Стандарты работы Колл-центра

Общие условия

(A) Настоящие Требования следует читать вместе с Матрицей внедрения, содержащейся в Приложении 1 к настоящему документу, где детально описаны стили поведения и результаты, которые компания BT будет, как правило, считать приемлемыми при рассмотрении вопроса выполнения Требований Поставщиком.

(B) Компания BT может проводить оценки рисков для контактного центра, как предусмотрено разделом 3.10 Требований компании BT в отношении безопасности операций с поставщиками («Требования безопасности») в любой момент, как до, так и в процессе предоставления услуг. Не ограничивая любые другие средства судебной защиты, имеющиеся в распоряжении компании BT, BT может предусмотреть меры по устранению последствий, компенсирующие средства контроля и контрмеры с целью управления выявленными рисками и/или случаями неудовлетворительного выполнения или невыполнения настоящих Требований, которые будут реализованы Поставщиком и документально оформлены в форме Приложения к настоящему стандарту; при этом все расходы, связанные с внедрением новых Требований безопасности, подлежат согласованию обеими сторонами.

(C) Компания BT, в случае получения соответствующего запроса, имеет право на изучение политик и процедур Поставщика, обеспечивающих выполнение требований этого стандарта, в рамках работы по оценке рисков для контактного центра. Такие политики могут включать, но не ограничиваться ими: Политику использования компьютеров, утилизацию средств IT, аутентификацию клиентов, проверки перед принятием на работу, процедуры оценки и управления рисками и т.д.

1. Физическая защита

1.1 Поставщик обязан обеспечить физическое отделение площадей контактного центра (см. Глоссарий), используемых для управления учетной записью BT/EE, от всех прочих бизнес-площадей специальными средствами физического контроля.

1.2 Поставщик обязан внедрить проверяемую аудитом процедуру доступа, предусматривающую подачу запроса и утверждение нового физического доступа или запрет доступа в зону контактного центра. [1]

1.3 Поставщик обязан обеспечить внедрение нормы, согласно которой для получения прав физического доступа в помещения контактного центра (включая внутренние перемещения и изменения) один раз в три месяца должна проводиться проверяемая аудитом процедура обзора доступа с регистрацией даты обзора.

1.4 Поставщик обязан предотвращать случаи работы в зоне контактного центра в отсутствии других лиц. Данное требование распространяется на уборщиков и других работников третьих сторон.

1.5 Поставщик обязан внедрить проверяемую аудитом процедуру предотвращения несанкционированного прохода нескольких лиц по одному предъявленному идентификатору через контролируемые двери и/или турникеты. Процесс подлежит

[1] Примеры проверяемой аудитом процедуры доступа представлены в Матрице внедрения

исполнению в принудительном порядке, при этом повторное нарушение предусматривает наложение дисциплинарных санкций.

2. Пропуска и посетители

2.1 Поставщик обязан обеспечить опознаваемость работников (при выполнении ими своих обязанностей), имеющих разрешение на ношение и использование мобильных телефонов, переносных компьютеров, устройств iPads и/или планшетных компьютеров в помещениях контактного центра, другими работниками и руководителями.[2]

2.2 Поставщик обязан внедрить проверяемую аудитом процедуру выдачи, в случаях необходимости, пропусков и временных пропусков в контактный центр работникам, включающую автоматическое аннулирование прав допуска после истечения периода действия пропуска.

2.3 Поставщик обязан обеспечить, чтобы пропуска и значки не идентифицировали место работы работника.

2.4 Поставщик обязан внедрить проверяемую аудитом процедуру посещения, доведенную до сведения всех работников. В центре надлежит вести журнал регистрации посетителей.[3]

2.5 Пропуска посетителей должны быть отличимыми от пропусков работников и должны изыматься в момент покидания посетителями контактного центра, а все пропуска, которые не были возвращены, должны блокироваться на следующий рабочий день.

2.6 Поставщик обязан обеспечить постоянное сопровождение посетителей контактного центра и ношение ими видимых значков или пропусков посетителей.

3. Работники

3.1 Поставщик обязан обеспечить хранение всех личных вещей (включая мобильные устройства) в специальных локерах вдали от зоны контактного центра.

3.2 Поставщик обязан разрешить содержание в зоне контактного центра необходимых личных медикаментов и базового медицинского оборудования, включая ингаляторы, инсулин и лекарства от кашля.

