использование и средства контроля всех мобильных и портативных устройств, администрирование или управление которыми осуществляет Поставщик, чтобы обеспечить соответствие мобильных и портативных устройств применимым техническим и организационным мерам безопасности.

15. <u>Защита данных при передаче</u>

Поставщик обязуется:

15.1 использовать криптостойкое шифрование для передачи конфиденциальной информации и персональных данных за пределы контролируемых CWT или Поставщиком сетей или при передаче конфиденциальной информации и персональных данных в любой незащищенной сети;

15.2 отправлять физически передаваемые документы в бумажном виде, на микрофишах или электронных носителях, содержащие конфиденциальную информацию и персональные данные, доверенной курьерской службой или иным образом, который можно отследить, быть надежно упакованы и соответствовать спецификациям производителя; транспортировка документов, содержащих конфиденциальную информацию и персональные данные, должна осуществляться в закрытых на замок контейнерах.

16. <u>Защита данных по месту хранения</u>

Поставщик обязуется

16.1 использовать криптостойкое шифрование для защиты конфиденциальной информации и персональных данных по месту хранения;

16.2 не хранить конфиденциальную информацию и персональные данные в электронном виде за пределами сетевой среды Поставщика (или собственной защищенной компьютерной сети CWT), если устройство хранения данных (например, ленточный накопитель, ноутбук, карта памяти, компьютерный диск и т. д.) не защищено криптостойким шифрованием;

16.3 не хранить конфиденциальную информацию и персональные данные на съемных носителях (например, флеш-накопителях USB, флеш-накопителях, картах памяти, ленточных накопителях, компакт-дисках или внешних жестких дисках), за исключением следующих случаев: (а) с целью резервного копирования, обеспечения непрерывности деятельности, послеаварийного восстановления и обмена данными, как допускается и требуется в соответствии с контрактом, и (б) при использовании криптостойкого шифрования;

16.4 надлежащим образом хранить документы в бумажном виде или на микрофише, содержащие конфиденциальную информацию и персональные данные, в защищенных местах, доступ к которым предоставляется только уполномоченному персоналу;

16.5 если иное прямо не указано CWT в письменной форме, при сборе, формировании или создании конфиденциальной информации и персональных данных в бумажном виде и на резервных носителях для CWT, при посредничестве, от имени или под торговой маркой CWT гарантировать, что такая информация и данные являются конфиденциальной информацией и персональными данными и, когда это практически осуществимо, маркировать такую информацию CWT пометкой «Конфиденциально». Поставщик признает, что конфиденциальная

информация и персональные данные остаются в собственности CWT вне зависимости от маркировки или ее отсутствия.

17. Возврат, уничтожение и утилизация

Поставщик обязуется:

17.1 по запросу CWT и без взимания дополнительной платы с CWT предоставить CWT копии любой конфиденциальной информации и персональных данных в течение тридцати (30) дней после даты такого запроса. Поставщик также обязуется вернуть, или, по решению CWT, уничтожить всю конфиденциальную информацию и персональные данные, в том числе все копии на электронных и бумажных носителях, как это предусмотрено в Договоре, или, если не предусмотрено в Договоре, в течение девяноста (90) дней после наступления первого из следующих событий: (а) окончания срока действия или прекращения действия Договора; (б) получения запроса CWT о возврате конфиденциальной информации и персональных данных или (в) даты, когда Поставщику больше не требуется конфиденциальная информация и персональные данные для предоставления услуг и реализации продуктов в соответствии с Договором;

17.2 в случае если CWT выберет вместо возврата конфиденциальной информации и персональных данных ее уничтожение, в письменном виде подтвердить факт полного и безвозвратного уничтожения конфиденциальной информации и персональных данных; полностью уничтожить все копии конфиденциальной информации и персональных данных во всех местах и системах, где хранится конфиденциальная информация и персональные данные, в том числе системах ранее утвержденных третьих сторон Поставщика. Такая информация должна быть уничтожена с соблюдением процедуры полного уничтожения в соответствии с отраслевым стандартом, например, национальным стандартом Министерства обороны США DOD 5220.22M, рекомендацией Американского национального института стандартизации Special Publication 800-88, или с использованием рекомендованного производителем средства размагничивания для задействованной системы. До уничтожения Поставщик обязуется соблюдать все применимые технические и организационные меры безопасности для защиты безопасности, анонимности и конфиденциальности персональных данных и конфиденциальной информации;

17.3 утилизировать конфиденциальную информацию и персональные данные таким образом, чтобы гарантированно обеспечить невозможность восстановления информации в пригодном для использования формате. Бумажные носители, слайды, микрофильмы, микрофиши и фотографии должны быть утилизированы путем перекрестного измельчения или сжигания. Материалы, содержащие конфиденциальную информацию и персональные данные, которые подлежат уничтожению, должны храниться в защищенных контейнерах и перевозиться с использованием надежной третьей стороны.

