Приложение [XX] – Требования к безопасности поставщиков компании BT

Содержание

ГЛАВА 1: ВВЕДЕНИЕ

1 ВВЕДЕНИЕ

1.1 Настоящий документ устанавливает требования к безопасности в компании BT.

1.2 В настоящем документе применяются термины, приведенные в Главе 5 **«Определения»**. В противном случае в настоящем документе будут применяться положения Договора, а все слова и выражения, используемые F в настоящем документе, должны иметь то же значение, что и в Договоре.

1.3 Настоящие Требования безопасности дополняют, не исключая каких-либо других обязательств Поставщика по Договору (включая, помимо прочего, его обязательства в соответствии с положениями глав «**Конфиденциальность**», «**Защита персональных данных**» и «**Соответствие**»).

ГЛАВА 2: ТРЕБОВАНИЯ К ОГРАНИЧЕНИЮ ДОСТУПА

2 ТРЕБОВАНИЯ К ОГРАНИЧЕНИЮ ДОСТУПА

Положения этого раздела рекомендуется применять в случае, если Поставщик выполняет Поставки, связанные с ограниченным доступом к информации о клиентах компании BT или компании BT, или имеет доступ на уровне пользователя к административным системам компании BT. Поставщики, попадающие под эту категорию, не будут обязаны выполнять какие-либо другие части настоящего документа.

2.1 Без исключения каких-либо возможных обязательств относительно конфиденциальности, если Поставщик или персонал по контракту имеют доступ к информации компании BT, Поставщик обязан:

2.2 исключить раскрытие информации о компании BT персоналу по контракту или предоставление доступа к такой информации персоналу по контракту, кроме случаев, когда это необходимо для Поставки; а также

2.3 внедрить технические и организационные меры согласно требованиям Передовых отраслевых методов обеспечения безопасности для обеспечения безопасности и конфиденциальности информации и систем компании BT.

ГЛАВА 3: ОБЩИЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

Обязательно при соответствии Главе 2: Требования к ограничению доступа не рекомендованы к применению.

3 ОБЩИЕ ПОЛОЖЕНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Общие положения по защите информации

3.1 Поставщик обязан внедрять системы и процессы (технические и организационные), чтобы:

3.1.1 обеспечить безопасность и конфиденциальность информации и систем компании BT, как предписано настоящими Требованиями безопасности;

3.1.2 обеспечить доступность, качество, целостность и достаточный объем для обеспечения бесперебойной доставки в соответствии с требованиями отраслевых Передовых отраслевых практик обеспечения безопасности.

3.2 Поставщик обязан внедрить и использовать формальную процедуру управления изменениями IT, чтобы гарантировать, что любые изменения процессов и систем Поставщика будут реализованы таким образом, чтобы исключить нарушение Поставщиком положений настоящих Требований безопасности.

3.3 По письменному запросу компании BT Поставщик обязан предоставить компании копии любых сертификатов безопасности и заявлений о соответствии, относящихся к Поставкам, в целях демонстрации доказательств соблюдения настоящих Требований безопасности.

3.4 Поставщик обязан принять все обоснованные меры для назначения соответствующего ответственного лица (лиц) на должность контактного лица по Обеспечению безопасности, Управления инцидентами и Управления соответствием. Поставщик обязан сообщить Контактному лицу компании BT по безопасности контактные данные такого лица (лиц) и уведомлять о любых изменениях в них. Контактные данные должны включать в себя:

Ф.И.О., обязанности, должность, групповой адрес электронной почты и/или номер телефона

3.5 Поставщик подтверждает и соглашается с тем, что компания BT периодически может вносить обоснованные изменения в Требования безопасности компании BT, если:

3.5.1 Поставщик подвергается слиянию, приобретению или существенным изменениям в форме собственности или управления;

3.5.2 внесены изменения в технологии или отраслевые стандарты безопасности;

3.5.3 внесены существенные изменения Поставки или порядок их предоставления

(каждый пункт является «**Изменением требований безопасности**»).

После получения письменного уведомления от компании BT о необходимости внесения изменений в Требования безопасности Поставщик обязан незамедлительно при любых обстоятельствах внести соответствующие изменения в требования безопасности в приемлемые сроки (с учетом характера изменений и риска для BT).

3.6 Поставщик обязан, как минимум, ежегодно или в случае существенных изменений в Поставках или порядке их предоставления, пересматривать Требования безопасности, чтобы обеспечить их соответствие всем применимым Требованиям безопасности.

3.7 Если Поставщик передает обязательства по Договору субподрядчику, Поставщик обязан заключить все договора с соответствующими Субподрядчиками, включая письменные условия, требующие от Субподрядчика соблюдения Требований безопасности поставщика компании BT в том объеме, в какой они применимы. Эти условия должны быть внедрены между Поставщиком и его Субподрядчиком до того, как Субподрядчик или любой его персонал смогут получить доступ к системам и информации компании BT.

Использование информации компании BT

3.8 Поставщик не должен использовать информацию BT в каких-либо целях, кроме тех, для которых она была предоставлена Поставщику, и только в той мере, в какой это необходимо для выполнения Поставщиком обязанностей согласно Договору. В случае обработки персональных данных Поставщик не должен использовать личные данные, являющиеся частью информации компании BT в любых целях, кроме целей, указанных в Приложении «Обработка».

3.9 Информация компании BT может храниться до тех пор, пока это необходимо для выполнения обязательств по Договору, после чего она должна храниться не более двух лет, если иное не будет согласовано между компанией BT и Поставщиком, или требуется по закону. Во избежание неправильного толкования обработки персональных данных Поставщиком он не должен хранить Персональные данные, являющиеся частью информации компании BT, дольше, чем указано в Приложении «Обработка», или Правилах **«Защита персональных данных»**.

3.10 Поставщик обязан соблюдать следующие применимые политики и стандарты:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Если Поставки напрямую поддерживаются британским правительственным договором, Поставщик обязан соблюдать положения новейшей версии правил Cyber Essentials Plus.

Обработка информации

3.12 Поставщик обязан иметь и соблюдать правила обработки информации, которые в значительной степени соответствуют положениям Правил классификации и обработки данных третьих сторон и, как минимум, обязывают Поставщика:

3.12.1 внедрить соответствующие процессы для предотвращения несанкционированного распространения информации компании BT в любой форме, в том числе по электронной почте, факсу, в социальных сетях, в печати или по почте (например, чтобы обеспечить четкую политику чистого стола и экрана, и исключить возможность отправки информации с грифом «Совершенно секретно» по факсу или электронной почте);

3.12.2 не обсуждать информацию компании BT на собраниях, кроме случаев, когда участники собраний: (i) уполномочены присутствовать на собрании; (ii) должны знать обсуждаемую информацию; (iii) знают и соблюдают свои обязанности по работе с конфиденциальной информацией;

3.12.3 не хранить информацию компании BT:

3.12.3.1 в облаке или с использованием интернет-сервисов, включая, помимо прочего, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin или Facebook, если иное не согласовано с компанией BT в письменной форме;

3.12.3.2 на любом ноутбуке или другом устройстве, если он не защищен полной функцией полнодискового шифрования (например, BitLocker), соответствующей стандартам в пункте 3.15; или

3.12.3.3 удалять или размещать информацию BT за пределами ежедневной коммерческой деятельности безопасным образом.

Контроль доступа

3.13 Поставщик обязан контролировать доступ в системах поставщика согласно режиму и характеру поставок в компанию BT, в том числе обеспечивать, где это применимо:

3.13.1 присвоение всем пользователям, в том числе администраторам, уникальных идентификаторов;

3.13.2 регулярное изменение паролей (через 90 дней или чаще);

3.13.3 соответствующую защиту после неудачных попыток входа в систему для предотвращения хакерских атак;

3.13.4 автоматическую деактивацию неиспользуемых учетных записей;

3.13.5 надежные пароли (не менее 8 символов с тремя из следующих категорий: (i) верхний регистр; (ii) нижний регистр; (iii) числа; (iv) не буквенно-цифровые. История паролей должна запрещать использование ранее используемых паролей в течение 12 месяцев;

3.13.6 доступ к системам поставщиков в зависимости от должности с усиленным контролем доступа для администратора; а также

3.13.7 регулярный контроль и аудит доступа пользователей.

Удаленный доступ

3.14 Поставщику запрещено предоставлять персоналу по контракту дистанционный доступ к информации с грифом «Совершенно секретно», если иное не согласовано с компанией BT в письменной форме. Если разрешен удаленный доступ, Поставщик обязан принять меры по обеспечению безопасности удаленного доступа в организации Поставщика, включая, но не ограничиваясь, удаленный доступ для пользователей с надежной двухфакторной аутентификацией. Если используется удаленный доступ через общедоступные сети для обеспечения поддержки, соединения должны быть зашифрованы согласно стандартам, изложенным в пункте 3.15.