3.3 Кроме случаев получения разрешения по результатам оценки рисков, персоналу, работающему в зоне контактного центра, не разрешается ношение телефонов или мобильных устройств, если они не разрешены. Поставщик обязан проводить регулярные внезапные выборочные проверки персонала, чтобы убедиться в том, что мобильные телефоны не вносятся в помещение контактного центра, а также обеспечить размещение надписей, запрещающих использование таких устройств. Кроме того, это требование должно доводиться до сведения персонала в ходе обучения по вопросам безопасности, при этом необходимо внедрить процедуру применения дисциплинарных санкций за нарушения.

[2] Матрица внедрения дает примеры объектов, которые могут быть легко опознаны

[3] Матрица внедрения содержит перечень данных, которые должны регистрироваться в журнале регистрации посетителей

3.4 Поставщик обязан внедрить процедуру, позволяющую третьим лицам связаться с работниками в неотложных случаях.[4]

3.5 Должна быть внедрена проверяемая аудитом процедура авторизации и использования ручек, карандашей и бумаги в зоне контактного центра. Использование ручек, карандашей и бумаги не допускается, за исключением случаев получения работниками разрешения на такое использование от их менеджеров в связи с выполнением служебных обязанностей.

3.6 Поставщик обязан обеспечить контроль над всеми письменными заметками, сделанными работниками в ходе выполнения служебных обязанностей, и их безопасное хранение (согласно процедурам обращения с информацией и ее классификации) или их утилизацию[5] в конце рабочего дня с целью демонстрации «Политики чистого стола»[6].

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 Поставщик обязан обеспечить наличие "белых досок" и стираемых записных книжек (включая сухие ручки и ветошь) в качестве альтернативы ручкам, карандашам и бумаге, что позволит работникам делать заметки в ходе звонков. Поставщик обязан обеспечить удаление этих заметок сразу после завершения обработки запроса клиента, при этом в конце смены каждого консультанта должны быть удалены все заметки, сделанные на досках. Для обеспечения выполнения этого требования менеджеры и руководители обязаны перемещаться по этажу и проводить выборочные проверки.

3.8 Поставщик обязан обеспечить автоматическое удаление всех временных заметок, сделанных в режиме он-лайн или в электронных устройствах (при обработке звонков клиентов), в конце смены каждого консультанта или в конце рабочего дня. Такие записи должны удаляться либо автоматически, либо необходимо вести ежедневный журнал выполнения данного требования.

3.9 Поставщик обязан обеспечить внедрение проверяемой аудитом процедуры использования досок/бумаги для обеспечения:

- Безопасного хранения или утилизации бумаг в конце рабочего дня; и
- Очистки досок в конце каждой смены и в конце рабочего дня. [7]

3.10 Поставщик обязан обеспечить регистрацию всех контактов с клиентами в учетной записи (меморандум или записная книжка, в зависимости от используемой системы).

3.11 Поставщик обязан обеспечить выполнение запрета на регистрацию всех контактов с клиентами в программах Microsoft Office, кроме случаев, когда работники будут уполномочены на это по результатам оценки рисков в рамках выполнения служебных обязанностей.

3.12 Поставщик обязан обеспечить оценку рисков любой роли, уполномоченной на выполнение любых указанных ниже действий в зоне контактного центра, в соответствии с Требованиями, изложенными в разделе 11. Такие действия могут включать, но не ограничиваться ими:

- Использование программ Microsoft Office

[4] Матрица внедрения представляет примеры процедур связи в неотложных случаях
[5] Матрица внедрения представляет примеры безопасного хранения или утилизации
[6] Матрица внедрения представляет примеры правил, подлежащих включению в Политику чистого стола
[7] Матрица внедрения представляет примеры действий, выполняемых в рамках аудита досок/бумаг

- Использование служебных мобильных устройств
- Использование служебных переносных компьютеров
- Использование личных вещей (в соответствии с определением, представленным в глоссарии)
- Способность печатать или копировать клиентскую информацию
- Способность загружать с сервера (серверов) записи разговоров
- Доступ к средствам внешней, внутренней и другой связи, например, к системе мгновенных отношений
- Использование ручек/карандашей и бумаги для ведения заметок
- Отправка сообщений одновременно нескольким клиентам
- Удаленный доступ к клиентскому оборудованию

3.13 Поставщик обязан запретить возможность отправки сообщений одновременно нескольким клиентам (одного текстового сообщения нескольким клиентам), за исключением случаев получения работниками разрешения на такие действия в связи с выполнением служебных обязанностей. Если такие тексты передаются, следует вести записи для фиксации дат соответствующих событий, получателя (получателей) и причин для отправки.

