Содержание

1. Введение и сфера действия

1.1 Настоящий документ представляет собой базовые требования безопасности ВТ по диапазону работы, осуществляемой Поставщиком. Данные требования применяются на 3 уровнях.

1-й уровень требований в разделе 2 относится к Поставщикам, которые осуществляют работу, связанную с ограниченным объемом Информации ВТ и могут иметь ограниченный доступ к административным Системам ВТ и Сетям ВТ. Поставщики, которые относятся к данной категории, не обязаны выполнять какие-либо иные требования, предусмотренные настоящим документом.

2-й уровень - это разделы 3 - 6, обязательные к исполнению для всех иных видов работ.

К 3-му уровню, в зависимости от диапазона работ, может быть применимо одно или несколько требований, предусмотренных разделами 7-18. Ваш представитель Департамента закупок ВТ предоставит вам рекомендации.

В некоторых требованиях могут содержаться ссылки на Приложение, которое приведено ниже по тексту и содержит дополнительную информацию.:

Приложение 1 "Классификация информации"
Приложение 2 "Обязательное обучение"
Приложение 3 "Передача запросов/проблем на рассмотрением Контактному лицу ВТ в области безопасности"
Приложение 4 "Доступ к объектам и зданиям ВТ организациями, не входящими в состав ВТ"
Приложение 5 - "Требования к безопасности внешнего хостинга"

1.2 Настоящие Требования безопасности дополняют и не ограничивают любые иные обязательства Поставщика по Контракту (включая, помимо прочего, его обязательства, предусмотренные Условиями под заголовками "Конфиденциальность", "Защита персональных данных" и "Проверки при приеме на работу (ППР))".

2. Информационная безопасность при ограниченном доступе

Выполнение положений Раздела 2 представляет собой единственное применимое требование, если Поставщик осуществляет работу, связанную с ограниченным доступом к Информации ВТ и может иметь ограниченный доступ к административным Системам ВТ, например, к iSupplier и Сетям ВТ (типы работ включают, помимо прочего, поставку канцелярских принадлежностей, управление системами здания, инженерно-геологические изыскания, ваучерные планы и продукты по скидкам для сотрудников, поставщиков ТВ-контента ВТ и Правообладателей).

Без ограничения любых иных предусмотренных для него обязательств в области конфиденциальности, в случае если Поставщик или Контрактный персонал имеет доступ к Информации ВТ или клиента ВТ (включая персональные данные), связанной с ВТ или Клиентами ВТ, Поставщик:

(а) гарантирует, что такая Информация (включая персональные данные) не раскрывается Контрактному персоналу, который не принят на работу для непосредственного выполнения работ ВТ, и такой персонал не имеет к ней доступа, а также
(б) сохраняет (и обеспечивает сохранение всем соответствующим Контрактным персоналом) безопасность и конфиденциальность такой Информации (включая персональные данные) (в том числе, помимо прочего, путем реализации таких систем и процедур, которые необходимы для защиты безопасности всей информации, принадлежащей ВТ или контролируемой ВТ, в той степени, в которой она находится во владении или под контролем Поставщика, в соответствии с передовыми отраслевыми методиками, и неукоснительно следит за функционированием всех таких систем и процессов).

Разделы 3 - 6 (включительно) применимы ко всем случаям привлечения поставщиков для работы с ВТ (за исключением поставщиков, предоставляющих исключительно Товары с ограниченным доступом)

3. Общие принципы информационной безопасности

3.1 Поставщик незамедлительно сообщает ВТ данные Контактного лица Поставщика в области безопасности, а также любые изменения, вносимые в них.

3.2 В начале выполнения Контракта Поставщик сообщает Контактному лицу ВТ в области безопасности в письменном виде, с использованием Приложения 3, сведения о географическом расположении объектов, на которых оказываются основные услуги, находятся соответствующий Контрактный персонал или осуществляется обработка или хранение Информации ВТ. В течение срока действия Контракта Поставщик также обязан сообщать Контактному лицу ВТ в области безопасности о любых предполагаемых изменениях в географическом положении посредством Приложения 3, с тем, чтобы ВТ могла осуществить переоценку рисков для ВТ или Информации Клиентов ВТ.

3.3 Поставщик гарантирует, что все контракты с соответствующими Субподрядчиками включают оформленные в письменном виде условия, требующие от Субподрядчика выполнения Требований безопасности ВТ в той степени, в которой они применимы. Такие условия должны действовать в отношениях между Поставщиком и его Субподрядчиком до момента, когда Субподрядчик или любой из его сотрудников может получать доступ к Системам ВТ и Информации ВТ.

3.4 Поставщик не имеет права использовать Информацию ВТ в каких-либо целях, отличных от цели, для которых ВТ предоставила Информацию ВТ Поставщику, и может использовать ее только в той степени, в которой это требуется Поставщику для выполнения Контракта. Поставщик обращается со всей Информацией или использует ее таким образом, который отвечает требованиям, предусмотренным Приложением 1 настоящих Требований безопасности, а также в соответствии с положениями применимого законодательства.

3.5 Поставщик уведомляет Контактное лицо BT в области безопасности с использованием Приложения 3, если имеет место слияние, поглощение Поставщика или изменения в его структуре собственности, с тем, чтобы BT могла осуществить переоценку рисков для BT и Информации BT или Информации Клиентов BT.

3.6 Поставщик, не реже одного раза в год или при внесении любых изменений в Товары или способ их поставки, осуществляет пересмотр настоящих Требований безопасности для того, чтобы обеспечить их соответствие всем применимым Требованиям безопасности.

3.7 Поставщик безопасным образом осуществляет управление любыми Материальными активами BT и/или Объектами BT, закрепленными BT за Поставщиком.

- Материальные активы BT и Объекты BT должны храниться безопасным образом в то время, когда они не используются. В числе примеров (помимо прочего) - аппаратные ключи для удаленного доступа, переносные компьютеры, сетевое оборудование, серверы и документация BT.
- Материальные активы BT не должны покидать территории осуществления работ без предварительного разрешения.

3.8 Поставщик, в отношении предоставления Товаров, обязан иметь официальные процедуры управления происшествиями в системе безопасности с определенными обязанностями, причем любая информация о любом происшествии в системе безопасности должна рассматриваться как Конфиденциальная. Поставщик, в течение обоснованного срока после того, как ему становится об этом известно, информирует Контактное лицо BT в области безопасности, с использованием Приложения 3, о любом происшествии:

i) связанном с существенной утратой, искажением, ущербом или злоупотреблением Информацией BT, Материальными активами BT, Объектами BT или ненадлежащим или неразрешенным доступом к Системам BT и Информации BT или нарушением любого из обязательств Поставщика, предусмотренных настоящими Требованиями безопасности; или
ii) связанном с невозможностью поставки Товаров в соответствии с контрактом.
iii) о любых действиях, которые приводят к нарушению требований данного документа в области Безопасности.

По обоснованному требованию, Поставщик незамедлительно предоставляет BT письменный отчет с описанием плана восстановительных мер, включающего график и описание мер, которые будут приняты для предотвращения повторения происшествия.

3.9 Поставщик обеспечивает незамедлительное устранение рисков в отношении конфиденциальности, целостности или доступности Информации BT в процессах Поставщика или в Системах Поставщика.

3.10 BT может осуществлять оценку рисков по любой соответствующей части услуги (в том числе - по субподрядчикам, связанным с услугой) с целью выявления дополнительных рисков для BT, обусловленных предоставлением Товаров (в зависимости от конкретного случая). BT может указать дополнительные меры противодействия с целью устранения рисков. Любые издержки по принятию мер противодействия подлежат согласованию обеими сторонами.