18. Длительное хранение

Поставщик обязуется:

18.1 согласовать соответствующие требования к хранению с контактными лицами CWT до получения конфиденциальной информации и персональных данных и в соответствии с любым перечнем работ или заказом на поставку;

18.2 обеспечить защиту любых резервных копий конфиденциальной информации и персональных данных, автоматически созданных службами, системами, устройствами или носителями Поставщика («**Архивные копии**»); если в Договоре прямо не оговорено иное, в течение 90 календарных дней после окончания срока действия или прекращения действия Договора или ранее, в случае обоснованного запроса CWT, уничтожить без возможности восстановления все архивные копии конфиденциальной информации и персональных данных, следуя процедуре, соответствующей отраслевым стандартам, не менее строгим, чем стандарт DOD 5220.22M или рекомендация Американского национального института стандартизации Special Publication 800-88.

19. Меры реагирования и оповещения об инцидентах

Поставщик обязуется:

19.1 разработать и использовать регламент реагирования на инциденты и связанные с ним процедуры, а также выделить специализированные ресурсы, необходимые для выполнения такого регламента и процедур реагирования на инциденты; незамедлительно и ни в коем случае не позднее чем через двадцать четыре (24) часа сообщать CWT о любых предполагаемых или подтвержденных атаках, вторжениях, случаях несанкционированного доступа, потере или других инцидентах, касающихся информации, систем или других ресурсов CWT;

19.2 после первоначального оповещения CWT регулярно предоставлять CWT актуальную информацию о ходе реагирования на инцидент, в том числе, помимо прочего, информировать о мерах, принятых для устранения такого инцидента, через взаимно согласованные промежутки времени на протяжении всего срока существования инцидента, и в разумно возможный кратчайший срок после устранения инцидента предоставить CWT письменный отчет, содержащий описание инцидента, меры, принятые Поставщиком в ходе реагирования, и планы дальнейших действий Поставщика по предотвращению подобных инцидентов;

19.3 не разглашать публично сведения о любых подобных нарушениях неприкосновенности информации, систем или других ресурсов CWT, предварительно не оповестив об этом CWT; работая напрямую с CWT, уведомить представителей соответствующих органов власти на региональном, национальном или местном уровне или службы кредитного мониторинга, лиц, пострадавших от такого нарушения, и любые компетентные средства массовой информации, в соответствии с требованиями закона;

19.4 внедрить регламент оперативного выявления нарушений контроля безопасности, в том числе изложенных в настоящих Требованиях по обеспечению информационной безопасности, допущенных персоналом Поставщика. По отношению к персоналу Поставщика, допустившему такие нарушения, будут применены надлежащие меры дисциплинарного воздействия в соответствии с действующим законодательством. Невзирая на вышеизложенное, персонал Поставщика остается под руководством Поставщика. CWT не будет считаться работодателем персонала Поставщика.

20. Обеспечение непрерывности деятельности и послеаварийное восстановление

Поставщик обязуется:

20.1 разработать, использовать, организовать и пересматривать планы обеспечения непрерывности деятельности и послеаварийного восстановления с целью уменьшения влияния инцидентов на продукты и услуги CWT и Поставщика; такие планы должны включать следующее: указание ресурсов, выделенных специально для обеспечения непрерывности деятельности и послеаварийного восстановления, определение целевых показателей времени восстановления и целевых точек восстановления, ежедневное резервное копирование данных и систем, удаленное хранение резервных носителей информации и документов, планы обеспечения защиты документов и экстренных действий, соответствующие требованиям Договора; хранить такие планы под надежной защитой за пределами территории (удаленно) и обеспечивать их предоставление Поставщику по мере необходимости;

20.2 по запросу CWT предоставить CWT документально оформленный план обеспечения непрерывности деятельности, гарантирующий, что Поставщик сможет выполнять свои обязательства по Договору, в том числе требования любого применимого технического задания или соглашения об уровне предоставляемых услуг; такие планы должны предусматривать восстановление и одновременную защиту целостности и конфиденциальности персональных данных и конфиденциальной информации;

20.3 внедрить документально оформленные процедуры защищенного резервного копирования и восстановления конфиденциальной информации и персональных данных, которые должны включать, по меньшей мере, процедуры транспортировки, хранения и удаления резервных копий конфиденциальной информации и персональных данных, и, по запросу CWT, предоставлять такие документированные процедуры CWT;

20.4 обеспечить резервное копирование всей хранящейся конфиденциальной информации и персональных данных или программного обеспечения и конфигурации систем, используемых CWT, не реже одного раза в неделю;

20.5 регулярно, не реже одного раза в год или после внесения любых существенных изменений в планы обеспечения непрерывности деятельности или послеаварийного восстановления, отрабатывать комплексную реализацию таких планов за собственный счет Поставщика; такие учебные мероприятия должны обеспечить надлежащее функционирование используемых технологий и осведомленность персонала о таких планах;

20.6 оперативно пересматривать план обеспечения непрерывности деятельности с учетом дополнительных или новых источников или сценариев угроз и по запросу в разумные сроки предоставлять CWT высокоуровневую сводку планов и испытаний;

20.7 обеспечить круглосуточный и непрерывный (24 часа в сутки, 7 дней в неделю) контроль на всех собственных или арендуемых объектах Поставщика, используемых для размещения или обработки конфиденциальной информации и персональных данных, с целью обеспечения защиты от вторжения, пожара, затопления и других вредных факторов окружающей среды.