Передача данных

3.15 Передача повседневных массивов данных должна осуществляться при помощи программы кодировки PGP или другой утвержденной в отрасли платформе.

Кодировка

3.16 Поставщик обязан обеспечить кодировку информации компании BT с грифом «Секретно» и «Совершенно секретно» при хранении и передаче в соответствии с Передовыми отраслевыми методами обеспечения безопасности, гарантирующими, что устаревшие стандарты не используются. Действующие стандарты кодировки, утвержденные компанией BT на Дату начала действия и соответствующие требованиям пункта 3.15 настоящего документа, изложены в Правилах классификации и обработки данных третьих сторон.

Корректировка программ

3.17 Поставщик обязан иметь и соблюдать формальную процедуру управления корректировками, которая, как минимум, должна гарантировать, что Поставщик:

3.17.1 выполняет корректировку в следующие периоды времени:

Тип корректировки	Описание	Время на выполнение
Критически важные корректировки	Корректировки для устранения уязвимости «нулевого дня»	В кратчайшие сроки, однако не более 14 дней с момента доступности корректирующего ПО
Важные корректировки	Уязвимость 7.0 - 8.9 по шкале Системы общей уязвимости (CVSS)	Не более 30 дней с момента доступности корректирующего ПО

Прочие корректировки	Все корректировки, не относящиеся к критически важным и важным	Не более 8 недель с момента доступности корректирующего ПО

3.17.2 следит за выходом корректирующего ПО у соответствующих поставщиков;

3.17.3 использует корректирующее ПО от поставщиков, которое подтверждается (i) цифровой подписью или (ii) хэшем поставщика (кроме хэша MD5), для пакета обновлений, чтобы корректирующее ПО можно было определить как исходящее от надежного разработчика открытого программного обеспечения;

3.17.4 перед использованием корректирующего ПО в производственной системе проверяет все корректирующее ПО на системах, точно отображающих конфигурацию целевых производственных систем; проверяет правильность работы исправленного сервиса после любой корректировки; а также

3.17.5 поддерживает и обновляет системы поставщика, чтобы использовать самое новое корректирующее ПО от разработчиков.

3.18 Если Поставщик не может применить корректирующее ПО к системе, он обязан уведомить об этом компанию BT в письменном виде. При получении такого уведомления компания BT обязана оценить риск для компании BT и информации компании BT, в случае продолжения использования системы Поставщиком. Компания BT может потребовать от Поставщика выполнить любые целесообразные действия (за счет Поставщика), чтобы устранить любые такие риски.

Управление уязвимостью

3.19 Поставщик обязан иметь и соблюдать формальную процедуру управления уязвимостью, которая, как минимум, должна гарантировать, что Поставщик:

3.19.1 предпринимает соответствующие меры (например, выполняет сканирование) для идентификации недостатков;

3.19.2 выполняет собственные испытания на возможность несанкционированного проникновения в систему с отчетностью;

3.19.3 реагирует на любое уведомление о недостатках и реализует планы действий по устранению выявленных недостатков в соответствии с пп. 3.22-3.27.

Испытания на возможность несанкционированного проникновения в систему

3.20 Поставщик обязан:

3.20.1 давать разрешение компании BT (или уполномоченному субподрядчику компании BT) выполнять приемлемые испытания на возможность несанкционированного проникновения в систему;

3.20.2 обеспечить компании BT доступ к существующим собственным отчетам по испытаниям на возможность несанкционированного проникновения в систему в рамках осуществляемых поставок.

Аудит и регистрация

3.21 Поставщик обязан иметь и соблюдать формальную процедуру аудита и регистрации событий, которая, как минимум, должна гарантировать, что Поставщик регистрирует (соответствующим образом) следующие события:

3.21.1 точки начала и окончания процесса регистрации событий;

3.21.2 изменения типа регистрируемых событий в соответствии с требованиями аудита (например, параметры запуска и любые изменения в них);

3.21.3 запуск и выключение системы Поставщика;

3.21.4 успешные входы с использованием логина и пароля;

3.21.5 неудачные попытки входа с использованием логина и пароля (например, неправильное имя пользователя или пароль);

3.21.6 все операции, выполняемые привилегированными пользователями (например, пользователи с расширенным доступом к системным утилитам или приложениям);

3.21.7 успешное и неуспешное расширение привилегий;

3.21.8 все случаи доступа Поставщика или персонала по контракту Поставщика или операции с информацией под грифом «Совершенно секретно»; а также

3.21.9 создание, изменение и удаление профилей пользователей.

3.22 По каждому факту проверки Поставщик обязан вести контрольный журнал с защитой от несанкционированного доступа, который позволяет восстановить такие события.

3.23 Принимая во внимание критичность компонента / данных, Поставщик обязан регулярно проверять и анализировать журналы аудита для выявления подозрительного или аномального поведения, и принимать соответствующие меры и/или поднимать тревогу.

3.24 Все факты тревоги должны быть задокументированы. Реакция на сигналы тревоги должна быть своевременной. Время реакции определяется критичностью сигнала тревоги.

3.25 Поставщик обязан хранить все учетные файлы 3 месяца (если их удаление не требуется в соответствии с положениями раздела **«Защита персональных данных»**), и делать копии или разрешать доступ к учетным файлам по запросу компании BT в формате, согласованном обеими Сторонами.

Управление угрозами и инцидентами информационной безопасности

3.26 Поставщик обязан иметь и соблюдать формальную процедуру управления инцидентами информационной безопасности. Процесс включает в себя выполнение определенных обязанностей для урегулирования соответствующего инцидента информационной безопасности. Любой информации, связанной с инцидентами информационной безопасности, присваивается гриф **«Секретно»**.

3.27 Поставщик обязан информировать Контактное лицо компании BT по безопасности и Коммерческое контактное лицо компании BT в течение приемлемого периода времени после того, как он узнает о любом соответствующем инциденте информационной безопасности, однако не позднее, чем через 12 (двенадцать) часов с момента выявления Поставщиком инцидента информационной безопасности.

3.28 Поставщик обязан немедленно принять надлежащие и своевременные корректирующие меры для устранения любых рисков и смягчения последствий, связанных с соответствующим инцидентом информационной безопасности, чтобы уменьшить тяжесть и продолжительность инцидента.

3.29 Поставщик обязан дать согласие на предоставление всей информации, обоснованно требуемой компанией BT в отношении соответствующего инцидента информационной безопасности, включая, но не ограничиваясь:

3.29.1 дата и время;

3.29.2 место;

3.29.3 тип инцидента;

3.29.4 последствия;

3.29.5 классификация затронутой информации;

3.29.6 статус;

3.29.7 итог (в том числе заключительные рекомендации и принятые меры).

3.30 Поставщик обязан обеспечить своевременное устранение выявленных опасностей для конфиденциальности, целостности или доступности информации компании BT в процессах или системах Поставщика.

3.31 Если в ходе инцидента информационной безопасности произошла утечка персональных данных, Поставщик обязан выполнить требования раздела **«Защита персональных данных»** в дополнение к положениям настоящих Требований безопасности. Во избежание сомнений Поставщик обязан также соблюдать положения раздела **«Защита персональных данных»** в отношении всех нарушений конфиденциальности персональных данных, независимо от того, является ли нарушение инцидентом информационной безопасности.

4 БЕЗОПАСНОСТЬ ПЕРСОНАЛА ПО КОНТРАКТУ

4.1 Доступ персоналу по контракту предоставляется только после успешного прохождения Тренинга по информационной безопасности компании BT, доступного по адресу https://workingwithbt.extra.bt.com или в системе подготовки компании BT, где персоналу по контракту присваиваются идентификационные номера компании BT. Тренинг по информационной безопасности компании BT следует проходить повторно, как описано на https://workingwithbt.extra.bt.com. Поставщик обязан вести учет обучения и предоставлять его для проверки по требованию компании BT.

4.2 Поставщик обязан обеспечить подписание всеми сотрудниками по контракту соглашения о конфиденциальности, которое включает те же обязательства, что предъявляются Поставщику в части 2 выше. Соглашение о конфиденциальности должно быть подписано до начала работы сотрудника по контракту в зданиях или системах компании BT либо до получения доступа к информации компании BT. Поставщик обязан хранить эти

Соглашения
о конфиденциальности и предоставлять для проверки по требованию компании BT.