3.11 Поставщик обладает политиками и процессами в области безопасности, а также ведет документацию (копии которой предоставляются на английском языке) с целью демонстрации выполнения настоящих Требований безопасности и предоставления ВТ доступа к доказательствам в соответствии с Разделом 7 ниже по тексту.

3.12 Поставщик обеспечивает наличие процедур и средств контроля для защиты Передачи Информации ВТ посредством сообщений электронной почты, голосовой, факсимильной и видеосвязи. (Например, при проведении телеконференции, гарантирует, что всем лица, участвующим в ней, разрешено обсуждать Информацию ВТ) Дополнительная информация по обращению с Информацией ВТ изложена в Приложении 1.

3.13 Поставщик реализует процедуры для устранения угроз нарушения безопасности, направленных на ВТ или третью сторону, осуществляющую работы от имени ВТ, с целью надлежащей защиты Информации ВТ.

3.14 Поставщик гарантирует, что в отношении деятельности по удаленной работе и надомной работе в отношении Информации ВТ и Систем ВТ действуют надлежащие меры безопасности в рамках организации Поставщика, включая, помимо прочего, удаленный доступ пользователей с использованием устойчивой аутентификации.

3.15 При расторжении или при истечении срока действия Контракта Поставщик безопасным образом уничтожает, а также обеспечивает безопасное уничтожение любым Контрактным персоналом и Субподрядчиками, в соответствии с Приложением 1 к настоящим Требованиям безопасности, любую Информацию ВТ, которая находится во владении или под контролем Поставщика или его Субподрядчиков, за исключением случаев, когда обратное установлено ВТ или требуется в соответствии с любыми установленными законом или нормативными актами обязанностями. Архивированная информация должна быть выведена из оборота при повседневной деятельности.

3.16 Поставщик обязан хранить Информацию ВТ в течение такого срока, который необходим для оказания услуги, но не более двух лет, за исключением случаев, когда иной срок хранения установлен ВТ или необходим для выполнения установленных законом или нормативными актами требований.

3.17 Поставщик обеспечивает доступность, качество, целостность и достаточные мощности для обеспечения необходимой системной производительности или Товаров с бесперебойной доступностью, путем принятия следующих мер:

- Наличие резервного плана
- Защита критически важных системных данных (если это применимо)
- Реализация альтернативных мер в случае, если это является согласованным требованием
- Обеспечение возможности восстановления системы или обслуживания после крупного отказа или катастрофы
- Отработка плана не реже одного раза в год
- Изготовление и регулярное тестирование резервных копий информации и программного обеспечения (в применимых случаях), а также наличие согласованной политики резервного копирования для обеспечения восстановления неизмененных данных.

4. Безопасность Контрактного персонала

4.1 Соответствующему Контрактному персоналу Доступ предоставляется только после прохождения им обучения ВТ в области Безопасности, как предусмотрено Приложением 2 к настоящим Требованиям безопасности. Обучение ВТ по Информационной безопасности может быть заменено собственным обучением поставщика в области безопасности информации (при условии одобрения со стороны Службы безопасности ВТ). Впоследствии обязательное обучение должно проводиться повторно, как предусмотрено Приложением 2. Поставщик ведет учетную документацию по обучению, которая предоставляется в ВТ для проверки.

4.2 Поставщик гарантирует подписание всем Контрактным персоналом соглашения о конфиденциальности Поставщиков до момента начала выполнения работ в зданиях ВТ или в Системах ВТ или до момента получения доступа к Информации ВТ. Данные соглашения о конфиденциальности должны храниться Поставщиком и предоставляться в ВТ для ознакомления в ходе проверки.

4.3 Поставщик устраняет нарушения требований политик и процедур в области безопасности с использованием официальных процедур, включая соответствующие меры дисциплинарного воздействия.

4.4 Поставщик поддерживает функционирование доступной всему его персоналу конфиденциальной линии оперативной поддержки, которую Контрактный персонал, в степени, допустимой законодательством, использует в случае получения указаний действовать неподобающим образом в нарушение настоящих Требований безопасности. Соответствующие отчеты доводятся до сведения Контактного лица ВТ в области безопасности с использованием Приложения 3.

4.5 В случае, если Контрактный персонал перестает быть закрепленным за Товарами, Поставщик обеспечивает прекращение доступа к Информации ВТ, а также возврат соответствующей оперативной группе ВТ или уничтожение, в соответствии с Приложением 1 к настоящим Требованиям безопасности, любых активов ВТ или Объектов ВТ или Информации ВТ, находящихся во владении Контрактного персонала. В применимых случаях Поставщик реализует процедуру контролируемого выхода, которая включает письменное требование к Оперативному руководителю ВТ об аннулировании доступа к доступу к ВТ и Идентификационных данных ВТ. Контрактный персонал должен быть поставлен в известность о том, что подписанное соглашение о конфиденциальности сохраняет силу, а также что информация ВТ, полученная в процессе работы по Товарам, не подлежит раскрытию.

4.6 В рамках предоставления Доступа Поставщик осуществляет ведение и предоставление учетной документации по всему Контрактному персоналу, которому необходим доступ или который осуществляет предоставление Товаров ВТ, включая имя, место работы, рабочий адрес электронной почти и прямой рабочий телефонный номер и добавочный номер (если это применимо), и/или мобильный номер, дату, запрошенный Идентификационный номер пользователя (UIN) (при наличии такового), дату закрепления его за проектом ВТ, дату прохождения им обязательного обучения, дату его выхода из проекта ВТ, а также заявление по Проверке при приеме на работу. Контактное лицо Поставщика в области безопасности в любой момент времени

гарантирует, что Разрешение предоставлено только Соответствующему контрактному персоналу.

5. Проверки и анализ безопасности

5.1 Поставщик, в отношении Товаров и при условии поддержания Поставщиком конфиденциальности информации, относящейся к другим его клиентам, предоставляет, по обоснованному запросу (а также обеспечивает предоставление всем Контрактным персоналом) BT или ее уполномоченным представителям такой доступ к помещениям, системам и учетной документации с Информацией BT или Информацией Клиентов BT Поставщика и любого соответствующего Субподрядчика, который обоснованно необходим для оценки выполнения Поставщиком настоящих Требований безопасности.

Это может включать оценку всех элементов физических и логических средств контроля, а также проверку Систем Поставщика, в которых хранится Информация BT. Поставщик оказывает содействие в проведении такой оценки путем предоставления BT разрешения на сбор, хранение или анализ информации, связанной с предоставлением Товаров (в зависимости от конкретного случая) с целью выявления возможных рисков нарушения безопасности, а также предоставляет BT такие отчеты и присутствует на таких встречах, которые BT может обоснованно потребовать.

Если этого требует BT, Поставщик принимает участие в удаленной интерактивной проверке работоспособности с целью установления фундаментального выполнения требований безопасности в соответствии с условиями безопасности, предусмотренными настоящими Требованиями безопасности.

6. Проведение расследований

6.1 Если у BT имеются основания подозревать наличие нарушения Поставщиком или любым субподрядчиком положений настоящих Требований безопасности, которые отражаются на Системах BT и/или Информации BT, BT информирует об этом Контактное лицо Поставщика в области безопасности. Поставщик в полной мере сотрудничает с BT в ходе любого последующего расследования, проводимого BT и/или любыми правоохранительными органами, что может включать в себя доступ к Информации BT в помещениях Поставщика с уведомлением Поставщика за обоснованное время.

В процессе проведения расследования Поставщик сотрудничает с BT, предоставляя обоснованную помощь и средства, необходимые для расследования нарушения. BT может потребовать от Поставщика подвергнуть карантину любые принадлежащие Поставщику материальные или нематериальные активы с целью содействия расследованию, причем Поставщик не имеет права необоснованно отказывать в выполнении данного требования или откладывать его выполнение.

Относительно условий разделов 7 - 18, описание по каждому разделу определяет, к какому виду Товаров применимы условия.

