Содержание

1. Вводная часть

1.1 В настоящем документе изложены Требования безопасности "BT", и он применим ко всем третьим сторонам, работающим на или от имени BT Group и входящих в неё Openreach, EE и PlusNet, которые далее будут совместно называться «"BT".

1.2 Настоящие требования безопасности дополняют и не ограничивают любые другие обязательствам третьей стороны по Контракту.

1.3 Все стандарты, упомянутые в этом документе, можно найти здесь Стандарты для третьих сторон

2. Требования ограниченного доступа

2.1 Без ущерба для каких-либо обязательств конфиденциальности, которые может иметь персонал третьей стороны, имеющий доступ к информации "BT", третья сторона должна:

2.2 Гарантировать, что информация "BT" не разглашается и не доступна персоналу третьей стороны, за исключением случаев, когда это необходимо для предоставления услуг; и

2.3 Внедрить все системы и процессы, как технические, так и организационные, необходимые для защиты информации "BT" (i) от случайного или незаконного уничтожения и (ii) потери, изменения, несанкционированного раскрытия или доступа к информации "BT" в соответствии с добросовестной отраслевой практикой обеспечения безопасности.

3. Общая информационная безопасность

3.1 По обоснованному запросу третья сторона должна предоставить "BT" копии сертификатов безопасности и декларации соответствия, относящихся к услугам, для подтверждения соответствия настоящим Требованиям безопасности.

3.2 В случае существенного изменения технологий, отраслеВых стандартов безопасности или каких-либо существенных изменений в услугах или способе их предоставления "BT" может внести поправки в Контракт в течение срока его действия, если есть необходимость в изменении действующих Требований безопасности. Третья сторона обязуется соблюдать согласованные поправки к Контракту в течение разумного периода времени с учётом характера изменений и риска для "BT".

3.3 Третья сторона должна не реже раза в год или после каких-либо существенных изменений в услугах или способе их предоставления пересматривать настоящие Требования безопасности и соответствующие стандарты, чтобы гарантировать, что они по-прежнему соответствуют всем действующим правилам безопасности.

3.4 Если третья сторона передаёт обязательства по Контракту субподрядчикам, она должна гарантировать, что все контракты с соответствующими субподрядчиками и их субподрядчиками включают письменные условия, требующие от них соблюдения применимых частей настоящих Требований безопасности или таких же требований безопасности третьей стороны.

3.5 Срок хранения информации "BT" должен быть достаточным для Выполнения Контракта, после завершения действия которого информация должна храниться не более двух лет, если только между "BT" и третьей стороной не был согласован другой срок или продление срока не является требованием действующего законодательства.

3.6 Если услуги предоставляются по контракту с правительством Великобритании, третья сторона должна Выполнять требования последней версии правил Государственного центра кибербезопасности.

3.7 Третья сторона должна гарантировать, что информация "BT" обрабатывается с использованием средств контроля, указанных в следующих стандартах:

- Стандарт по классификации и обращению с информацией третьей стороной, редакция 4.0
- наш Стандарт контроля для третьих сторон редакция 1.1,

  Раздел 1 Роли и обязанности

  Раздел 2 Система контроля

  Раздел 3 Управление инцидентами

  Раздел 4 Управление изменениями

  Раздел 5 Управление киберрисками и киберугрозами

  Раздел 6 Управление идентификационными данными и контроль доступа

  Раздел 10 Классификация и защита данных

  Раздел 12 Предотвращение утечки данных

  Раздел 13 PCI-DSS (если входит в перечень услуг)

  Раздел 19 Управление уязвимостями

  Раздел 22 Непрерывная регистрация и контроль безопасности

4. Требования безопасности к персоналу третьей стороны

4.1 Третья сторона должна гарантировать, что весь её персонал подписал соглашения о конфиденциальности перед началом работы в зданиях "BT" или с системами "BT" или до получения доступа к информации "BT". Эти соглашения о конфиденциальности должны храниться третьей стороной и предъявляться "BT" во время для аудита.

4.2 Третья сторона должна реагировать на нарушения действующих правил контроля и стандартов безопасности (её и "BT"), принимая официальные меры, включая дисциплинарные, которые могут предусматривать:

4.2.1 лишение нарушителя доступа к системам или информации "BT"; или

4.2.2 отстранение нарушителя от работ, связанных с предоставлением услуг.

Кроме того, третья сторона должна гарантировать наличие процедур, препятствующих доступу отстранённого персонала к системам и информации "BT" и работе, связанной с предоставлением услуг "BT".