3.14 Поставщик обязан запретить или предотвратить возможность загрузки записей разговоров с сервера (серверов) записи на настольные или переносные компьютеры, за исключением случаев получения работниками разрешения на такие действия в связи с выполнением служебных обязанностей. Если будет утверждено соответствующее решение, следует регистрировать лица, уполномоченные на выполнение этой функции, а в случаях загрузки записей следует вести записи, демонстрирующие основания для этого, фиксировать соответствующие звонки и причины для загрузки. Необходимо регулярно проверять действительность полномочий консультантов и все случаи нарушений.

4. Оборудование

4.1 Поставщик обязан обеспечить защиту всеми консультантами экранов компьютеров и невозможность видеть их содержание лицам, находящимся за пределами контактного центра.[8]

4.2 Поставщик обязан обеспечить расположение всех принтеров и факсов в безопасных местах, доступ в которые разрешен только уполномоченному персоналу исключительно для служебных целей. Перечень уполномоченных пользователей и цели использования машин должны регулярно пересматриваться для обеспечения их постоянной действительности. Все бумажные копии должны безопасно храниться в соответствии с правилами классификации данных и стандартам обращения, при этом их вынос из контактного центра без разрешения ВТ запрещен.

4.3 Поставщик обязан обеспечить любое печатание или копирование с использованием идентификатора пользователя и кода безопасности, так чтобы все операции печатания проходили мониторинг и регистрацию для целей аудита.

4.4 Поставщик обязан обеспечить установку уничтожителей бумаг с поперечной резкой и мусорных баков для конфиденциальных данных в местах расположения принтеров и

[8] Матрица внедрения представляет примеры «защищенных экранов компьютеров»

факсов. Следует обеспечить регулярное опорожнение уничтожителей бумаг и мусорных баков и безопасную утилизацию содержимого.

4.5 Поставщик обязан обеспечить безопасную утилизацию всей информации на бумажных носителях либо путем уничтожения, либо путем помещения в мусорные баки для конфиденциальных данных в соответствии с разделом 4.4.

4.6 Поставщик обязан обеспечить возврат всех материальных активов, выданных лицам в начале их работы, до наступления момента завершения выполнения ими их ролей в зоне контактного центра или после прекращения соответствующими лицами контракта с ВТ/ЕЕ, при этом необходимо вести инвентарный перечень материальных активов.[9]

4.7 Поставщик обязан обеспечить безопасную утилизацию материальных активов в соответствии с требованиями безопасной утилизации после их получения или выноса.[10]

5. Доступ к системам

5.1 Для защиты клиентских данных все консультанты обязаны фиксировать свой идентификатор пользователя в момент получения доступа к учетной записи клиента, а также причину такого доступа. Доступ предоставляется только после утверждения Собственником системы или линейного менеджера. Кроме того, разрешение на доступ к учетной записи клиента должно предоставляться исключительно для целей выполнения консультантом его роли, и такой доступ должен предоставляться на минимальном уровне, необходимом для выполнения консультантами их работы. Доступ в систему ВТ и/или ЕЕ для просмотра записей клиентов не предоставляется лицам, не нуждающимся в таком доступе.

5.2 За исключением случаев, когда этого требуют операционные потребности, следует предотвращать возможность доступа к данным в режиме просмотра. Случаи санкционированного доступа в режиме просмотра должны регистрироваться и проходить мониторинг для предотвращения ненадлежащего использования данных.

5.3 Поставщик обязан запретить работникам доступ к сети Интернет, персональной электронной почте или средствам внешней электронной почты, доступ к социальным сетям (таким как Facebook) или иным средствам коммуникации, таким как мессенджеры или коммуникаторы, кроме случаев, когда это будет разрешено ВТ в связи с выполнением работниками их служебных обязанностей.

5.4 Поставщик обязан обеспечить регистрацию и мониторинг случаев отправки текстовых сообщений внутри систем поставщиков. Если такие тексты передаются, следует вести записи для регистрации дат соответствующих событий, получателя (получателей) и причин отправки.