7. Общие требования и политика безопасности

Выполнение условий Раздела 7 является обязательным, если Поставщик имеет доступ к "Закрытой информации" (в соответствии с определением данного термина) или выполняет функции по разработке, установке, техническому обслуживанию, поддержке или обслуживанию сетей или оказывает Профессиональные ИТ-услуги.

7.1 Поставщик должен быть сертифицирован по стандарту ISO27001 или должен выполнять Требования безопасности сертификации по стандарту ISO27001 или политик безопасности, приведенных в соответствии со стандартом ISO27001 и/или работать над получением сертификата по стандарту ISO27001 в сроки, согласованные с BT.

7.2 В случае их предоставления, BT может время от времени актуализировать политики, директивы и требования в области безопасности, а также иные требования. BT включает соответствующие актуальные изменения в обновленную версию настоящих Требований безопасности по запросу на внесение изменений в контракт, который доводится Поставщиком в письменном виде до сведения BT. Любые издержки по реализации новых требований безопасности подлежат согласованию обеими сторонами.

7.3 Поставщик предоставляет BT копии Сертификатов безопасности и заявление о применимости, соответствующее оказываемым услугам, с целью подтверждения сведений о выполнении требований данного Плана.

8. Физическая безопасность - Помещения BT

В случае предоставления Поставщиком Товаров в Помещениях BT выполнение условий Раздела 8 является обязательным.

8.1 Весь Контрактный персонал, работающий в помещениях BT, имеет карту Разрешенного поставщика или предоставленную BT идентификационную карту. Данная карта должна всегда использоваться в качестве средства подтверждения идентификационных данных в помещениях BT и включает отображаемое на карте фотографическое изображение, которое должно быть четким и достоверно отражать внешний вид Контрактного персонала. Контрактному персоналу также может предоставляться электронная карта доступа и/или временная карта посетителя, которые используются в соответствии с местными указаниями по их выпуску.

8.2 Подключаться непосредственно к доменам BT (подсоединяться к LAN-порту или к беспроводной сети) разрешается только одобренным серверам службы построений BT, ПК-веб-топам BT и Доверенным конечным устройствам. Поставщик не имеет права подключать (а также, в соответствующих случаях, гарантирует, что любой Контрактный персонал не подключает), без предварительного письменного разрешения Контактного лица BT в области безопасности (с использованием Приложения 3), какое-либо не одобренное BT оборудование к какому-либо Домену BT. Контактное лицо BT в области безопасности предоставляет письменное разрешение

после инициирования процесса проверки соответствия политике безопасности в рамках ВТ.

8.3 Без предварительного разрешения ВТ запрещается перемещать Информацию ВТ за пределы помещений ВТ, а также удалять или устанавливать в Помещениях ВТ Оборудование или программное обеспечение.

8.4 Необходимо следовать принципам физической защиты и указаниям по работе в Помещениях ВТ, например, по сопровождению при посещении охраняемых зон. Кроме того, поручения или указания, предоставленные Представителю Поставщика считаются предоставленными Поставщику.

8.5 В случае если Поставщику разрешено предоставлять своему Контрактному персоналу удаленный доступ к зонам на территории ВТ, разрешенное лицо с правом подписи, не являющееся сотрудником ВТ, и Контрактный персонал обязаны выполнять требования инструктивного документа "Доступ к объектам и зданиям ВТ со стороны организаций, не входящих в состав ВТ", включенного в Приложение 4. Кроме того, разрешенное лицо с правом подписи, не являющееся сотрудником ВТ, и Контрактный персонал должны проходить проверки при приеме на работу как минимум Уровня 2.

9. Физическая безопасность - Помещения Поставщика

Выполнение условий Раздела 9 является обязательным, если Поставщик предоставляет Товары с территории вне помещений ВТ. Это относится ко всему Контрактному персоналу, Субподрядчикам, а также сотрудникам, субподрядчикам и агентам Поставщика.

9.1 Доступ к территориям вне помещений ВТ (объекты, здания или внутренние зоны), где осуществляется предоставление Товаров, или где осуществляется хранение или обработка Информации ВТ, предоставляется Разрешенному поставщику, которому выдается идентификационная карта. Данная карта должна всегда использоваться в качестве средства подтверждения идентификационных данных в соответствующих помещения и, в этой связи, отображаемое на карте фотографическое изображение, должно быть четким и достоверно отражать внешний вид владельца. Также может предоставляться Разрешенная электронная карта доступа. Ее единственная цель - получение доступа к соответствующим помещениям или безопасный доступ с использованием кнопочной панели и процессов по контролю Разрешений, распространения и изменений, вносимых в обычный Код / специализированный Код.

9.2 Поставщик гарантирует, что доступ к объектам, зданиям или внутренним зонам, где производятся Товары, или осуществляется хранение или обработка Информации ВТ, является разрешенным и должен отвечать требованиям процессов и процедур системы безопасности, в том числе - в отношении Субподрядчиков, имеющих физический доступ к таким зонам например, техническое обслуживание климатического оборудования, компании, устанавливающие сигнализацию).

9.3 Если этого потребует предприятие ВТ или ответственный за проект ВТ, Поставщик обеспечивает отделение Соответствующего контрактного персонала безопасным образом от всего иного персонала Поставщика.

9.4 Охраняемые зоны в помещениях Поставщика (например, помещения с сетевым оборудованием) отделяются и защищаются при помощи соответствующих средств контроля входа с тем, чтобы гарантировать, что доступ к таким охраняемым зонам имеет только Разрешенный контрактный персонал. Доступ Контрактного персонала в эти зоны должен проходить регулярную проверку, а также, не реже одного раза в год, должна осуществляться выдача повторных разрешений на права доступа в эти зоны.

9.5 Замкнутые системы охранного видеонаблюдения и сопутствующие носители информации используются Поставщиком в качестве ответа на происшествия в системе безопасности, в качестве инструмента наблюдения за безопасностью, в качестве сдерживающего фактора или в качестве средства содействия возможному задержанию нарушителей, задержанных при совершении преступления. В случае записи изображений в замкнутой системе охранного видеонаблюдения (на пленку или в цифровом виде) они должны храниться не менее 20 дней. Тем не менее, данный период может быть увеличен в следующих ситуациях:
i) Если видеодоказательства из замкнутой системы охранного видеонаблюдения должны сохраняться в целях осуществления расследования происшествия или преступления.
ii) Если это обязательное требование предусмотрено законодательством.

Все видеопленки замкнутой системы охранного видеонаблюдения, используемые для записи изображений с камеры, должны храниться в закрытом на замок ящике, а хранение ключа должно осуществляться безопасным образом, а доступ к нему - контролироваться. Доступ к ящику должен предоставляться только разрешенному персоналу.
Все видео/цифровые видеорегистраторы замкнутой системы охранного видеонаблюдения должны быть расположены в незаметных местах для того, чтобы исключить возможность неразрешенного доступа и "случайного" просмотра любых связанных экранов системы видеонаблюдения.

9.6 Поставщик регулярно проверяет на предмет рисков и угроз окрестности объектов Поставщика, используемых для Продуктов и/или Услуг (в зависимости от обстоятельств).

9.7 Силовые кабели и кабели связи, по которым передаются данные или которые содействующие оказанию информационных услуг или услуг радиосвязи/спутниковой связи и используемые при предоставлении Товаров, должны оцениваться Поставщиком в части уровня защиты с целью предотвращения перебоев в коммерческой деятельности. Меры обеспечения физической безопасности, соразмерные степени критичности для коммерческой деятельности, которые они обслуживанию, должны быть реализованы следующим образом:
i) Критичные для бизнеса проезжие части, экранирующая оболочка кабеля, люки или колодцы, в которых находятся критичные для бизнеса кабели, должны быть защищены.
ii) Доступ к кабельным шахтам или кабельным колодцам в производственных зданиях должен быть ограничен при помощи электронных считывающих устройств для контроля доступа или эффективного управления ключами.
iii) Компьютерные каналы связи и коммуникационное оборудование в компьютерных системах должны быть защищены физически и от воздействия атмосферных явлений.
iv) Каналы радиосвязи и сотовой связи, а также коммуникационное оборудование должны быть надлежащим образом защищены.