4.3 Третья сторона, в рамках, разрешённых законом, должна организовать службу анонимного информирования, куда её персонал сможет сообщать о фактах

побуждения к действиям, несовместимым или нарушающим настоящие требования безопасности. Соответствующие отчёты должны передаваться "BT".

- После отстранения персонала третьей стороны от предоставления услуг любые физические актиВы или информация "BT", находящиеся у персонала третьей стороны, должны быть (по усмотрению "BT") или возвращены соответствующей оперативной группе "BT" или
- уничтожены в соответствии со Стандартом по классификации и обращению с информацией третьей стороной в редакции 4.0.

4.4 Третья сторона должна гарантировать наличие соответствующих процедур для обеспечения возврата персоналом третьей стороны средств контроля, указанных в следующих стандартах:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 15. Социальные сети

Раздел 23. Обучение и информирование

5. Аудит и анализ состояний безопасности

5.1 Без ущерба для любого другого права аудита, которое может иметь "BT" для оценки соответствия третьей стороны настоящим требованиям безопасности и связанным стандартам, третья сторона будет предоставлять "BT" или её представителям доступ и содействие (по мере необходимости) для проверки документов и проведения Выездных аудитов безопасности. Перед проведением планового Выездного аудита третья сторона будет уведомляться о нём не менее, чем за 30 рабочих дней.

Предметом аудита являются все аспекты политик, процессов и систем третьей стороны (при условии, что третья сторона защищает конфиденциальность любой информации, не связанной с предоставлением услуг "BT"), связанных с предоставляемыми услугами.

5.2 Третья сторона обязуется сотрудничать с "BT" и Выполнить за свой счёт согласованные рекомендации и любые корректирующие действия, определённые как необходимые в результате проверки документации или Выездного аудита безопасности в течение 30 дней с момента уведомления от "BT" или согласованного сторонами периода.

5.3 Если "BT" привлечёт независимого аудитора и после такого аудита Выяснится, что третья сторона не соблюдает принципы и методы ISO/IEC 27001: 2013, третья сторона будет должна за свой счёт предпринять действия по достижению соответствия требованиям безопасности и полностью возместить расходы "BT"при проведении такого аудита.

6. Право инспектирования

6.1 Третья сторона должна предоставить "BT" право инспектирования согласно:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 24. "Право инспектирования"

7. Сертификация системы безопасности

7.1 Системы, услуги, связанные услуги, процессы и физические объекты должны постоянно соответствовать стандарту ISO/IEC 27001: 2013 (или сертификации, обеспечивающей эквивалентный уровень контроля и подтверждённой актом проверки независимого аудитора), а также любой исправленной или будущей редакции Стандарта. Это соответствие должно быть подтверждено или:

7.1.1 сертификацией системы управления информационной безопасностью третьей стороны в Службе аккредитации Соединённого Королевства или равноценным полномочным международным органом сертификации или

7.1.2 результатами двустороннего аудита и тестирования, назначенного "BT".

7.2 Третья сторона должна предоставлять действительный сертификат после подписания Контракта и повторной сертификации в будущем.

7.3 После изменения области действия сертификата или положения о применимости третья сторона должна представить эти изменения для повторной проверки с помощью процедуры контроля изменений (или, при отсутствии процедуры контроля изменений, с помощью процедуры обработки изменений). Третья сторона должна сообщать "BT" в течение 2 рабочих дней о любом серьёзном несоответствии, Выявленном органом по сертификации или третьей стороной.

8. Физическая безопасность — помещения "BT"

8.1 Если третья сторона работает в помещениях "BT", будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 25. Физическая безопасность — помещения "BT"

9. Физическая безопасность — помещения третьей стороны

9.1 Если для предоставления услуг используются помещения третьей стороны, будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 9. Физическая безопасность в помещениях третьей стороны, **исключая** средства контроля 9.10 и 9.11, "Предоставление помещений для размещения оборудования "BT".

10. Предоставление помещений для размещения оборудования "BT"

10.1 Если для размещения оборудования используются помещения третьей стороны, будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 9. Физическая безопасность в помещениях третьей стороны — средства контроля 9.10 и 9.11, "Предоставление помещений для размещения оборудования "BT".

11. Разработка безопасного программного обеспечения

11.1 Если третья сторона предоставляет программное обеспечение или системы, будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 17. (17.1 и 17.2) Разработка безопасного программного обеспечения.

12. Условное депонирование

12.1 Если для защиты всех сторон необходимо условное депонирование, будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 17. (Только 17.3) Разработка безопасного программного обеспечения.