4.3 Поставщик обязан устранять недостатки в политиках и процедурах безопасности Поставщика и компании посредством формальных процессов, в том числе применять дисциплинарные меры, лишающие лицо:

4.3.1 доступа к системам или информации компании BT;

4.3.2 возможности выполнять работы по обеспечению Поставок.

Кроме того, Поставщик обязан принять соответствующие меры, чтобы сотрудники по контракту, которым был закрыт доступ, не получили впоследствии доступ к системам и информации компании BT или возможность выполнять работы по обеспечению поставок.

4.4 Поставщик обязан в рамках законодательства содержать анонимную горячую линию, доступную для всего его персонала Поставщика для использования по контракту в случае получения распоряжений совершать действия, противоречащие настоящим Требованиям безопасности. Соответствующие отчеты должны отправляться Контактному лицу компании BT по безопасности.

4.5 По окончании работы персонала по контракту с Поставками, Поставщик обязан:

4.5.1 лишить персонал по контракту доступа к информации компании BT;

4.5.2 на выбор компании BT, любые физические активы или информация компании BT, находящаяся в распоряжении персонала по контракту, должна быть:

4.5.2.1 передана обратно соответствующей рабочей группе компании BT, или

4.5.2.2 уничтожена согласно требованиям новейшей редакции Правил классификации и обработки данных третьих сторон.

4.6 Если иное не согласовано в письменной форме с контактным лицом компании BT по безопасности, Поставщик обязан выполнить контролируемую процедуру выхода персонала по контракту, включающую письменный запрос Контактному лицу компании BT по безопасности на закрытие доступа к системам и информации компании BT и любых других доступов. Персонал по контракту следует уведомить о том, что его соглашение о конфиденциальности остается в силе и что информация компании BT, полученная в ходе работы с Поставками, не подлежит разглашению.

4.7 В рамках предоставления доступа Поставщик обязан вести и предоставлять учет всех сотрудников по контракту, которым нужен доступ или которые участвуют в обеспечении Поставок для компании BT, включая их имя, место работы, служебный адрес электронной почты, прямой служебный номер телефона и расширение (если применимо) и/или номер мобильного телефона, дату запроса идентификатора пользователя (UIN) (при наличии), дату назначения на работу с поставками для компании BT, дату завершения обязательного тренинга, дату прекращения работы с Поставками для компании BT и декларацию проверки перед поступлением на работу. Контактное лицо Поставщика по безопасности несет ответственность за предоставление допуска только персоналу по контракту.

4.8 Поставщик обязан внедрить политику и процессы, гарантирующие, что сотрудники по контракту не используют социальные сети для публикаций, любые заявления, комментарии, контент или изображения, которые:

4.8.1 можно обоснованно принять за точку зрения компании BT;

4.8.2 разглашают какую-либо информацию компании BT с грифом «Секретно» или «Совершенно секретно».

4.8.3 дискредитируют компанию BT и могут нанести ущерб бренду и репутации компании BT.

5 АУДИТ И ПЕРЕСМОТР СИСТЕМЫ БЕЗОПАСНОСТИ

5.1 Без исключения любого другого права аудита компании BT, для проверки соблюдения Поставщиком настоящих Требований безопасности, а также и, если применимо, положений раздела **«Защита персональной информации»**, компания BT или ее назначенные представители имеют право периодически контролировать соблюдение любого или всех требований политики, процессов и системы(м) Поставщика (при условии, что Поставщик защищает конфиденциальность любой информации, не связанной с Поставками для компании BT), по документам или на объекте Поставщика и любом соответствующем объекте(ах) Субподрядчика, участвующих в Поставках или выполнении Договора.

5.2 Поставщик обязан предоставить компании BT или ее назначенным представителям доступ и адекватную помощь при необходимости при проверке документации по безопасности или проверках на объектах. Перед плановой проверкой на объекте Поставщику будет вручено уведомление не позже чем за 30 рабочих дней, однако, во

избежание сомнений, в случае факта или предположения о нарушении конфиденциальности персональных данных или нарушения безопасности компания BT будет приступать к проверке без уведомления.

5.3 Поставщик обязан содействовать компании BT в реализации согласованных рекомендаций и осуществлении любых корректирующих действий, которые компания BT сочтет необходимыми по результатам проверки документации или проверки на объекте в течение 30 дней после получения уведомления о таких рекомендациях или корректирующих действиях в течение другого периода по согласованию между Сторонами за счет Поставщика.

5.4 Если компании BT необходимо провести независимый аудит Поставщика, при котором будет выявлено несоблюдение требований стандарта ISO/IEC 27001:2013 Поставщиком, Поставщик обязан за свой счет предпринять необходимые меры в целях обеспечения необходимого соответствия и полностью возместить любые расходы, понесенные компанией BT в связи с такой проверкой.

6 РАССЛЕДОВАНИЕ

6.1 В случае подозрения компании BT на:

6.1.1 нарушение конфиденциальности персональных данных;

6.1.2 нарушение безопасности;

6.1.3 нарушение настоящих требований безопасности

компания BT обязана сообщить Контактному лицу Поставщика по безопасности, а Поставщик соглашается за свой счет:

6.1.4 незамедлительно принять меры по расследованию предполагаемого нарушения и идентификации, предотвращения и принятия обоснованных мер для смягчения последствий любого такого нарушения; а также

6.1.5 выполнить восстановление или другие действия, необходимые для устранения нарушения.

6.1.6 предоставлять компании BT отчеты, которые компания BT обоснованно требует, по результатам расследования, а также о действиях, предпринятых для устранения или смягчения последствий нарушения,

В случае серьезного нарушения Поставщик обязан оказывать полное содействие компании BT в любом последующем расследовании или проверке компанией BT контролирующим органом и/или любым правоохранительным органом. Расследование или проверка должны включать (по обоснованному уведомлению компанией BT Поставщика) доступ к информации компании BT, хранящейся в помещениях или системах Поставщика

Поставщик обязан оказывать содействие компании BT в ходе любого расследования путем предоставления доступа и адекватной помощи по мере необходимости для расследования нарушения. Компания BT может потребовать ввести карантин Поставщика для оценки любого материального или нематериального актива, принадлежащего Поставщику, в целях содействия расследованию, а Поставщик не должен необоснованно воздерживаться или откладывать такой запрос.

ГЛАВА 4: СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ В СФЕРЕ БЕЗОПАСНОСТИ

7 СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И ПОЛИТИКА В СФЕРЕ БЕЗОПАСНОСТИ

7.1 Поставщик гарантирует и демонстрирует, что Системы Поставщика, Поставки, сопутствующие услуги, процессы и физические местоположения соответствуют и будут постоянно соответствовать стандарту ISO / IEC 27001:2013 и любой измененной или будущей версии данного стандарта. Соответствие должно быть обеспечено по собственному усмотрению компании BT путем:

7.1.1 аккредитации ISMS Поставщика Аккредитационной службой Великобритании (UKAS) или аналогичным международным органом сертификации, в котором содержание и положение о применимости подтверждены компанией BT; или

7.1.2 двухстороннего аудита и тестирования, указанного компанией BT.

7.2 Поставщик обязан получить действующий сертификат ISO/IEC 27001 в начале действия Договора и при последующих повторных сертификациях.

7.3 В случае изменения содержания сертификата или положения о применимости Поставщик обязан представить эти изменения на повторную аккредитацию с использованием процедуры управления изменениями (или, в случае отсутствия такой процедуры, посредством процесса внесения изменений). Поставщик обязан уведомить компанию BT в течение 2 рабочих дней о любом серьезном несоответствии, выявленном органом по аккредитации или Поставщиком.

8 ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ – ПОМЕЩЕНИЯ КОМПАНИИ BT

Соблюдение положений этого раздела требуется, если Поставщик осуществляет Поставки в помещениях компании BT.

8.1 Все сотрудники по контракту, работающие в помещениях компании BT, обязаны иметь и носить на видном месте предоставленную Поставщиком или компанией BT идентификационную карточку, подтверждающую авторизацию персонала по контракту (**«Карта авторизированного доступа»**). Карта авторизованного доступа должна содержать четкую и хорошо видимую фотографию владельца. Персоналу по контракту также может быть предоставлена электронная карта доступа и/или кратковременная карта для использования в соответствии с местными правилами оформления.

8.2 Если карта авторизированного доступа выдана сотруднику по контракту компанией BT, Поставщик обязан незамедлительно, однако не позже чем через 5 рабочих дней, уведомить компанию BT о том, что сотрудник по контракту больше не нуждается в доступе в помещения BT.