9.8 Службы безопасности с участием человека являются необходимыми для дополнения мер электронной и физической безопасности на объектах Поставщика при следующих обстоятельствах:

- Объект является важным для операционной деятельности
- Обрабатываемая Информация ВТ может повлиять на Бренд и оказать воздействие на репутацию
- Большой объем обрабатываемой Информации ВТ (например, аутсорсинг процессов Предприятия)
- Договорные требования Клиента
- Риск/угроза, специфичные для конкретного объекта
- Поставщик располагает Информацией ВТ с высокой степенью конфиденциальности.

9.9 Для защиты Оборудования ВТ (такого, как Серверы или Коммутаторы ВТ), находящегося в помещениях Поставщика, от экологических угроз и опасностей, а также от возможности неразрешенного доступа, Оборудование ВТ должно находиться в охраняемой зоне и изолировано от оборудования, используемого для каких-либо систем организаций, не входящих в состав ВТ. Уровень изоляции должен гарантировать, что безопасность оборудования ВТ не будет преднамеренно или случайно подвергнута риску в результате предоставления доступа организациям, не входящим в состав ВТ, и может, например, быть реализован в форме установки безопасных перегородок, закрываемых на замок ящиков или металлических решеток.

9.10 Для предотвращения перебоев в установке, вызванных приостановкой оказания значимых услуг или иным экологическим воздействием принимаются меры для профилактики и выявление проблем.

- Пожар,
- Газ,
- Затопление
- Перебой в электропитании

Сигнализация должна быть установлена и подключена к посту с постоянным присутствие персонала с целью выявления следующего:

- Пожар,
- Газ,
- Перебой в электропитании,
- Отказ источника бесперебойного питания (ИБП).
- Отказ системы кондиционирования воздуха/контроля влажности/температуры

9.11 Периметры безопасности (такие барьеры, как стены, заборы, контролируемые при помощи карт доступа входные ворота или стойки регистрации с персоналом) используются для защиты зон, в которых находится Информация ВТ и средства обработки информации.

9.12 Такие точки доступа, как зоны доставки и погрузки, а также иные точки, в которых на территорию могут проникнуть неуполномоченные лица, должны находиться под контролем и, если это возможно, изолироваться от средств обработки информации во избежание неразрешенного доступа или преднамеренных атак.

9.13 Необходимо гарантировать, что физический доступ в зоны, в которых имеется Доступ к Информации ВТ, осуществляется исключительно при помощи смарт-карт или

бесконтактных карт (или эквивалентных систем безопасности), причем Поставщик регулярно проводит внутренние проверки для того, чтобы обеспечить выполнение требований настоящих положений.

9.14 Поставщик гарантирует реализацию запрета на фотографирование и/или фиксацию изображений любой Информации BT или Информации Клиентов BT. В исключительных обстоятельствах, когда требования бизнеса могут предусматривать фиксацию таких изображений, от Контактного лица BT в области безопасности необходимо в письменном виде получить временное исключение из этого правила с использованием Приложения 3.

9.15 Для защиты Информации BT Поставщик придерживается политики "чистый стол и чистый экран".

10. Предоставление среды хостинга

Выполнение условий Раздела 10 является обязательным, если Поставщик предоставляет среду хостинга для оборудования BT или Клиентов BT.

10.1 В случае если Поставщик предоставляет зону безопасного доступа в своих помещениях для хостинга оборудования BT или Клиентов BT ("Объект Поставщика"), Поставщик обязан:

(а) обеспечить наличие у всего Контрактного персонала, осуществляющего доступ к Объекту Поставщика, идентификационной карты или электронной карты для контроля доступа. Данная карта должна всегда использоваться в качестве средства подтверждения идентификационных данных на Объекте Поставщика и, в этой связи, отображаемое на карте фотографическое изображение, должно быть четким и достоверно отражать внешний вид Контрактного персонала; а также

(б) реализовать процедуры для устранения угроз безопасности, направленных на оборудование BT или Клиентов BT или третьей стороны, осуществляющей работы от имени BT, с целью защиты Информации BT и Информации Клиентов BT на Объекте Поставщика; а также

(в) использовать на Объекте Поставщика замкнутые системы охранного видеонаблюдения и сопутствующие носители информации в качестве ответа на происшествия в системе безопасности, в качестве инструмента наблюдения за безопасностью, в качестве сдерживающего фактора и в качестве средства содействия возможному задержанию нарушителей, задержанных при совершении преступления. Поставщик обязан обеспечить хранение записей замкнутой системы охранного видеонаблюдения в течение 20 дней в качестве инструмента расследования происшествий; а также

(г) предоставить BT поэтажный план выделенного места в безопасной зоне на Объекте Поставщика; а также

(д) гарантировать, что ящики BT и Клиентов BT на Объекте Поставщика закрываются на ключ, и к ним могут получать доступ только разрешенный персонал BT, утвержденные представители BT и соответствующий Контрактный персонал; а также

(е) реализовать на Объекте Поставщика процесс безопасного управления ключами; а также

(ж) регулярно осматривать окрестности Объекта Поставщика на предмет наличия рисков и угроз; а также

(з) осуществлять документирование и сопровождение операционных процедур (на языке страны происхождения Работ BT) с целью выполнения требований безопасности,

предусмотренных настоящим пунктом 12, а также, по запросу, предоставлять ВТ доступ к такой документации.

10.2 ВТ предоставляет Поставщику:
(а) учетную документацию о материальных активах ВТ и/или клиента ВТ, которые находятся на Объекте Поставщика; а также
(б) сведения о сотрудниках, субподрядчиках и агентах ВТ, которым необходим доступ к Объекту Поставщика (на постоянной основе).

11. Разработка Товаров

Выполнение условий Раздела 11 является обязательным, если Поставщик осуществляет деятельность по разработке Товаров для использования ВТ и/или Клиентами ВТ. (Сюда входят "серийные компоненты", Конфигурации программного обеспечения и производственные компоненты для Товаров)

11.1 Поставщик принимает согласованные меры безопасности по всем поставляемым компонентам, такие, как меры защиты конфиденциальности, доступности и целостности Товаров, путем:

(i) ведения соответствующей документации (на языке страны происхождения Работ ВТ) в отношении реализации мер безопасности и гарантирует, что она и такие меры безопасности соответствуют передовым отраслевым методикам
(ii) минимизации возможностей получения неразрешенными лицами (например, хакерами) доступа к Системам ВТ и Информации ВТ, Сетям ВТ или Услугам ВТ, а также
(iii) минимизации риска злоупотребления Системами ВТ и Информацией ВТ, Сетями ВТ или Услугами ВТ, которое потенциально способно привести к неполучению дохода или неоказанию услуг.

11.2 Поставщик по требования демонстрирует, что любая сборка поставляемого программного или аппаратного обеспечения (как проприетарного, так и серийного) предоставляется ВТ именно в таком виде, который согласован с ВТ. Поставщик поддерживает целостность сборок, включая обновление версий, операционные системы и приложения, от завода до рабочего места.

11.3 Поставщик гарантирует, что разработка систем для использования ВТ или конструкция и техническое обслуживание аппаратного обеспечения в собственности ВТ соответствуют Требованиям ИТ-безопасности ВТ (если они предоставлены операционной группой ВТ) или передовым методикам Отрасли.