13. Доступ к системам "BT".

13.1 Если для систем или персонала третьей стороны требуется подключение/доступ к системам "BT", будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 8. Доступ к системам "BT".

14. Системы третьей стороны, в которых хранится информация "BT"

14.1 При использовании систем третьей стороны, которые будут хранить информацию "BT", будут применяться средства контроля, указанные в следующих стандартах:

Стандарт по классификации и обращению с информацией третьей стороной, редакция 4.0

- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 7 Управление информационными активами

Раздел 11. Криптография

Раздел 16 Конфигурация систем

Раздел 18 Защита от вредоносных программ

Раздел 21. Защита от атак типа «отказ в обслуживании»

15. Третья сторона, хранящая информацию "BT"

15.1 В тех случаях, когда информация "BT" хранится у третьей стороны, для помещений хранения должен быть получен сертификат ISO/IEC 27001 системы управления безопасностью (или сертификаты, которые демонстрируют наличие эквивалентных средств контроля, что подтверждается отчётом независимого аудитора).

15.2 Должны применяться средства контроля, указанные в следующих стандартах:

- Стандарт по классификации и обращению с информацией третьей стороной, редакция 4.0
- наш Стандарт контроля для третьих сторон редакция 1.1,

Раздел 7 Управление информационными активами

Раздел 11. Криптография

Раздел 16 Конфигурация систем

Раздел 18 Защита от вредоносных программ

Раздел 21. Защита от атак типа «отказ в обслуживании»

16. Безопасность сети — собственная сеть "BT"

16.1 В тех случаях, когда третья сторона будет устанавливать оборудование, настраивать, обслуживать, ремонтировать или контролировать сеть "BT", будут применяться средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

  Раздел 26. Безопасность сети — собственная сеть "BT"

17. Безопасность сети третьей стороны

17.1 Если для доступа к информации "BT" или для предоставления услуг будет использоваться собственная сеть третьей стороны, необходимо применять средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

  Раздел 16 Конфигурация систем

  Раздел 20 Целостность сетей

18. Облачная информационная безопасность

18.1 Если третья сторона будет предоставлять "BT"облачные услуги, необходимо применять средства контроля, указанные в следующем стандарте:

- наш Стандарт контроля для третьих сторон редакция 1.1,

  Раздел 14. Облачные / сетеВые Вычисления

19. Контактный центр

19.1 Если третья сторона будет предоставлять "BT" услуги контактного центра, необходимо применять средства контроля, указанные в следующем стандарте:

- Стандарт по предоставлению услуг контактного центра третьей стороной, редакция 1.0

20. Информация, классифицируемая правительством Её Величества как «служебная» или Выше

20.1 Если Поставщик обязан осуществлять доступ, хранить, обрабатывать или передавать информацию, классифицированную как HMG OFFICIAL Поставщик или Выше должен провести оценку риска безопасности персонала для всех ролей, указанных в п. 2 Официальной конфиденциальной декларации, в соответствии с требованиями, изложенными в документе «Разрешение на национальную безопасность CPNI - Руководство» (4-е издание - июнь 2013 г. или позднее).

20.2 К каждой третьей стороне, занимающейся хранением, обработкой или передачей информации, классифицируемой как «служебная и конфиденциальная» в соответствии с регулярно обновляемой Системой классификации безопасности Её

Величества, будут применяться Дополнительные требования безопасности, изложенные в Приложении 1 к настоящим Требованиям безопасности.

20.3 Третья сторона должна обеспечить Выделенную логическую сеть для систем и инфраструктуры, применяемых для предоставления услуг. Такая сеть должна состоять только из систем, образующих защищённый комплекс обработки данных клиентов.

21. Термины и их толкование

21.1 Если иное не указано ниже, слова и Выражения, используемые в настоящих Требованиях безопасности, имеют то же значение, что и в Контракте:

Доступ — обработка, обращение или хранение информации "BT", полученной с использованием одного или нескольких из следующих способов или источников:

a. посредством подключения к системам "BT";
b. информации, предоставленной в бумажном или неэлектронном формате;
c. информации "BT" в системах поставщика;
d. посредством мобильных средств распространения информации

и/или посредством доступа в помещения "BT" для предоставления услуг, исключая предоставление аппаратных средств и присутствие на совещаниях.

Информация "BT" — вся информация, касающаяся "BT" или клиента "BT", предоставленная Поставщику, и вся информация, которая обрабатывается Поставщиком от имени "BT" или клиента "BT" по Контракту.