8.3 К доменам компании BT разрешается подключать напрямую (через порт LAN или по беспроводному соединению) только одобренные серверы сборок, компьютеры Webtop BT и надежные оконечные устройства. Поставщик не должен (и, при необходимости, обязан запрещать персоналу по контракту) без письменного разрешения Контактного лица компании BT по безопасности подключать к доменам компании BT какое-либо оборудование, не одобренное компанией BT. Контактное лицо компании BT по безопасности предоставляет письменное разрешение только в случае запуска процедуры разрешения на отклонение от политики безопасности компании BT. В любом случае Поставщик обязан не допустить, чтобы какое-либо личное оборудование персонала по контракту или других сотрудников (включая подрядчиков, временных сотрудников и работников от агентства), не использовалось для хранения, доступа или обработки любых данных компании BT.

8.4 Передача какой-либо информации компании BT или вынос какого-либо оборудования за пределы помещений компании BT или удаление/установка программного обеспечения в помещениях BT без предварительного разрешения компании BT запрещены.

8.5 Физическая защита и руководства по работе в помещениях BT подлежат соблюдению и должны включать, не ограничиваясь, сопровождение персонала по контракту и соблюдение надлежащих методов работы в зонах действия системы безопасности.

8.6 Если Поставщик уполномочен предоставлять персоналу по контракту безхостинговый доступ к зонам, находящимся в собственности компании BT, авторизованная компанией BT подписавшаяся сторона и персонал по контракту обязаны придерживаться положений руководства **«Доступ поставщика к объектам и зданиям компании BT»** https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm. Дополнительно, авторизованная не компанией BT подписавшаяся сторона и персонал по контракту обязаны иметь декларацию проверки перед поступлением на работу не ниже уровня L2 https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ – ПОМЕЩЕНИЯ ПОСТАВЩИКА

Соблюдение положений этого раздела требуется, если Поставщик осуществляет Поставки в помещениях Поставщика. (например, Поставщик или третьи стороны Поставщика)

9.1 Доступ в помещения, не принадлежащие компании BT (объекты, здания или внутренние зоны), где осуществляются Поставки или хранится/обрабатывается информация компании BT, разрешается только по Карте доступа авторизованного Поставщика. Эта карта используется как удостоверение личности в соответствующих помещениях в любое время, поэтому фотография владельца на карте должна быть четкой и хорошо видимой. Физическим лицам также может быть выдана электронная карта доступа для доступа к соответствующим помещениям или код доступа через клавиатуру. Поставщик обязан внедрить процессы для: авторизации, разброса графика изменений кода (которые должны происходить не реже одного раза в месяц); и изменения кода для конкретных случаев.

9.2 Поставщик обязан обеспечить авторизацию доступа к помещениям, не принадлежащим компании BT, в которых осуществляются Поставки или где хранится или обрабатывается информация компании BT, и соблюдать процессы

и процедуры безопасности в отношении контроля и мониторинга персонала по контракту, посетителей и других лиц, в том числе третьих лиц, имеющих физический доступ к этим областям (например, техники экологического контроля, установщики сигнализации, уборщики).

9.3 По требованию компании BT Поставщик обязан обеспечить безопасную изоляцию персонала по контракту от всех других сотрудников Поставщика. Кроме того, Поставщик обязан убедиться в том, что системы и инфраструктура, используемые для обеспечения Поставки, включены в специальную логическую сеть. Эта сеть должна состоять только из систем, предназначенных для защищенной передачи и обработки данных.

9.4 Безопасные зоны в помещениях Поставщика (например, в комнатах для сетевых коммуникаций) должны быть разделены и защищены соответствующими элементами контроля входа, чтобы гарантировать, что доступ в безопасные зоны был разрешен только авторизованному персоналу по контракту. Порядок доступа в эти зоны персоналом по контракту подлежит проверке не реже одного раза в месяц, а оценка повторной авторизации прав доступа – не реже одного раза в год.

Поставщик обязан предоставлять подтверждение оценки риска по запросу компании BT. Если оценка по запросу компании BT не предоставляется, по своему усмотрению, компания BT или ее представитель должен провести оценку риска окружающей среды, используемой для поставки Сервиса (например, центров обработки данных, зон обработки данных, компьютерных залов) до начала Поставки. Кроме того, компания BT должна быть проинформирована о предстоящих работах в любых помещениях, которые могут нести угрозу безопасности информации компании BT.

9.5 Системы видеонаблюдения CCTV и связанная с ними среда записи должны использоваться Поставщиком в ответ на инциденты информационной безопасности, в качестве средства наблюдения за безопасностью, сдерживающего средства, средства для возможного задержания лиц, пойманных при совершении преступления. Если изображения с системы CCTV записываются (на пленку или на цифровой носитель), они подлежат хранению не менее 20 дней. Этот срок может увеличиться в следующих ситуациях:

9.5.1 если видео с системы CCTV требуется для расследования инцидента или уголовного преступления;

9.5.2 если это необходимое требование для соблюдения законодательства.

9.5.3 Записи с камер системы CCTV подлежат хранению в запертом помещении, ключ от которого хранится в надежном месте, исключающем доступ посторонних лиц. Доступ в помещение разрешается только авторизованным лицам.

9.6 Все камеры системы видеонаблюдения должны быть расположены таким образом, чтобы исключить возможность модификации или снятия, а также возможность «случайного» просмотра любых экранов видеонаблюдения и в соответствии с указаниями по использованию системы CCTV, которые можно найти на

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 Все зоны помещений Поставщика, используемые для предоставления Услуг и обеспечения Поставок, должны быть проверены Поставщиком на наличие рисков и угроз не реже одного раза в месяц. Поставщик обязан учесть и внедрить необходимые меры физической безопасности с учетом следующего:

9.7.1 локальные угрозы, включая, но не ограничиваясь, потенциальные угрозы от близлежащих промышленных объектов и близость хранилищ опасных материалов; а также

9.7.2 стихийные бедствия, включая, но не ограничиваясь, наводнениями, оползнями или экстремальными погодными условиями.

9.8 Силовые и телекоммуникационные кабели в помещениях Поставщика, несущие данные или поддерживающие информационные сервисы, или радио/спутниковые сервисы, используемые при обеспечении Поставки, должны быть защищены Поставщиком на уровне, предотвращающем прерывание деловых операций. Меры физической защиты, соизмеримые в зависимости от важности защищаемых ими операций, должны быть внедрены следующим образом:

9.8.1 дороги, экранировка кабелей, люки или тротуарные ящики, где есть критически важные кабели, должны быть защищены;

9.8.2 доступ к кабельным шахтам или шкафам для кабельной разводки в рабочих помещениях должен быть ограничен путем использования электронных считываемых устройств контроля доступа или эффективной системы управления ключами доступа;

9.8.3 компьютерные коммуникации и коммуникационное оборудование в вычислительных центрах должны быть защищены физически и от воздействия окружающей среды; а также

9.8.4 средства и коммуникации радио и спутниковой связи должны быть защищены надлежащим образом.

9.9 Если иное не согласовано между Поставщиком и Контактным лицом Компании BT по безопасности, Компания BT обязана требовать, чтобы Поставщик применял меры по защите с участием людей в дополнение к электронным и физическим средствам безопасности в помещениях Поставщика, если:

9.9.1 местоположение имеет операционное значение (например, контактные центры, центры обработки данных, ключевые сетевые сайты и т. д.),

9.9.2 обработанная информация компании BT может негативно повлиять на бренд и репутацию компании BT;

9.9.3 обрабатывается большой объем информации компании BT (например, при аутсорсинге бизнес-процессов)

9.9.4 Требования клиента по Договору

9.9.5 на объекте присутствует особый риск/угроза

9.9.6 Поставщик располагает особо ценной информацией.

9.10 Для защиты оборудования компании BT (например, серверов или коммутаторов компании BT) в помещениях Поставщика от экологических угроз или опасностей, а также от несанкционированного доступа, оборудование компании BT должно располагаться на защищенной территории и отделено от оборудования, используемого для любых систем организаций, не относящихся к компании BT. Уровень разделения должен гарантировать, что безопасность оборудования компании BT не может быть нарушена преднамеренно или случайно в результате доступа организаций, не относящихся к компании BT, и может представлять собой, например, защитные перегородки, запираемые шкафы или металлические клетки.