5.5 Поставщик обязан разрешить использование исключительно предварительно утвержденных средств удаленного доступа к устройствам клиентов для целей поддержки, и дать право на их использование исключительно персоналу, которому они необходимы для выполнения своих ролей. Права доступа подлежат пересмотру один раз в 3 месяца, при этом они аннулируются в случае отсутствия необходимости в

[9] Матрица внедрения представляет примеры вещей, подлежащих регистрации в инвентарном перечне материальных активов

[10] Матрица внедрения представляет примеры требований к безопасной утилизации

доступе. Необходимо внедрить решения по идентификации неутвержденных средств удаленного доступа.[11]

5.6 Поставщик обязан запретить удаленный доступ работников контактного центра к рабочей электронной почте или любой иной системе для целей оценки записей клиента.

5.7 Поставщик обязан обеспечить, чтобы работники имели доступ «только в режиме чтения» к ресурсам совместного пользования, предоставленным и контролируемым только ВТ и/или ЕЕ. Использование других ресурсов совместного пользования в контактном центре запрещено. Загрузка, копирование, вынос или изменение клиентской информации, хранящейся в любой системе, программе или базе данных ВТ и/или ЕЕ не допускаются.

6. Записи разговоров

6.1 Поставщик обязан обеспечить запись всех разговоров с клиентами. Поставщик обязан обеспечить защиту записей разговоров (голос и экран) в процессе их передачи с настольного компьютера на сервер(ы) голосовых записей.[12]

6.2 Поставщик обязан обеспечить защищенное хранение записей телефонных звонков, в частности, если они включают данные платежных карт, для предотвращения потери или ненадлежащего использования этих клиентских данных. Данные PCI подлежат шифрованию с помощью ключевого управленческого решения, внедренного для защиты, с использованием передовой отраслевой практики. Время от времени ВТ и/или ЕЕ могут пересматривать средства шифрования и решения в сфере защищенного хранения для обеспечения их приемлемости и надежности. .

7. Идентификация клиента

7.1 Поставщик обязан обеспечить наличие утвержденной процедуры идентификации клиента в ходе «исходящих» и «входящих» звонков. [13]

7.2 Поставщик обязан обеспечить, чтобы ПИНы и пароли, используемые клиентами для подтверждения их личности, не были видны другим работникам контактного центра, например, за счет использования защищенных экранов или физического отделения.

7.3 Поставщик обязан обеспечить автоматизацию процедуры идентификации, чтобы она не требовала от клиента раскрытия его полного ПИНа или пароля консультанту, например, за счет использования запроса системы на генерирование случайных цифр/букв пароля, например, 1, 3 и 5. ВТ и/или ЕЕ могут время от времени пересматривать процедуру идентификации клиентов для обеспечения выполнения настоящих Требований.

[11] Матрица внедрения представляет примеры действий по идентификации и описывает средства удаленного доступа

[12] Матрица внедрения представляет примеры способов защиты передаваемых голосовых записей.

[13] Матрица внедрения представляет примеры процедур идентификации клиента.

7.4 Поставщик обязан обеспечить, чтобы в случае, когда клиент забудет свой ПИН или пароль и будет нуждаться в их сбросе, любой сброс происходил лишь после правильного прохождения клиентом дополнительных проверок по вопросам идентификации.[14]

7.5 Поставщик обязан обеспечить автоматизацию систем установки ПИН или пароля учетной записи клиентов и осуществление указанных действий без контакта с работником контактного центра.

7.6 Поставщик обязан обеспечить создание новых ПИН или паролей, генерированных автоматической системой, а также отправку всех новых ПИН или паролей непосредственно клиенту текстом или по электронной почте без участия консультанта.

7.7 Поставщик обязан обеспечить клиентам возможность изменения пароля или персонального идентификационного кода в режиме он-лайн или через систему интерактивного речевого ответа (IVR).

7.8 Поставщик обязан обеспечить наличие функции «сброс с помощью работника», позволяющую клиентам осуществлять сброс с помощью работника контактного центра. Возможность осуществлять сброс пароля или персонального идентификационного кода должна быть предоставлена ограниченному количеству работников.[15]

7.9 Поставщик обязан быть способным, при получении соответствующего запроса, генерировать аудиторский след, фиксирующий случаи сброса ПИНа и пароля клиента, определить систему, использованную для выполнения сброса (он-лайн, интерактивная система речевой связи или помощь работника), а также личность работника, который участвовал в трансакции.