11.4 Поставщик гарантирует, что среды разработки и тестирования не содержат производственных данных и изолированы от производственной среды. Тестовые данные, которые предоставляет ВТ, должны удаляться по истечении срока, определенного ответственным за данные лицом ВТ.

11.5 Поставщик гарантирует принятие всех обоснованных мер для того, чтобы обеспечить отсутствие в Программном обеспечении и/или аппаратном обеспечении (а также в предоставляемой в электронной форме Документации), помимо прочего, всех форм:
(i) "электронного владения" и "логических бомб";
(ii) "вирусов" и "червей", которые могли быть выявлены с использованием последнего (по состоянию на дату отправки)

коммерчески доступного антивирусного программного обеспечения; а также
(ii) "программ-шпионов", "рекламного ПО" и иного вредоносного программного обеспечения.
(указанные выражения имеют значения, общепринятые в компьютерной отрасли);
Поставщик гарантирует, что в момент и после приемки, Программное обеспечение и/или аппаратное обеспечение будет функционировать в соответствии с Функциональной спецификацией в течение Гарантийного периода; а также Поставщик применяет только качественные материала, методики и Требования безопасности при выполнении Контракта и в любой момент времени применяет Требования безопасности с той степенью аккуратности, профессионализма и осмотрительности, которые соответствуют добросовестной практике выполнения работ в компьютерной сфере и методикам защитного кодирования.

11.6 Поставщик сотрудничает с BT с целью обеспечения выполнения требований безопасности согласно соответствующей инфраструктуре(инфраструктурам) безопасности за счет Поставщика; время от времени это может потребовать проведения соответствующего тестирования Товаров на предмет безопасности.

11.7 Все недостатки безопасности в Товарах, выявленные BT или Поставщиком, устраняются за счет Поставщика в течение такого срока, который обоснованно потребует BT.

12. Доступ к информации

Применимо, если это предусмотрено Требованиями.

12.1 В течение 14 дней с момента письменного требования BT и по выбору BT:
(a) Стороны, оплачивая свои собственные соответствующие расходы, оформляют и предоставляют друг другу соглашение о доступе к информации по форме Соглашения о доступе к информации, изложенному в Дополнении 3; или
(б) Поставщик, за свой собственный счет, заключает договор об условном депозите, оформленный, в существенных отношениях, по форме соглашения, предусмотренной Дополнением 21, в отношении всей Информации и документации, связанных с Товарами (включая, помимо прочего, связанные с Программным обеспечением, всем исходным кодом, компоновочными данными, списками программного обеспечения, полными техническими данными, примечаниями программиста, всей информации и документации, связанной с Программным обеспечением, которое необходимо для сопровождения, видоизменения и доработки Программного обеспечения и оказания всех уровней поддержки по Программному обеспечению) ("Условно доступная информация") и передает на условное хранение в "Эн-Си-Си Эскроу Интернешнл Лимитед" (NCC Escrow International Limited) ("Депозитарный агент") актуальную копию Условно доступной информации. Поставщик гарантирует, что такая Условно доступная информация позволит BT и/или любым компетентным третьим сторонам от имени BT:

(i) выполнять любые невыполненные обязательства Поставщика по Контракту, включая, помимо прочего, обязательства, которые существовали бы (включая требования о выполнении любых заказов, которые BT в ином случае разместила бы согласно Контракту), если бы Контракт не был расторгнут со стороны BT (за исключением случаев, предусмотренных пунктом 4 Условия под заголовком "Расторжение") до момента истечения его естественного

срока действия (что включает в себя любой срок продления по любому решению BT продлить первоначальный срок действия); а также
(ii) без труда понимать Условно доступную информацию, осуществлять сопровождение (в том числе - актуализацию), видоизменение и исправление Условной доступной информации и Товаров.

12.2 Поставщик гарантирует, что сопровождение Условно доступной информации, переданной на хранение в BT или Депозитарному агенту (в зависимости от обстоятельств), осуществляется и будет осуществляться таким образом, который достаточен для того, чтобы достаточно квалифицированный программист или аналитик мог осуществлять сопровождение или доработку Программного обеспечения, не прибегая к любому иному лицу или справочной информации; Поставщик также обязуется обеспечивать полную актуальность Условно доступной информации в течение Срока действия.

12.3 При наступлении любого события, которое разрешает BT или Депозитарному агенту (в зависимости от обстоятельств) использовать и/или предоставлять Условно доступную информацию, Поставщик обязан немедленно предоставить BT за свой собственный счет на обоснованный срок такие консультации, поддержку, содействие, данные, информацию, доступ к ключевому персоналу Поставщика или его лицензиару Программного обеспечения с целью понимания, сопровождения (включая актуализацию), совершенствование, видоизменение и исправление любой Условно доступной информации и/или Программного обеспечения.

12.4 Без ограничения любых иных прав, которые она может иметь, BT автоматически имеет неисключительное, вечное, безотзывное, действующее по всему миру право безвозмездно использовать Условно доступную информацию, после ее предоставления, с целью сопровождения и поддержки Товаров с неисключительным, вечным, безотзывным, действующим по всему миру правом использовать, копировать, сопровождать (в том числе - актуализировать), видоизменять, адаптировать, совершенствовать и исправлять Товары и любые видоизмененные, адаптированные, усовершенствованные и/или исправленные Товары, а также лицензировать такие Товары третьим сторонам (с учетом ограничений любых лицензий, выданных Поставщику), вместе с правом разрешать третьим сторонам осуществлять любые из вышеописанных действий от имени BT.

12.5 Настоящее Условие сохраняет силу после истечения срока действия или расторжения Контракта.

12.6 Если это необходимо с целью обеспечения выполнения требований в связи с вопросами безопасности, Контактное лицо BT в области сетевой безопасности (и/или назначенные им лица, которые должны быть сотрудниками BT) имеют аналогичные права (с учетом необходимых изменений), в случае, если они требуются в составе Товаров, Ознакомления и Проверки (в соответствии с определениями в Соглашении о доступе к информации) в отношении Исходного материала (в соответствии с определением в Соглашении о доступе к информации).

13. Доступ к Системам BT

Выполнение условий Раздела 13 является обязательным, если Контрактному персоналу Поставщика необходимо получить доступ к Системам BT с целью предоставления Товаров.

13.1 BT может, по своему собственному усмотрению, в степени, в которой определяет BT, предоставлять доступ для предоставления Товаров в то время как Поставщику Разрешено осуществлять доступ.

13.2 В отношении доступа, Поставщик обязан (а также, в соответствующих случаях, должен гарантировать, что весь Контрактный персонал обязан):

а) гарантировать, что средства идентификации пользователей, пароли, PIN-коды, аппаратные ключи и доступ к телеконференциям предназначены для конкретного Контрактного персонала и не передаются иным лицам. Информация должна храниться безопасным образом изолированно от устройства, для доступа к которому она используется. Если пароль становится известным иному лицу, он должен быть немедленно изменен.

б) По обоснованному требованию предоставлять BT такие отчеты, которые BT запросит относительно Контрактного персонала, которому Разрешено осуществлять доступ к Системам BT.

в) Перекрестное подключение между доменами к Системам BT не допускается, за исключением случаев, когда это в явной форме одобрено и разрешено Контактным лицом BT в области безопасности с использованием Приложения 3.

г) Прилагать все обоснованные усилия для того, чтобы гарантировать отсутствие проникновения вирусов или вредоносного кода (в соответствии с общепринятым в компьютерной отрасли пониманием данных выражений) с целью минимизации риска повреждения Систем BT или Информации BT.

д) Прилагать обоснованные усилия для того, чтобы гарантировать, что персональные файлы, которые содержат информацию, данные или носители, не имеющие отношения к Товарам, не хранятся на серверах BT, Предоставленных BT переносных и настольных компьютерах, в централизованных хранилищах или Системах BT.