Системы "BT" — сервисы и компоненты сервисов, продукты, сети, серверы, процессы, печатные системы или IT-системы (полностью или частично), принадлежащие и/или управляемые "BT", или другие системы, которые могут быть размещены в помещениях "BT".

Договор — договор, заключенный сторонами на поставку товаров, программного обеспечения или услуг, в котором есть ссылки на настоящие Требования безопасности.

Важнейшие аспекты кибербезопасности (Cyber Essentials Plus) — поддерживаемая правительством Великобритании система, помогающая организациям защитить себя от обычных кибератак.

Эскроу — соглашение об условном депонировании исходного кода, заключённое в соответствии с Договором, для использования, копирования, сохранения и изменения такого исходного кода в коммерческих целях "BT" (включая право на компиляцию такого исходного кода).

Добросовестная отраслевая практика обеспечения безопасности — в отношении любых взятых обязательств и обстоятельств означает реализацию мер безопасности, политик, стандартов и инструментов, которую следует обычно и обоснованно ожидать от квалифицированного и опытного человека, занимающегося одним и тем же видом деятельности при тех же или аналогичных обстоятельствах.

Безопасность сетей — безопасность взаимосвязанных каналов и узлов связи, которые логически соединяют технологии конечного пользователя вместе, а также связанных систем управления.

Заявление в отношении конфиденциальной служебной информации — письменное заявление, которое должно делаться Поставщиком в отношении ролей с доступом к информации, классифицированной как «служебная и конфиденциальная», или дающих Высокие привилегии доступа к инфраструктуре хранения, обработки или передачи информации, классифицированной как «служебная и конфиденциальная», форма которого приведена в Приложении 1.

Требования безопасности — это настоящий документ с периодическими обновлениями.

Субподрядчик — субподрядчик Поставщика, который предоставляет или участвует в предоставлении услуг или который нанимает или привлекает лиц, занимающихся предоставлением услуг.

Персонал третьей стороны —любые лица, привлечённые Поставщиком или его субподрядчиками к Выполнению обязательств Поставщика по Контракту.

Услуга — все **Товары**, **Программное обеспечение** или **Услуги**, указанные в Контракте.

Системы третьей стороны — любые принадлежащие Поставщику компьютерные, программные или сетеВые системы, используемые для доступа, хранения или обработки информации "BT" или задействованные в предоставлении Услуг.

Толкование словесных Выражений

21.2 Любые слова, следующие за словами «включая», «включает», «в частности», «например» или любыми аналогичными Выражениями, должны толковаться как пояснительные и не ограничивать смысл слов, описаний, определений, фраз или терминов, стоящих перед такими Выражениями.

21.3 Если обязательство или право Стороны Выражается в виде обязательства или права, которое она «**может**» осуществить или реализовать, принятие решения в отношении такого осуществления или реализации остаётся на усмотрение этой Стороны.

21.4 Там, где в документе приведена какая-либо гиперссылка («**URL**»), она будет обеспечивать переход на такой онлайн-ресурс, который доступен по этому URL-адресу или другому URL-адресу, периодически сообщаемому соответствующей Стороне.

Версия нет	описание	Изменение сделано	Дата
4.0	новый	Karen Tanner	02/02/20
4.1	Дополнительный пункт для набора предложений HMG 20	Karen Tanner	20/02/20

ПРИЛОЖЕНИЕ 1 – Дополнительные требования безопасности

Если третья сторона обязана осуществлять доступ, хранить, обрабатывать или передавать информацию Правительства Её Величества, классифицированную как «служебная и конфиденциальная», она должна будет соблюдать настоящие Требования безопасности и, кроме того, требования, изложенные в настоящем Приложении 1, а также предоставить "BT" заполненную форму "Заявления в отношении служебной конфиденциальной информации" до подписания Контракта. В любом случае, требования более Высокого уровня конфиденциальности будут иметь преимущественную силу над любыми из требований безопасности в настоящем документе, касающихся услуг и систем, указанных в «Заявлении в отношении служебной конфиденциальной информации».

1. РАБОТНИКИ

1.1. Все роли, определённые третьей стороной для получение доступа к информации, классифицированной как «служебная и конфиденциальная», или дающие Высокие привилегии доступа к инфраструктуре хранения, обработки или передачи «служебной и конфиденциальной» информации, будут указаны в «Заявлении в отношении конфиденциальной служебной информации».