9.11 Поставщик обязан внедрить необходимые меры физической безопасности с учетом следующего:

9.11.1 противопожарные меры, включая, но не ограничиваясь, аварийные средства, оборудование для обнаружения и подавления;

9.11.2 климатические условия (температура, влажность и статическое электричество) и системы управления, мониторинга и реагирования на экстремальные условия (например, автоматический останов, аварийные сигналы);

9.11.3 контролирующее оборудование, включая, но не ограничиваясь, кондиционирование воздуха и обнаружение утечки воды;

9.11.4 расположение резервуаров для воды, труб и т. д. внутри помещений;

9.11.5 контролируемый доступ – по возможности доступ персонала к системам должен быть контролируемым;

9.11.6 надзор за персоналом по контракту, обычно не связанным с управлением или доступом к системам компании BT.

9.12 Защитные ограждения по периметру (стены, ограждения, входные ворота с доступом по карте или стойка регистрации с дежурным сотрудником) должны использоваться для защиты зон, содержащих закрытую информацию компании BT или информацию клиента компании BT (включая персональные данные) и связанные с ними объекты обработки.

9.13 Точки доступа, например, зоны доставки и погрузки, а также другие точки, через посторонние лица могут попасть в помещение, должны контролироваться и, по возможности, изолироваться от средств обработки информации, чтобы избежать несанкционированного доступа или умышленных атак.

9.14 Поставщик обязан предусмотреть, чтобы физический доступ в зоны с доступом к информации компании BT или информации клиента компании BT (включая персональные данные), проводился по смарт-или бесконтактным картам (или эквивалентным системам безопасности). Кроме того, Поставщик обязан как минимум проводить ежемесячные внутренние аудиты для обеспечения соблюдения этих положений.

9.15 Поставщик обязан исключить возможность фотографирования и/или снимки экрана с любой информацией компании BT или клиента компании BT (включая персональные данные). В исключительных случаях, когда необходимость фотографирования может возникнуть в деловых целях, разрешение на временное освобождение от этого положения должно быть получено в письменной форме от контактного лица компании BT по безопасности.

9.16 Поставщик должен соблюдать политику чистого стола и экрана для защиты информации компании BT.

10 ХОСТИНГОВОЕ ОБОРУДОВАНИЕ

Соблюдение этого раздела требуется, если Поставщик предоставляет среду для размещения оборудования компании BT или клиента BT.

10.1 При предоставлении защищенной зоны в своих помещениях для размещения оборудования BT или клиента BT (**«Объект поставщика»**) Поставщик обязан:

10.1.1 обеспечить доступ сотрудников по контракту на объект Поставщика по идентификационной карте или электронной карте доступа. Эта карта используется как удостоверение личности на объектах Поставщика в любое время, поэтому фотография владельца на карте должна быть четкой и хорошо видимой.

10.1.2 внедрить процедуры устранения угроз безопасности оборудованию компании BT, клиента BT или третьей стороны, действующей от имени компании BT, чтобы защитить информацию клиента компании BT и компании BT на объекте поставщика; а также

10.1.3 использовать системы видеонаблюдения CCTV и связанную с ними среду записи на объекте Поставщика в ответ на инциденты информационной безопасности, в качестве средства наблюдения за безопасностью, сдерживающего средства, средства для возможного задержания лиц, пойманных при совершении преступления. Поставщик обязан обеспечить запись видео с системы CCTV и хранить их не менее 20 дней на случай расследования, и

10.1.4 предоставить компании BT план выделенного пространства в защищенной зоне объекта Поставщика; а также

10.1.5 обеспечить, чтобы шкафы клиента BT и компании BT на объекте поставщика были заперты, а доступ к ним имели только авторизованные сотрудники компании BT, утвержденные представители компании BT и соответствующий персонал по контракту; а также

10.1.6 внедрить и соблюдать надежную процедуру управления ключами на объекте Поставщика; а также

10.1.7 регулярно проверять прилегающие к объекту Поставщика территории на наличие рисков и угроз; а также

10.1.8 документировать и соблюдать рабочие процедуры (на языке страны происхождения работы компании BT) для соблюдения требований безопасности, подробно изложенных в параграфе 10, и по запросу предоставлять компании BT доступ к такой документации.

10.2 Компания BT обязана предоставить Поставщику:

10.2.1 учет материальных активов компании BT и/или клиентов BT на объекте Поставщика;

10.2.2 подробные данные сотрудников компании BT, субподрядчиков и агентов, которым необходим доступ к объекту Поставщика (на постоянной основе).

11 РАЗРАБОТКА СЕРВИСОВ

Соблюдение этого раздела требуется, если Поставщик разрабатывает услуги в рамках Поставки для компании BT и/или клиентов компании BT. К таким относятся готовые к использованию программы и производственные компоненты для обеспечения Поставок.

11.1 Поставщик обязан внедрить согласованные меры по защите всех поставляемых компонентов, которые составляют Поставки и/или Сервисы для обеспечения конфиденциальности, доступности и целостности Поставок, в том числе путем:

11.1.1 ведения соответствующей документации (на языке страны происхождения работы компании BT) в отношении защиты безопасности, и обеспечения их соответствия передовым отраслевым практикам;

11.1.2 сведения к минимуму возможности получить доступ к системам, информации, сетям и Поставкам компании неавторизованными лицами (например, хакерами);

11.1.3 минимизации риска неправильного использования систем, информации, сетей и Сервисов компании BT, которые потенциально могут привести к потере дохода или сервиса.

11.2 По запросу Поставщик обязан продемонстрировать §, что любое поставляемое программное обеспечение или аппаратная сборка (как запатентованная, так и готовая), поставленная в компании BT, соответствует соглашению с компанией BT. Поставщик обязан поддерживать целостность сборки, включая обновления, а также готовых операционных систем и приложений.

11.3 Поставщик обязан гарантировать, что разработка систем для компании BT, или сборка и обслуживание аппаратного обеспечения, принадлежащего компании BT, соответствует требованиям IT-безопасности компании BT, если она предоставлена операционной группой компании BT или разработана с использованием передовых отраслевых практик.

11.4 Поставщик должен обеспечить, чтобы системы и процессы, используемые для испытаний и разработки, были отделены от производственных систем. Для продвижения любого кода в производственную среду должен применяться процесс управления изменениями. Предоставленные компанией BT тестовые данные должны быть

удалены после периода, определенного владельцем данных компании BT. Использовать для разработки или тестирования рабочие и производственные данные запрещено.

11.5 Все критические для безопасности уязвимые элементы, обнаруженные при тестировании безопасности и классифицированные как средний или высокий риск, должны быть исправлены до выпуска ПО. Любые недостатки безопасности в Сервисах, выявленные компанией BT или Поставщиком, должны быть устранены за счет Поставщика в обоснованно требуемые компанией BT сроки.

11.6 Перед выпуском объекты Поставки должны проходить независимые испытания на возможность несанкционированного проникновения в систему, по заказу и за счет Поставщика не реже одного раза в год или после существенных изменений или инцидентов.

11.7 Объекты Поставки, разработанные для использования компанией BT или ее клиентами, должны разрабатываться с использованием задокументированного признанного отраслевого стандарта Безопасного жизненного цикла разработки (SDLC), чтобы минимизировать риск ослабления безопасности в производственной среде и/или для клиентов. Процедура SDLC должна включать следующие входы с осязаемыми результатами каждой проверки и быть доступной для проверки компанией BT в рамках аудита, описанного в параграфе 5 Части 3 настоящих требований безопасности:

11.7.1 проверка безопасности деловых требований;

11.7.2 проверка безопасности дизайна;

11.7.3 ручная и/или автоматическая проверка кода безопасности;

11.7.4 общая проверка безопасности продукта до развертывания (с имитацией атак) согласно утвержденному плану для конкретного проекта на основании отчетов, полученных в результате проверок безопасности деловых требований, дизайна и кода.

Дальнейшие рекомендации можно найти в Стандартах отраслевых руководств третьих сторон в разделе «Защитная кодировка»:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 ДЕПОНИРОВАНИЕ

Содержится в основном Договоре.

13 ДОСТУП К СИСТЕМАМ КОМПАНИИ BT

Соблюдение этого раздела требуется, если для выполнения Поставок персоналу по контракту требуется доступ к системам компании BT.

13.1 В случае необходимости для обеспечения Поставки компания BT по собственному усмотрению может предоставить ограниченный доступ.