13.3 В случае если BT предоставила Поставщику доступ в Интернет/к внутренней сети, Поставщик обязан, а также должен гарантировать, что Контрактный персонал обязан, осуществлять доступ в Интернет/к внутренней сети надлежащим образом для того, чтобы иметь возможность предоставлять Товары (в зависимости от обстоятельств). Поставщик обязан гарантировать доведение следующих указаний по злоупотреблению Интернетом и электронной почты до сведения Соответствующего Контрактного персонала не реже одного раза в год.

Запрещается доступ к материалам, которые могут рассматриваться как: -

а. Оскорбительные, сексуальные, сексистские, расистские, политически оскорбительные;
б. Действие, которое может нанести ущерб репутации BT или физических лиц;
в. Ведение частного бизнеса;
г. Нарушение авторского права;
д. Телефонная связь или обмен сообщениями через Интернет, например, Skype
е. Обход или преодоление межсетевого экрана BT или иных механизмов обеспечения безопасности;

ж. Запрещается размещать на сайтах сообщения или публиковать в Интернете заявления, которые могут быть обоснованно сочтены точкой зрения ВТ.
з. Неприемлемые или опасные сайты должны быть заблокированы и недоступны пользователю.

13.4 Поставщик немедленно уведомляет ВТ в случае, если любой Соответствующий Контрактный персонал более не нуждается в правах доступа к Системам ВТ, или его роль по какой-либо причине изменяется по сравнению с указанной в Соглашении, что дает возможность ВТ аннулировать или видоизменить права доступа к Системам ВТ.

14. Доступ к Информации ВТ в Системах Поставщика

Выполнение условий Раздела 14 является обязательным, если Информация ВТ хранится или Обрабатывается в Системах Поставщика.

14.1 Если Контрактному персоналу предоставлен Доступ к Системам Поставщика, связанным с предоставлением Поставщиком Продуктов и/или Услуг для ВТ, Поставщик:

а) гарантирует наличие у каждого физического лица уникального пользовательского идентификатора и пароля (который отвечает передовым методикам, соответствующим отраслевым стандартам), известных только такому физическому лицу для исключительного использования им/ей для осуществления процесса безопасного входа в систему.
б) представляет Доступ к Системам в собственности Поставщика, на которых осуществляется хранение или доступ к Информации ВТ, только в минимальной степени, необходимой для того, чтобы предоставить Контрактному персоналу возможность выполнять свои служебные обязанности в соответствии с Соглашением.
в) поддерживает функционирование официальных процедур для контроля распределения, пересмотра и отзыва и/или прекращения действия прав доступа.
г) гарантирует, что распределение и использование расширенных привилегий и доступа к конфиденциальным инструментам и средства в Системах Поставщика контролируется и ограничивается только кругом пользователей, у которых имеется деловая потребность. Доступ к системным консолям и управление ими осуществляется в рамках безопасной среды, которая соизмерима активам, для управления которыми они используются. Для предотвращения неразрешенного доступа должны иметься соответствующие средства физической безопасности.
д) гарантирует, что распределение пользовательских паролей к Системам в собственности Поставщика, на которых осуществляется доступ или хранение Информации ВТ, контролируется при помощи официального проверяемого процесса управления.
е) регулярно осуществляет пересмотр пользовательских прав доступа.
ж) гарантирует, что физический доступ к компьютерному оборудованию, которое имеет доступ или на котором хранится Информация ВТ, осуществляется исключительно при помощи смарт-карт или бесконтактных карт (или эквивалентных систем безопасности), причем Поставщик регулярно проводит внутренние проверки для того, чтобы обеспечить выполнение требований настоящих положений.
з) демонстрирует, что пользователи придерживаются передовых методик в области безопасности при управлении своими паролями.

и) реализует систему управления паролями, которая предоставляет безопасное и эффективное интерактивное средство, гарантирующее высокое качество паролей.
к) гарантирует завершение пользовательских сеансов по истечении определенного периода неактивности.
л) гарантирует создание контрольных журналов для фиксации действий пользователей и связанных с безопасностью событий, а также управление такими журналами безопасным образом. Ведение журналов осуществляется в течение обоснованного периода для содействия в проведении любого расследования при полном отсутствии у Поставщика возможности позволить осуществление любого неразрешенного доступа или изменение контрольных журналов.
м) гарантирует, что мониторинг контрольных журналов и журналов событий и аналитических отчетов на предмет аномального поведения и/или попыток неразрешенного доступа осуществляется персоналом Поставщика, независимым от пользователей, которые являются предметом мониторинга.

14.2 Поставщик поддерживает функционирование систем, позволяющих выявлять и фиксировать любую попытку нанесения ущерба, видоизменения или неразрешенного доступа к Информации ВТ или Системам Поставщика. В числе примеров (помимо прочего) - процессы регистрации и контроля систем, системы обнаружения вторжений, системы предотвращения вторжений и т.п.

14.3 поддерживает функционирование средств контроля для выявления и защиты от вредоносного программного обеспечения и обеспечивает реализацию соответствующих процедур осведомления пользователей.

14.4 гарантирует, что любое неразрешенное программное обеспечение не реже одного раза в неделю выявляется и удаляется из Систем Поставщика, на которых осуществляется хранение, обработка или доступ к Информации ВТ.

14.5 гарантирует безопасный контроль доступа к диагностическим и административным портам, а также диагностическим инструментам.

14.6 гарантирует ограничение доступа к проверочным инструментам Поставщика кругом Соответствующего Контрактного персонала, а также мониторинг их использования.

14.7 гарантирует, что анализ кода и испытания на возможность проникновения по всему программному обеспечению собственной разработки, используемому для обработки Информации ВТ, осуществляется группой, независимой от разработчиков.

14.8 В той степени, в которой какие-либо серверы используются для предоставления Товаров, они не должны разворачиваться в недоверенных сетях (сетях за пределами вашего периметра безопасности, которые находятся вне вашего административного контроля, например, сетях с выходом в Интернет) без надлежащих мер безопасности.

14.9 Изменения в отдельные Системы Поставщика, на которых осуществляется хранение и обработка Информации ВТ, и/или которые используются для

предоставления Продуктов и/или Услуг для BT, должны контролироваться с учетом требований официальных процедур контроля изменений.

14.10 Все системы должны иметь собственные внутренние часы, синхронизируемые с доверенным источником.

15. Хостинг Информации BT у Поставщика

Выполнение условий Раздела 15 является обязательным в случае если Поставщик осуществляет внешний хостинг Информации BT, классифицированной как Конфиденциальная или выше, в среде Облачных служб или в серверной среде Поставщика или Субподрядчиков.

15.1 Поставщик, по отношению к Товарам, гарантирует, что среды, в которых осуществляется хостинг Информации BT, отвечают требованиям, предусмотренным Приложением 5.

16. Сетевая безопасность

Выполнение условий Раздела 16 является обязательным в случае, если Поставщик осуществляет создание, разработку или поддержку Сетей BT или Сетевых активов.

16.1 Поставщик, по отношению к Товарам, реализует такие согласованные меры безопасности по всем поставляемым компонентам, которые обеспечивают защиту конфиденциальности, доступности и целостности Сетей BT и/или активов 21CN. Поставщик предоставляет BT полную документацию в отношении реализации Сетевой безопасности в части Товаров, а также гарантирует, что он и такая безопасность:

(а) отвечает всем правовым и регулятивным требованиям; а также
(б) прилагает максимальные усилия для предотвращения получения неразрешенными лицами (например, хакерами) доступа к Элементам управления сетью и иным элементам, доступ к которым осуществляется через Сети BT и/или 21CN; а также
(в) прилагает максимальные усилия для снижения риска злоупотребления Сетями BT и/или 21CN, который потенциально способен привести к потере дохода или неоказанию услуги, лицами, которым разрешено получать к ним доступ; а также
(г) прилагает максимальные усилия для выявления нарушений защиты, которые все же происходят, позволяя оперативно устранить любые возникшие в результате проблемы, выявить лиц, которые получали доступ, и определить способ, как они это осуществили; а также
(д) минимизирует риск неправильного конфигурирования Сетей BT, например, путем предоставления минимальных разрешений, необходимых для выполнения договорной роли.