21. <u>Нормативно-правовое соответствие и сертификация</u>

Поставщик обязуется:

21.1 сохранять полную и точную документацию, относящуюся к его исполнению своих обязательств, возникающих в связи с настоящими Требованиями по обеспечению информационной безопасности и подтверждающую их соблюдение Поставщиком в формате, который позволяет выполнить оценку или проверку за период не менее трех (3) лет или более , как может потребоваться в соответствии с постановлением суда, гражданским или

регулятивным производством. Невзирая на вышеизложенное, Поставщик обязан вести журналы безопасности только в течение не менее чем шести (6) месяцев после каждого продления срока действия Договора;

21.2 CWT имеет право, без каких-либо дополнительных затрат для CWT и при условии предварительного оповещения в разумные сроки, периодически проводить оценку или проверку используемых Поставщиком технических и организационных мер безопасности, во время которых CWT предоставит Поставщику письменные опросные листы и запросы о предоставлении документации. На все запросы Поставщик обязуется отвечать в письменной форме, сопровождая ответы доказательствами, немедленно, если это применимо, или в обоюдно согласованные сторонами сроки. Получив запрос CWT о проведении проверки CWT, Поставщик обязуется запланировать проверку безопасности не позднее чем через 10 (десять) рабочих дней после даты такого запроса. Для оценки системы контроля безопасности Поставщика CWT может потребоваться доступ к его объектам, системам, регламентам или процедурам;

21.3 по запросу CWT предоставить доказательства соблюдения условий настоящего документа, а также сертификаты, подтверждающие соответствие текущим версиям стандартов PCI-DSS, ISO 27001/27002, SOC 2, или подтверждения аналогичных результатов оценки системы безопасности Поставщика. В случае неспособности представить подтверждение соответствия требованиям и сертификаты Поставщик обязан предоставить письменный отчет, в котором подробно описаны случаи несоответствия требованиям и изложены меры по устранению такого несоответствия;

21.4 е случае если CWT, по своему собственному усмотрению, посчитает, что произошло нарушение правил безопасности, о котором не было сообщено CWT в соответствии с настоящим документом и регламентом реагирования на инциденты Поставщика, запланировать проверку или оценку безопасности не позднее чем через двадцать четыре (24) часа с момента уведомления CWT с требованием проведения такой оценки или проверки;

21.5 в течение тридцати (30) календарных дней после получения отчета о результатах оценки или проверки предоставить CWT письменный отчет с описанием корректирующих действий, которые Поставщик выполнил или планирует выполнить, содержащий график и сведения о текущем статусе выполнения каждого корректирующего действия; обновлять этот отчет CWT каждые тридцать (30) календарных дней, предоставляя актуальные сведения о статусе всех корректирующих действий до даты их полной реализации;выполнить все корректирующие действия в течение девяноста (90) дней с даты получения им отчета об оценке или проверке, или в течение альтернативного периода времени при условии, что такой альтернативный срок был обоюдно согласован сторонами в письменной форме в течение не более чем тридцати (30) дней после получения Поставщиком отчета об оценке или проверке;

21.6 в настоящем и будущем соответствовать требованиям любых применимых утвержденных государственными органами стандартам информационной безопасности и требованиям к отчетности, а также стандарту ISO 27001/27002. В тех случаях, когда Поставщик занимается обработкой номеров платежных счетов или любой другой связанной с ними платежной информации, Поставщик также обязан соответствовать требованиям текущей версии стандарта безопасности данных индустрии платежных карт PCI-DSS применительно к полному спектру систем, используемых для обработки такой информации, и продолжать соответствовать ему в дальнейшем. В том случае если любая часть полного спектра систем Поставщика, используемых для обработки данных, на которые распространяется стандарт PCI, больше не соответствует стандарту PCI-DSS, Поставщик обязан в кратчайшие сроки уведомить об этом CWT и незамедлительно, без необоснованной задержки, приступить к устранению такого

несоответствия и по запросу регулярно предоставлять CWT актуальные сведения о ходе устранения.

22. Стандарты, рекомендации, законы и подзаконные акты

Поставщик обязуется:

В том случае если Поставщик обрабатывает, использует, просматривает, хранит или управляет конфиденциальной информацией и персональными данными, относящимися к персоналу, партнерам, аффилированным лицам CWT, клиентам CWT или сотрудникам, подрядчикам или субподрядчикам клиентов CWT;применять технические и организационные меры безопасности не менее строгие, чем требуется применимыми международными, региональными, национальными и местными руководящими принципами, нормативными актами, директивами и законами.

23. Внесение изменений

CWT оставляет за собой право время от времени обновлять или изменять текст настоящих Требований по обеспечению информационной безопасности путем размещения их текущей версии на официальном сайте CWT.

Версия 2.0

Дата: 15 декабря 2017 г.