13.2 Поставщик обязан придерживаться в отношении доступа всех действующих политик, стандартов и инструкций компании BT, и требовать от всех сотрудников по контракту:

13.2.1 предоставлять индивидуальную идентификацию пользователя, пароли, PIN-коды, токены и доступ к конференц-связи, и допускать их совместного использования с другими лицами. Детали должны храниться надежно и отдельно от устройства, для доступа к которому они предназначены. В случае разглашения пароля другому лицу пароль подлежит немедленной смене;

13.2.2 по обоснованному запросу предоставлять компании BT отчеты, которые компания BT должна обоснованно требовать в отношении доступа персонала по контракту к системам компании BT;

13.2.3 междоменная связь с системами BT запрещена, если иное специально не одобрено и не санкционировано Контактным лицом компании BT по безопасности;

13.2.4 использовать все обоснованные усилия для недопущения попадания вирусов или вредоносных кодов (как их обычно понимают в компьютерной индустрии), чтобы свести к минимуму риск порчи систем или информации компании BT любыми средствами; а также

13.2.5 прилагать обоснованные усилия, чтобы файлы, содержащие информацию, данные или носители, не имеющие отношения к Поставке, не хранились на оборудовании, серверах, портативных и настольных компьютерах, в централизованных хранилищах или системах компании BT.

13.2.6 в случае предоставления доступа Поставщику Интернет- или интранет-доступа к сетям компании BT, обеспечить доступ персонала по контракту только в рамках обеспечения Поставки и что блокировку

неприемлемых или опасных веб-сайтов. Поставщик несет ответственность за доведение до персонала по контракту руководства по злоупотреблению электронной почтой и сетью Интернет не реже одного раза в год. Руководство должно

13.2.6.1 запрещать пользователю:

(i) переходить к любому контенту оскорбительного, сексуального, сексистского, расистского или политически оскорбительного характера;
(ii) выполнять любые действия, которые могут испортить репутацию компании BT или отдельных лиц;
(iii) вести частные дела;
(iv) (d) нарушать любые авторские права или;
(v) обходить или взламывать брандмауэр компании BT или другие механизмы безопасности;

13.2.6.2 Персоналу по контракту запрещено дополнять веб-сайты или публиковать онлайн-заявления, которые можно было бы принять за мнения компании BT.

13.3 Поставщик обязан регулярно проводить проверки защищенности этой функции Доступом. Копии документации по проверкам должны быть доступны для проверки компанией BT в рамках аудита, описанного в пункте 5.1:

13.4 Поставщик обязан немедленно, однако не позже чем 5 рабочих дней, уведомить компанию BT, если сотрудник, в том числе подрядчик, временный сотрудник и работник агентства, больше не нуждается в доступе к системам компании BT, например, при увольнении или перемещении на другую должность.

14 ДОСТУП К ИНФОРМАЦИИ КОМПАНИИ BT В СИСТЕМАХ ПОСТАВЩИКА

Соблюдение этого раздела требуется, если информация компании BT хранится или обрабатывается в системах Поставщика.

14.1 Если персоналу по контракту предоставляется доступ к системам Поставщика в целях обеспечения Поставки и / или Сервиса, Поставщик должен отчитываться за такой доступ (включая, помимо прочего, использование уникальных учетных записей пользователей, управление паролями и четкую проверку / отслеживание входа всех действий персонала по контракту.

14.2 Поставщик обязан внедрить и использовать системы, которые обнаруживают и фиксируют любые попытки повреждения, модификации или несанкционированного доступа к информации компании BT в системах Поставщика. Это, например, процессы регистрации и аудита системы, идентификаторы и IP-адреса и т. д.

14.3 Поставщик обязан внедрить и использовать элементы управления для обнаружения и защиты от вредоносного программного обеспечения, вирусов и вредоносных кодов в системах Поставщика и обеспечивать выполнение соответствующих процедур информирования пользователей.

14.4 Поставщик обязан обеспечивать обнаружение и удаление любого несанкционированного программного обеспечения из систем Поставщика, в которых хранится, обрабатывается или предоставляется доступ к информации компании BT не реже одного раза в месяц.

14.5 Поставщик обязан обеспечить надежную защиту и управление доступом к портам диагностики и управления, а также диагностическим инструментам.

14.6 Поставщик обязан ограничивать доступ к инструментам аудита Поставщика для персонала по контракту и обеспечивать возможность контроля его использования.

14.7 Поставщик обязан обеспечить проверку кода и испытания на возможность несанкционированного проникновения в систему относительно всего собственного программного обеспечения (любое программное обеспечение), используемого для обработки информации компании BT, независимой группой, в которую не должны входить разработчики программного обеспечения.

14.8 Любые серверы, используемые для обеспечения Поставки, не должны развертываться в ненадежных сетях (за пределами вашего периметра безопасности, за пределами вашего административного контроля, например, с доступом в Интернет) без соответствующих средств безопасности.

14.9 Поставщик обязан обеспечить контроль и формальную процедуру внесения изменений в отношении изменений в отдельных системах Поставщика, где хранится и обрабатывается информация BT и/или которые используются для обеспечения Поставок.

14.10 Поставщик обязан обеспечить синхронизацию всех системных часов и времени при помощи новейшей версии NTP или аналогичной технологии синхронизации времени.

14.11 В случае предоставления поставщиком систем, разрешающих онлайн-доступ для клиентов компании BT:

14.11.1 Онлайн-учетные данные для клиентов компании BT должны содержать как минимум:

14.11.1.1 идентификатор пользователя;

14.11.1.2 онлайн-пароль;

14.11.1.3 три вопроса аутентификации и ответы на них;

14.11.1.4 альтернативный метод контакта для аутентификации.

14.11.2 Клиент компании BT должен иметь возможность выбрать уникальный идентификатор пользователя для своей онлайн-учетной записи, онлайн-пароль не должен содержать уникальный идентификатор пользователя.

14.11.3 Онлайн-пароль клиента компании BT должен быть длиной не менее 8 символов и содержать не менее 1 символа из 3 следующих наборов; (i) десятичное число (0-9), (ii) буква в верхнем регистре (A-Z), (iii) буква в нижнем регистре (a-z) (iv) не буквенно-цифровой знак

14.11.4 Чтобы изменить онлайн-пароль, клиент компании BT должен ввести свой текущий пароль, а затем дважды ввести новый пароль.

14.11.5 Если клиента компании BT забыл идентификатор пользователя или пароль, система Поставщика должна отправить электронное письмо на зарегистрированный адрес электронной почты клиента компании BT со ссылкой на сброс идентификатора пользователя или пароля после внесения в онлайн-форму следующих данных:

14.11.5.1 номер MSISDN или номер городского телефона

14.11.5.2 онлайн-пароль

14.11.5.3 идентификатор пользователя компании BT

14.11.6 Ссылка на запрос сброса пароля должна иметь срок действия не более 30 минут. По истечении срока действия ссылки необходимо делать новый запрос на сброс онлайн-пароля.

14.11.7 После успешного сброса пароля клиент компании BT не должен иметь возможности использовать предыдущий пароль.

14.11.8 При восстановлении учетных данных пользователя клиента BT, в случае утери идентификатора пользователя и онлайн-пароля система должна отправить электронное письмо на зарегистрированный адрес электронной почты, содержащее идентификатор пользователя и ссылку на запрос сброса пароля после успешного ввода имени и фамилии, номера телефона и адреса электронной почты клиента BT.

14.11.9 Дополнительные уровни аутентификации клиентов могут потребоваться в зависимости от важности информации или функции, к которым необходим доступ.

15 ХОСТИНГ ИНФОРМАЦИИ КОМПАНИИ BT ПОСТАВЩИКОМ

Соблюдение этого раздела требуется, если Поставщик хранит информацию компании BT с грифом «Секретно» или «Совершенно секретно» в облачной среде или на серверах Поставщика или Субподрядчика.

15.1 Поставщик обязан обеспечить в рамках Поставок, чтобы среды, в которых размещается информация компании BT, соответствовали Требованиям к хранению данных третьих сторон, доступных по адресу:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 СЕТЕВАЯ БЕЗОПАСНОСТЬ

Соблюдение этого раздела требуется, если Поставщик развертывает, развивает или поддерживает сети компании BT или Сетевые активы.

16.1 Поставщик обязан в рамках Поставки применять согласованные меры безопасности в отношении всех поставленных компонентов, чтобы гарантировать конфиденциальность, доступность и целостность сетей и / или сетевых активов 21CN компании BT. Поставщик обязан обеспечить компанию полным комплектом документации по Сетевой безопасности в рамках Поставки и:

16.1.1 обеспечить соответствие Сетевой безопасности, за которую отвечает Поставщик, всем правовым и нормативным требованиям; а также

16.1.2 прилагать максимум усилий для предотвращения доступа неавторизованных лиц (например, хакеров) к элементам управления сетью и другим элементам, доступ к которым осуществляется через сети компании BT и/или 21CN; а также

16.1.3 прилагать максимум усилий для снижения риска злоупотребления сетями компании BT и / или 21CN лицами, которым разрешен доступ к ней, что может привести к потере дохода или услуги; а также

16.1.4 прилагать максимум усилий для своевременного выявления потенциальных нарушений безопасности для ускорения их устранения, а также идентификацию нарушителей и выявление способа получения ими доступа; а также

16.1.5 минимизировать риск неправильной конфигурации сетей компании BT, например, путем предоставления минимальных прав при предоставлении доступа персоналу по контракту.