16.2 Поставщик обязан принять все обоснованные меры для защиты всех интерфейсов на поставляемых компонентах, а также не должен исходить из того, что поставляемые компоненты работают в защищенной среде.

16.3 Поставщик предоставляет Контактному лицу BT в области сетевой безопасности имена, адреса (а также иные сведения, которые потребует BT) всего конкретного Контрактного персонала, который в соответствующий момент времени будет непосредственно участвовать в развертывании, техническом обслуживании и/или управлении Товарами до того, как они, соответственно будут привлечены к такому развертыванию, техническому обслуживанию и/или управлению.

16.4 В отношении деятельности по поддержке, осуществляемой в Великобритании, Поставщик нанимает квалифицированную группу в области безопасности, состоящую не менее чем из одного гражданина Великобритании, который доступен для поддержания связи и взаимодействия с Контактным лицом BT в области сетевой безопасности (или назначенными им лицами) и присутствия на таких совещаниях, которые Контактное лицо BT в области сетевой безопасности обоснованно потребует в соответствующее время.

16.5 Поставщик предоставляет Контактному лицу BT в области сетевой безопасности план (по мере необходимости актуализируемый в соответствующее время) всех активных компонентов, содержащихся в Товарах, а также их соответствующих источников.

16.6 Поставщик предоставляет сведения о своем конкретном персонале, который будет осуществлять связь и взаимодействие с группой BT по управлению уязвимостями (CERT) в части обсуждения выявленных BT и Поставщиком уязвимостей в Товарах. Поставщик своевременно предоставляет BT информацию об уязвимостях и выполняет такие обоснованные требования в отношении к уязвимостям, которые Контактное лицо BT в области сетевой безопасности может сообщать в соответствующее время (за счет Поставщика). Поставщик информирует BT о любых уязвимостях за время, достаточное для реализации минимизирующих средств контроля до момента публичного сообщения Поставщиком о таких уязвимостях.

16.7 Поставщик предоставляет Контактному лицу BT в области сетевой безопасности и назначенным им в соответствующее время лицам полный и неограниченный доступ в любые помещения, в которых осуществляется разработка, производство или сборка Товаров, для проведения испытаний и/или оценок на предмет соблюдения требований безопасности; Поставщик сотрудничает (а также гарантирует, что весь соответствующий Контрактный персонал сотрудничает) при проведении такого тестирования на предмет соблюдения требований.

16.8 Поставщик гарантирует, что любые связанные с безопасностью компоненты, включенные в Товары, которые в соответствующее время установлены BT или о которых BT поставлена в известность, проходят, за счет Поставщика, стороннюю оценку к обоснованному удовлетворению BT.

16.9 В отношении любой Информации, которую предоставляет BT или которая получена от BT, и которая помечена как "СТРОГО КОНФИДЕНЦИАЛЬНО" или которая явно может рассматриваться как конфиденциальная, Поставщик гарантирует, что:

(a) доступ к ней предоставляется только тому Контрактному персоналу, которому BT в явной форме разрешила просматривать ее и работать с ней, а также что ведется учетная документация по такому доступу;

(б) работа с ней, ее использование и хранение осуществляются с осторожностью, а также что она, до начала хранения, шифруется с использованием PGP или WinZip 9, а также при условиях, которые обеспечивают высокую степень защиты от преднамеренного нарушения функционирования (т.е. с использованием наиболее устойчивого алгоритма шифрования из имеющихся / с использованием устойчивого пароля) и дают возможность с большой долей вероятности выявить фактическое нарушение функционирования или его попытку;
(в) при ее передаче к ней применяются достаточные меры безопасности путем ее шифрования при помощи защищенной электронной почты, PGP или WinZip 9; а также
(г) она не будет экспортироваться за пределы Европейского экономического пространства без письменного разрешения BT.

16.10 Поставщик незамедлительно и, в любом случае, не позднее 7 Рабочих дней, предоставляет Контактному лицу BT в области сетевой безопасности полные сведения о любых характеристиках и/или функционале в любых Товарах (или таковых, которые запланированы в Оперативном плане для любых Товаров), которые в соответствующий момент времени:

(а) известны Поставщику; или
(б) Контактное лицо BT в области сетевой безопасности обоснованно полагает предназначенными или которые могут быть использованы для законного перехвата или любого иного перехвата телекоммуникационного информационного потока, и о которых оно сообщает Поставщику. Такие сведения включают всю Информацию, которая обоснованно необходима для того, чтобы позволить Контактному лицу BT в области сетевой безопасности составить полное представление о характере, составе и уровне таких характеристик и/или функционала.

16.11 С целью поддержания доступа к Сетям и/или Системам BT Поставщик немедленно уведомляет BT о любых изменениях, вносимых в способ своего Доступа через межсетевые экраны, включая предоставление данных о трансляции сетевых адресов.

16.12 Запрещается использовать инструменты сетевого мониторинга, позволяющие просматривать информацию приложений.

16.13 Функционал IPv6, включенный в операционные системы, должен быть отключен на ведущих узлах (устройствах конечных пользователей, серверах), подключающихся к сетевым доменам BT должен быть отключен, если он не является необходимым.

16.14 Поставщик выполняет и гарантирует, что Товары выполняют требования политик BT (если они предоставлены) и Требований безопасности BT; любые отклонения должны быть согласованы при подписании контракта или в соответствии с процедурой контроля изменений.

16.15 Поставщик гарантирует, что весь Контрактный персонал прошел проверки при приеме на работе, соответствующие уровню Доступа
http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

Требования безопасности BT для поставщиков

Поставщики, осуществляющие создание, разработку или поддержку Сетей BT или Сетевых активов BT, гарантируют, что весь Контрактный персонал прошел, как минимум, проверки при приеме на работу Уровня 2. Проверки при приеме на работу Уровня 3 обязательны для ролей, определенных Контактным лицом BT в области сетевой безопасности. В случае если у Поставщика отсутствует возможность непосредственно осуществить проверку безопасности Контрактного персонала в рамках проверок Уровня 3, BT содействует в осуществлении такой проверки безопасности за счет Поставщика.

17. Безопасность сетей Поставщика

Выполнение условий Раздела 17 является обязательным, если сеть Поставщика предполагается использовать для предоставления Товаров (сюда входят локальные сети, сети широкого охвата, Интернет, беспроводные сети и радиосети)

17.1 Поставщик, по отношению к Товарам, реализует такие меры безопасности по своим сетям, которые обеспечивают защиту конфиденциальности, доступности и целостности Информации ВТ. Данные меры должны:

(а) отвечать всем правовым и регулятивным требованиям; а также
(б) в максимальной степени способствовать предотвращению получения неразрешенными лицами (например, хакерами) доступа к Сети, а также
(в) в максимальной степени способствовать снижению риска злоупотребления Сетями, что потенциально способно привести к потере дохода или неоказанию услуги, лицами, которым разрешено получать к ним доступ; а также
(d) в максимальной степени способствовать выявлению нарушений защиты, которые все же происходят, позволяя оперативно устранить любые возникшие в результате проблемы, выявить лиц, которые получали доступ, и определить способ того, как они это осуществили

18. Облачная безопасность

Выполнение условий Раздела 18 также является обязательным, когда Поставщик предоставляет ВТ Облачные службы. Определение термина "Облачный" приведено в Публикации Национального института стандартов и технологий (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)

18.1 Поставщики предоставляют соответствующие свидетельства того, что предоставляемые Облачные службы отвечают требованиям к системе управления, предусмотренным Матрицей облачной безопасности (CCM) компании Cloud Security Alliance в последней выпущенной редакции, доступной по адресу https://cloudsecurityalliance.org (в дополнение к выполнению положений Приложения 5 настоящих Требований безопасности).