1.2. Персонал третьей стороны, которому назначены роли, указанные в «Заявлении в отношении конфиденциальной служебной информации» должен:

1.2.1. пройти предварительный отбор на работу в соответствии с базоВым стандартом безопасности персонала (BPSS);

1.2.2. подписать личную декларацию по "Закону о государственной тайне", а

1.2.3. персоналу, не прошедшему требуемую проверку безопасности, должно быть отказано в доступе к информации и системам.

2. ИНСТРУКТАЖ ПО БЕЗОПАСНОСТИ

2.1. После приёма персонала на работу третья сторона не реже раза в год должна проводить обязательный инструктаж по безопасности, который должен охватывать требования к обращению с информацией, классифицированной как «служебная» и «служебная и конфиденциальная» в соответствии с Системой классификации безопасности Её Величества, как указано в Руководстве "BT" по защите информации Её Величества третьими сторонами.

2.2. Третья сторона должна обновлять должностные инструкции для ролей, обозначенных в «Заявлении в отношении конфиденциальной служебной информации», с указанием обязательности участия в инструктаже, предусмотренном в пункте 2.1 Выше. Третья сторона будет вести протокол инструктажа, предоставляемый "BT" по её запросу.

3. КОНТРОЛЬ ДОСТУПА

3.1. При отзыве или изменении ролей сотрудников их права доступа к системам третьей стороны должны отзываться в течение одного (1) рабочего дня.

3.2. Если работники третьей стороны, включая подрядчиков, временных сотрудников и привлечённых работников, имеют Высокие привилегии доступа к инфраструктуре "BT", третья сторона должна письменно уведомить "BT" в течение 1 рабочего дня с момента, когда исчезает необходимость в доступе к системам "BT" (например, после увольнения или изменения роли).

3.3. Если работникам третьей стороны, включая подрядчиков, временных сотрудников и привлечённых работников, были Выданы постоянные карты доступа в помещения "BT", третья сторона должна письменно уведомить "BT" в течение 1 рабочего дня с момента, когда исчезает необходимость в доступе в помещения "BT" (например, после увольнения или изменения роли).

4. ОЦЕНКА И КЛАССИФИКАЦИЯ АКТИВОВ

4.1. Третья сторона должна ввести дополнительные процедуры для Выполнения требований к обращению с информацией, классифицированной как «служебная» и «служебная и конфиденциальная» в соответствии с периодически обновляемой Системой классификации безопасности Правительства Её Величества.

5. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И ОТЧЁТНОСТЬ ПО НИМ – СОГЛАШЕНИЯ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ

5.1. Третья сторона будет уведомляться о необходимости заключения отдельных соглашений об уровне обслуживания для поддержки процесса реагирования на инциденты. Они могут заменять любое предыдущее соглашение, указанное в настоящих Требованиях безопасности.

6. АУДИТ, ТЕСТИРОВАНИЕ И МОНИТОРИНГ

6.1. Третья сторона будет осуществлять круглосуточный мониторинг безопасности в формате 24/7 в случаях, когда это указано "BT".

6.2. Инфраструктура третьей стороны, подлежащая круглосуточному мониторингу безопасности, будет указана в «Заявлении в отношении конфиденциальной служебной информации».

7. НЕПРЕРЫВНОСТЬ РАБОТЫ И ПОСЛЕАВАРИЙНОЕ ВОССТАНОВЛЕНИЕ

7.1. Третья сторона подготовит план обеспечения непрерывности своей работы и послеаварийного восстановления в соответствии со стандартом BS ISO 22301 в течение 30 дней после подписания Контракта.

8. МЕСТОНАХОЖДЕНИЕ

8.1. Если иное не указано "BT", услуги должны предоставляться в пределах физических границ Великобритании или, если необходимо, ЕЭЗ.

ПРИЛОЖЕНИЕ 1, ДОКУМЕНТАЛЬНОЕ ПОДТВЕРЖДЕНИЕ 1 – ОБРАЗЕЦ ДОКУМЕНТА «ЗАЯВЛЕНИЕ В ОТНОШЕНИИ КОНФИДЕНЦИАЛЬНОЙ СЛУЖЕБНОЙ ИНФОРМАЦИИ»

1. Системы/объём предоставляемых услуг

Пожалуйста, перечислите системы и услуги, предоставляемые клиенту Правительства Её Величества.

Система	Услуга

2. Роли третьей стороны, требующие допуска к государственным секретам.

Должность	Требуемый уровень допуска к государственным секретам
* *Например, доступ к базам данных*	*Доступ к секретной информации*

3. Управление уязвимостями

Система	Оценка типа уязвимости	Периодичность

4. Аудит, тестирование и мониторинг

Системы с круглосуточным мониторингом согласно требованиям "BT"