16.2 Поставщик обязан предпринять все обоснованные меры для обеспечения безопасности всех интерфейсов в системе Поставки и/или Сервисах и не должен предполагать, что поставляемые компоненты работают в безопасной среде.

16.3 Поставщик обязан предоставить Контактному лицу компании BT по безопасности имена, адреса (и другие данные по требованию компании BT) всех сотрудников по контракту, которые периодически будут непосредственно участвовать в развертывании, обслуживании и / или управлении Поставками до начала этих работ.

16.4 В рамках мероприятий по поддержке на территории Великобритании Поставщик обязан создать и использовать квалифицированную группу обеспечения безопасности, состоящую как минимум из одного гражданина Великобритании, который будет доступен для связи с Контактным лицом компании BT по безопасности (или его заместителем). Группа должна присутствовать на собраниях, периодически организуемых Контактным лицом компании BT по безопасности.

16.5 Поставщик обязан предоставить Контактному лицу компании BT по безопасности перечень (обновляемый по мере необходимости) всех активных компонентов, входящих в состав Поставки и/или Сервисов и их соответствующие источники.

16.6 Поставщик обязан предоставить подробные данные своих сотрудников, которые будут поддерживать связь с Группой реагирования на компьютерные чрезвычайные происшествия (CERT) компании BT в отношении недостатков, выявленных компанией BT и Поставщиком в системе Поставки и/или Сервисах. Поставщик обязан предоставлять компании BT своевременную информацию о недостатках и выполнять (за счет Поставщика) обоснованные требования в отношении недостатков, о которых Контактное лицо компании BT по безопасности может быть периодически уведомлено. Поставщик обязан заблаговременно уведомлять компанию BT о любых недостатках, чтобы компания BT успевала принять компенсирующие меры до выпуска Поставщиком политики устранения недостатков.

16.7 Поставщик обязан периодически предоставлять Постоянному Контактному лицу компании BT по безопасности и его представителям полный и неограниченный доступ к любым помещениям, где разрабатываются, производятся или создаются Поставки для проведения проверок и/или оценок соответствия безопасности. Поставщик (и его персонал по контракту) обязан оказывать содействие компании BT в таких проверках.

16.8 Поставщик обязан за свой счет организовывать и выполнять независимую проверку компонентов безопасности, входящих в состав Поставки, по обоснованному требованию компании BT.

16.9 В отношении информации с грифом **«СОВЕРШЕННО СЕКРЕТНО»**, полученной от компании BT, или очевидно секретной информации, Поставщик обязан:

16.9.1 предоставлять доступ к просмотру и обработке таких данных только сотрудникам по контракту, специально авторизованным компанией BT, и вести учет доступа;

16.9.2 обеспечивать максимальную безопасность данных при обработке, использовании и хранении, зашифровывать данные перед отправкой на хранение с использованием PGP или WinZip 9. Обеспечивать максимальную защиту от взлома (наиболее эффективный алгоритм шифрования / надежный пароль), а также эффективные меры по обнаружению взлома/попыток взлома.

16.9.3 обеспечить защиту информации при передаче путем шифрования с помощью защищенной электронной почты, PGP или WinZip 9; а также

16.9.4 не допускать передачи информации без письменного разрешения компании BT за пределы Европейской экономической зоны.

16.10 Поставщик обязан немедленно, однако не позже чем 7 рабочих дней, предоставить Контактному лицу компании BT по безопасности исчерпывающую информацию о любых функциях и/или характеристиках в любом Приложении (или запланированных в схеме для любых Приложений), которые:

16.10.1 известны Поставщику; или

16.10.2 по обоснованному мнению Контактного лица компании BT по безопасности с уведомлением Поставщика, предназначены для законного перехвата или любого другого перехвата телекоммуникационного трафика, или могут быть использованы для его законного перехвата. Подробности должны включать в себя всю обоснованно необходимую информацию, позволяющую Контактному лицу по безопасности BT полностью понять суть, состав и объем таких функций и / или функциональных возможностей.

16.11 Чтобы поддерживать доступ к сетям/системами компании BT, Поставщик должен немедленно уведомлять компанию BT о любых изменениях своего метода доступа через брандмауэры, включая перевод сетевых адресов.

16.12 Поставщику запрещается использовать инструменты сетевого мониторинга, которые могут просматривать информацию о приложении.

16.13 Поставщик обязан гарантировать, что функция IPv6 в составе операционных систем, отключена на узловых компьютерах (например, устройствах конечных пользователях или серверах), которые подключаются к сети компании BT, а домены должны быть отключены если в них нет потребности.

16.14 Поставщик обязан соблюдать и обеспечивать соответствие Поставок или Сервисов политикам компании BT (если применимо) и Требованиям безопасности. Любое несоответствие подлежит согласованию при подписании Договора или при помощи процесса контроля изменений (или аналога).

16.15 Поставщик обязан удостовериться, что все сотрудники по контракту прошли предварительные проверки перед приемом на работу, соответствующие уровню доступа, как указано в https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Поставщик, развертывающий, развивающий или поддерживающий сети BT или сетевые активы, обязан обеспечить не менее двух проверок перед приемом на работу для всех сотрудников по контракту. Проверка L3 необходима для должностей, указанных Контактным лицом компании BT по безопасности. Если Поставщик не имеет возможности непосредственно обеспечивать доступ персоналу по контракту в рамках проверок L3, компания БТ окажет помощь в получении разрешения за счет Поставщика.

16.16 Поставщик обязан поддерживать аппаратное и программное обеспечение в соответствии со спецификациями производителей.

16.17 Поставщику запрещено использовать съемные носители (диски, USB-накопители и т. д.), предназначенные для поддержки и обслуживания, в любых других целях.

17 СЕТЕВАЯ БЕЗОПАСНОСТЬ ПОСТАВЩИКА

Соблюдение положений этого раздела требуется, если для обеспечения поставок будет использоваться сеть поставщика (LAN, WAN, интернет, беспроводные и радиосети).

17.1 Поставщик обязан в рамках Поставки/Сервиса применять меры безопасности в своих сетях, чтобы гарантировать конфиденциальность, доступность и целостность информации компании BT. В рамках данных мер Поставщик обязан:

17.1.1 обеспечить соответствие всем правовым и нормативным требованиям; а также

17.1.2 прилагать максимум усилий для предотвращения доступа неавторизованных лиц (например, хакеров) к сети(ям) Поставщика;

17.1.3 прилагать максимум усилий для снижения риска злоупотребления сетями Поставщика лицами, которым разрешен доступ к ней, что может привести к потере дохода или услуги; а также

17.1.4 прилагать максимум усилий для своевременного выявления потенциальных нарушений безопасности и быстро устранять их, а также идентифицировать нарушителей и выявлять способы получения ими доступа; а также

17.2 Принять соответствующие меры для обеспечения безопасности компонентов, включая, но не ограничиваясь:

17.2.1 использовать эффективную **«защиту в глубину»**

17.2.2 использовать средства предотвращения умышленных атак;

17.2.3 использовать брандмауэры, маршрутизаторы, коммутаторы;

17.2.4 обеспечивать безопасность связи между устройствами и станциями управления;

17.2.5 обеспечить надлежащую безопасную связь между устройствами, включая шифрование для доступа не администраторов консоли;

17.2.6 обеспечить надежную архитектуру, с несколькими уровнями и зонами и с эффективным надежным управлением идентификацией и конфигурацией операционной системы, которое должно быть надлежащим образом проверено и документировано;

17.2.7 отключать (если возможно) службы, приложения и порты, которые не будут использоваться.

17.2.8 отключать или удалять учетные записи гостей.

17.2.9 устанавливать новейшие обновления систем безопасности в сети (ях) Поставщика и системе (ах) как можно скорее после тестирования. Любые исключения должны быть сообщены компании BT, где исключения будут подвергнуты оценке рисков. Компания BT оставляет за собой право обязать Поставщика устанавливать обновления системы безопасности после оценки риска;

17.2.10 исключить доверительные отношения между доменами;

17.2.11 использовать передовой принцип **«минимальных прав»** при предоставлении доступа для выполнения работы;

17.2.12 обеспечивать надлежащие меры для устранения атак, вызывающих отказ в обслуживании законных пользователей;

17.2.13 обеспечивать надлежащие меры по обнаружению и/или защите от вторжений;

17.2.14 проводить мониторинг всех применимых разработчиков и других соответствующих источников информации для предупреждения о недостатках;

17.2.15 проводить, если применимо, мониторинг целостности данных для обнаружения любых дополнений, модификаций или удалений критических системных файлов или данных; а также

17.2.16 перед началом использования сетевых компонентов изменить все пароли, установленные по умолчанию или поставщиками.