18.2 Информация ВТ, используемая в электронной коммерции с применением публичных сетей, защищается при ее передаче и хранении в соответствии с Приложением 1 (включая Резервные копии) от мошеннических действий, неразрешенного раскрытия, доступа и видоизменения.

18.3 В соглашениях об уровне сетевого и инфраструктурного обслуживания (внутрифирменного и переданного на аутсорсинг) должны быть четко документированы меры безопасности, мощности и уровни обслуживания, а также требования бизнеса или требования клиента.

18.4 Поставщик разрешает проведение испытаний на возможность проникновения и/или доступ к существующим отчетам Поставщика по испытаниям на возможность

проникновения, имеющим отношение к предоставляемым Товарам; диапазон и сроки испытаний подлежат взаимному согласованию с ВТ.

18.5 Поставщик принимает согласованные меры безопасности по всем поставляемым компонентам, такие, как меры защиты конфиденциальности, доступности, качества и целостности Товаров, путем минимизации возможностей для неразрешенных лиц (например, иных клиентов облачных служб) получить доступ к Информации ВТ и Услугам ВТ.

Словарь терминов

В настоящих Требованиях применяются следующие определения, однако в других отношениях к настоящим Требованиям безопасности применимы условия Контракта, причем все слова и выражения, использованные в настоящих Требованиях безопасности, имеют те же значения, указанные для них в Контракте.
["**Доступ**" - Обработка, применение или хранение Информации ВТ одним или несколькими следующими способами:

- Путем взаимосвязи с Системами ВТ
- На бумажном носителе или в неэлектронной форме
- Посредством Информации ВТ в Системах Поставщика
- на мобильных носителях

и/или путем доступа к Зданиям ВТ с целью оказания услуг (за исключением предоставления аппаратного обеспечения и посещения собраний)"
[**Разрешенный**" - ВТ одобрила Доступ в рамках процесса Взаимосвязи систем ВТ, или от ответственного за предприятие или проект лица ВТ было получено письменное разрешение; "**разрешение**" истолковывается соответственно. Предоставленный уровень доступа должен быть адекватным и ограниченным уровнем, необходимым для оказания Услуг.]
"**Объекты ВТ**" - все объекты, которые ВТ предоставляет Поставщику, а также все объекты во владении Поставщика, которые принадлежат ВТ (например, ключи от ящиков, аппаратные ключи, карточки-пропуска, планы, технологические документы.)
"**Контактное лицо ВТ в области сетевой безопасности**" - Специалист по обеспечению доступности; целостности и безопасности информации из Службы безопасности ВТ, связь с которым осуществляется путем заполнения и подачи формы запроса, описанной в Приложении 3, или такое иное лицо, идентификационные и контактные данные которого могут быть в соответствующее время доведены до сведения Контактного лица по коммерческим вопросам Поставщика.
"**Материальные активы ВТ**" - все Материальные активы во владении Поставщика, которые принадлежат ВТ (например, маршрутизаторы, коммутаторы, серверы или документация)
"**Службы безопасности ВТ**" - организация по обеспечению безопасности в рамках ВТ.
"**Контактное лицо ВТ в области безопасности** " – Специалист по обеспечению доступности; целостности и безопасности информации из Службы безопасности ВТ, связь с которым осуществляется путем заполнения и подачи формы запроса, описанной в Приложении 3.
"**Политика безопасности ВТ**" означает соответствующую политику сетевой безопасности, которую предоставляет ВТ.
"**Системы ВТ**" – службы и компоненты служб, продукты, сети, серверы, процессы, системы в бумажной форме или ИТ-системы (целиком или частично) находящиеся в собственности или эксплуатируемые ВТ, BT Group plc или любой организацией ВТ

Group plc либо от имени таковых; или любые такие системы, хостинг которых может осуществляться в Помещениях BT (включая iSupplier (в соответствии с определением "iSupplier", приведенным в Разделе Соглашения, озаглавленном "Оплата и выставление счетов"), используемые в контексте "Доступа" (в соответствии с вышеприведенным определением).

"**Замкнутая система охранного видеонаблюдения**" - означает замкнутую видеосистему.

"**Начальная дата**" – в соответствии с определением, приведенным в контракте.

"**Контрактный персонал**", "**Соответствующий контрактный персонал"** - в соответствии с определением, приведенным в контракте.

"**Информация**" - означает информацию в вещественной или любой иной форме, включая, помимо прочего, спецификации, отчеты, данные, заметки, документацию, чертежи, программное обеспечение, политики, процедуры, процессы, стандарты, выводимые из компьютеров данные, конструкции, принципиальные схемы, модели, шаблоны, образцы, изобретения (с возможностью патентования или без таковой) и ноу-хау, а также носители (при наличии таковых), на которых поставляется такая информация.

"**ISO 27001**" - международный стандарт систем управления безопасностью, принятый Международной организацией стандартизации и Международной электротехнической комиссией.

"**Заказ(заказы**)" - заказ на Товары, размещенный BT у Поставщика в соответствии с Контрактом.

"**Сетевая безопасность**" - означает безопасность взаимосвязанных каналов и узловых точек связи и, которые логически соединяют конечные пользовательские технологические устройства и сопутствующие системы управления.

"**Персональные данные**" - имеет значения, указанные в Директиве 95/46/EC или любых последующих законодательных актах, принятых в связи с ней ("Директива").

"**Обрабатывать," "Обработанный" или "Обработка**" означает любую операцию или набор операций, которые выполняются с Информацией BT автоматическим или иным образом, такие как накопление, запись, организация, хранение, адаптация или изменение, извлечение, сверка, использование, раскрытие путем передачи, распространения или предоставления иным образом, компоновка или объединение, блокирование, удаление, возврат или уничтожение

"**Закрытая информация**" - любая Информация BT, классифицированная или помеченная как "Конфиденциальная" или выше, включая Персональные данные.

"**Субподрядчик**"- в соответствии с определением, приведенным в контракте.

"**Системы Поставщика**" - любые находящиеся в собственности Поставщика компьютерные, прикладные или сетевые системы, используемые для получения доступа, хранения или обработки Информации BT или участвующие в предоставлении ресурсов.

"**Контактное лицо Поставщика в области безопасности**" - лицо, контактная информация которого в соответствующее время доводится Поставщиком до сведения BT, и которое является Единым контактным лицом по вопросам, связанным с Безопасностью.

"**Товары**" - все компоненты, материалы, машины, инструменты, испытательное оборудование, документация, встроенные программы, Программное обеспечение, запасные части, детали и предметы, которые должны быть предоставлены для BT в соответствии с Контрактом, вместе со всем Информацией и Работами, которые должны быть поставлены или выполнены для BT согласно требованиям Контракта.

"**Передача" или "Переданный**" означает

(а) перемещение Информации ВТ во владении Контрактного персонала (включая, помимо прочего, Персональные данные) из одного объекта в другой или от одного лица другому, будь то физическим, голосовым или электронным образом; а также (б) предоставление доступа к Информации ВТ во владении Контрактного персонала (включая, помимо прочего, Персональные данные) одним объектом другому или одним лицом другому, будь то физическим, голосовым или электронным образом.

Дата	Изменения	Выпуск
апрель 2015 г.	Запуск	1.0
апрель 2015 г.	Смена нумерации	1.0
август 2015 г.	Изменение форматирования Приложения 4 и извлечение встроенных приложений	1.0
январь 2016 г.	Обновление ссылок на Обязательное обучение	1.0