18 ОБЛАЧНАЯ БЕЗОПАСНОСТЬ

Соблюдение положений этого раздела требуется, если Поставщик предоставляет компании BT услуги, связанные с облачным хранилищем.

18.1 Поставщик обязан:

соблюдать требования новейшей версии Матрицы контроля облачных хранилищ Альянса безопасности облачных вычислений (CCM), а также Требований компании BT к безопасности при внешнем хостинге, доступные по адресу: https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm Соглашения об уровнях обслуживания сети и инфраструктуры (внутреннем или внешнем) должны четко документировать элементы контроля безопасности, мощности и уровни обслуживания, а также требования организации или клиента.

18.2 Поставщик обязан внедрить и соблюдать согласованные меры безопасности в отношении всех поставленных компонентов, чтобы гарантировать конфиденциальность, доступность, качество и целостность Поставок путем минимизации возможности неавторизованных лиц (например, других пользователей облачных сервисов) получать доступ к информации и Поставкам компании BT.

19 КОНТАКТНЫЙ ЦЕНТР

Соблюдение положений этого раздела требуется, если Поставщик предоставляет контактный центр для BT.

19.1 Поставщик в рамках Поставки обязан обеспечить соответствие сред, в которых хранится, обрабатывается или просматривается информация компании BT, новейшей версии Стандарта по организации контактного центра третьих сторон, доступного по адресу:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

ГЛАВА 5: ОПРЕДЕЛЕНИЯ

В настоящем документе применяются следующие определения. В противном случае в настоящем документе будут применяться положения Договора, а все слова и выражения, используемые в настоящем документе, должны иметь то же значение, что и в Договоре.

«Доступ» – обработка, обращение и хранение информации компании BT одним или несколькими из следующих способов:

- подключение к системам компании BT

- предоставление на бумажном носителе или в неэлектронном виде
- информация компании BT в системах Поставщика
- с использованием мобильных устройств

и/или доступ в помещения компании BT с целью обеспечения Поставок, за исключением доставки аппаратного обеспечения и посещения собраний.

«Авторизация» – одобрение компанией BT доступа в составе системного межсетевого соединения компании BT, или выдача письменного разрешения на основании «Договора о безопасности компании BT». Термин **«авторизация»** должен толковаться соответствующим образом. Предоставляемый уровень доступа должен ограничиваться только тем, который требуется для обеспечения Поставки.

«Административные системы компании BT» – платформа для выставления счетов-фактур компании BT (в настоящее время iSupplier), или по соглашению с компанией BT другие сугубо административные системы;

«Клиент компании BT» – в контексте настоящих Требований безопасности корпорация или физическое лицо, которому компания BT предоставляет товары или услуги.

«Информация компании BT» – информация о компании BT или клиентах компании BT, предоставленная Поставщику, а также вся информация, которая обрабатывается или находится у Поставщика по поручению компании BT или клиента компании BT согласно Договору.

«Сеть компании BT» – сеть под контролем и администрированием компании BT.

«Материальные активы компании BT» – все физические активы (включая, без ограничений, маршрутизаторы, коммутаторы, ключи от серверов и шкафов, аппаратные токены, карточки-пропуски, планы или документацию), принадлежащие компании BT и находящиеся у Поставщика.

«Служба безопасности компании BT» – организация в составе компании BT, отвечающая за безопасность.

«Контактное лицо компании BT по безопасности» – специалист по обеспечению информационной безопасности в Службе безопасности компании BT или Коммерческое контактное лицо компании BT, с уведомлением Поставщика или центрального отдела безопасности 0800 321999 [+44 1908 641100], которое будет единственным контактным лицом по вопросам, связанным с настоящими требованиями безопасности и любым соответствующим инцидентом информационной безопасности.

«Системы компании BT» – сервисы и их компоненты, продукты, сети, серверы, процессы, бумажные или IT-системы (полностью или частично), принадлежащие и/или эксплуатируемые компанией BT или другие системы, которые могут размещаться в помещениях BT, в том числе iSupplier (как определено в разделе **«Оплата и выставление счетов»**).

«Массив данных» – объем информации более 1000 единиц информации компании BT под грифом «Секретно» или 100 единиц информации компании BT под грифом «Совершенно секретно».

«**Система CCTV**» – замкнутая система видеонаблюдения.

«Персонал по контракту», **«Соответствующий персонал по контракту»** – согласно определениям в Договоре.

«**Система Cyber Essentials Plus**» – система при поддержке правительства Великобритании, помогающая организациям защититься от обычных кибератак. Система доступна на https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

«Передовые отраслевые методы обеспечения безопасности» – применение в любых ситуациях практик, политик, стандартов и инструментов безопасности, обоснованно ожидаемых от квалифицированного и опытного специалиста, занимающегося одним видом деятельности в однотипных ситуациях.

«Информация» – информация в материальной или любой другой форме, включая, помимо прочего, спецификации, отчеты, данные, заметки, документацию, чертежи, программное обеспечение, вывод данных компьютера, разработки, электрические схемы, модели, наборы данных, образцы, изобретения (независимо от наличия патента) «ноу-хау», а также средства передачи этой информации (при наличии).

«Открытая», «**Для служебного пользования**», «**Секретно»** и «**Совершенно секретно»** – грифы секретности информации согласно Правилам классификации и обработки данных третьих сторон.

«Стандарт ISO 27001» – действующая версия международного стандарта управления системами безопасности, принятого Международной организацией по стандартизации и Международной электротехнической комиссией.

«Сетевые устройства» – устройство или другой компонент Сети компании BT, поддерживающий работу сети.

«Сетевая безопасность» – безопасность взаимосвязанных каналов и узлов связи, логически соединяющих технологические системы конечных пользователей с административными системами.

«Обрабатывать», **«Обработанный»** или **«Обработка»**, **«Обрабатывающее приложение»** и **«Персональные данные»** – значения определены разделом **«Защита персональных данных»**

«Выявленный инцидент информационной безопасности» – фактическое или подозреваемое нарушение безопасности в системах или сервисах, а также события безопасности, влияющие на Поставки или выполнение

Договора (включая фактические или прогнозируемые потери, ущерб, кражу или неправильное использование информации или систем компании BT), включая, но не ограничиваясь:

- потерю сервиса, оборудования или объектов;
- порчу, повреждение или злоупотребление материальными активами компании BT;
- неисправности или перегрузки системы;
- человеческий фактор;
- несоответствия требованиям безопасности, описанным в настоящем документе;
- нарушения мер физической безопасности;
- бесконтрольные изменения в системе;
- нарушение работы аппаратного или программного обеспечения;
- несанкционированный доступ;
- известные или предполагаемые потери данных в соединениях между системами компании BT и Поставщика.

«Удаленный доступ» – удаленный доступ к системе компании BT из дома или другого места через общедоступную сеть (например, Интернет) или сеть Поставщика.

«Требования безопасности» – своевременно обновляемые действующие Требования безопасности компании BT.

«Поставки» – обобщенное обозначение терминов **«Услуги», «Поставки», «Товары»** и **«Работы»** согласно Договору и его производным.

«Системы Поставщика» – любой принадлежащий Поставщику компьютер, приложение или сетевые системы, используемые для доступа, хранения или обработки информации компании BT, или участвующие в обеспечении Поставки.

«Контактное лицо Поставщика по безопасности» – лицо, чьи контактные данные Поставщик должен периодически сообщать компании BT, и которое будет единственным контактным лицом по вопросам, связанным с настоящими Требованиями безопасности, и любым Выявленным инцидентом информационной безопасности

«Передача» или **«Переданный»** – перемещение информации компании BT, находящейся во владении у персонала по контракту (включая, помимо прочего, персональные данные) от одного места/лица другому месту/лицу с использованием физических, голосовых или электронных средств, а также предоставление доступа к информации компании BT, находящейся во владении персонала по контракту (включая, помимо прочего, персональные данные) одним местом/лицом другому месту/лицу с использованием физических, голосовых или электронных средств.

«Правила классификации и обработки данных третьих сторон» – требования к работе с информацией Поставщика согласно https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm в новейшей редакции.