8. Защита данных

В дополнение к обязательному обучению по вопросам безопасности и защиты данных в компании ВТ (см. Приложение 2), которое должны пройти все работники Поставщика, после чего они должны подтвердить свое понимание изученного материала, следует обеспечить выполнение следующих требований:

8.1 Поставщик обязан обеспечить работникам контактного центра легкий доступ к существенной и необходимой информации о безопасности и защите данных, разместив ее на первой странице их домашней странички во внутренней корпоративной сети (а если у них нет доступа ко внутренней сети – путем регулярной отправки обновленных данных по электронной почте и проведения обучения).

8.2 Поставщик обязан минимум два раза в год отправлять всем работникам зоны контактного центра регулярные напоминания, формирующие позитивные стили поведения и стимулирующие применение передовой практики обеспечения безопасности.

9. Мониторинг

9.1 Поставщик обязан организовывать звонки с целью мониторинга "проверки качества" со стороны руководителей/менеджеров на основе случайно выбранных телефонных

[14] Матрица внедрения представляет примеры действий в рамках дополнительных проверок по вопросам идентификации.
[15] Матрица внедрения представляет примеры оказания работником помощи клиентам в ходе сброса.

звонков клиентов (входящих и исходящих). Такие проверки должны проводиться еженедельно с целью, среди прочего, проверки на предмет использования корректной процедуры идентификации клиентов.[16]

9.2 Поставщик обязан обеспечить признание "недействительными" телефонных звонков в тех случаях, когда работник не выполнил корректную процедуру идентификации клиента. После каждого недействительного телефонного звонка Поставщик должен проводить процедуру предоставления обратной связи с целью напомнить консультантам контактного центра об их обязанности надлежащим образом идентифицировать клиентов и/или обеспечивать безопасность паролей (в зависимости от обстоятельств).

9.3 Поставщик обязан внедрить процедуру действий в случаях повторных недействительных звонков со стороны работников контактного центра и невыполнения надлежащей процедуры идентификации клиента. Сюда следует включить информацию о последствиях повторного невыполнения консультантом надлежащей процедуры идентификации клиента или нарушения правил регистрации данных. Такие данные могут использоваться для целей оценки результатов работы работников или в процессе наложения дисциплинарных взысканий на соответствующих лиц.

10. Соответствие требованиям

10.1 Поставщик обязан обеспечить наличие задокументированной проверяемой аудитом процедуры для проведения и управления регулярными проверками на предмет выполнения требований на месте и/или выборочными проверками на предмет выполнения требований этого стандарта и Требовании ВТ в отношении безопасности, например, в процессе перемещения по этажу, проверки соблюдения требований политики чистого стола и т.д.[17]

10.2 Поставщик обязан внедрить процедуру, обеспечивающую проведение ежеквартальных проверок на основе данных (10 % выборка) работников контактного центра или любых лиц, работающих на ВТ и/или по контракту с ЕЕ, для проведения процедуры проверки перед принятием на работу и проведения обучения по вопросам безопасности (в рамках программы введения в должность) и обеспечить их эффективность. Это обеспечит адекватную проверку данных работников, работающих в помещениях контактного центра (в соответствии с политикой проверки персонала до приема на работу в ВТ), и прохождение ими обучения по вопросам безопасности, чтобы получить достаточную уверенность в том, что конфиденциальные данные клиентов защищены надлежащим образом.

10.3 Поставщик обязан внедрить процедуру, обеспечивающую проведение ежеквартальных проверок на основе данных (100 % выборка) работников контактного центра или любых лиц, работающих на ВТ и/или по контракту с ЕЕ, для того, чтобы обеспечить прохождение ежегодного обязательного обучения по вопросам безопасности и защиты данных.

10.4 Поставщик обязан обеспечить проведение ежеквартальных инструктажей в рамках программы повышения квалификации на тему обязанностей работников в сфере

[16] Матрица внедрения содержит примеры того, что следует, как минимум, включать в любую проверку качества

[17] Матрица внедрения содержит примеры действий, которые должны включаться в процедуры внезапных выборочных проверок на предмет выполнения требований.

безопасности и защиты данных, при этом надлежит организовать документирование фактов участия работников и проверку понимания ими предмета.

10.5 Поставщик обязан предоставить работникам контактного центра документацию, содержащую соответствующие политики, стандарты, инструкции и процедуры, с целью обеспечения выполнения этого стандарта и требований компании в отношении безопасности.

11. Оценка рисков

Поставщик обязан обеспечить оценку поставщиком рисков и документирование согласно процедурам управления рисками всех случаев нарушений, авторизаций или особых исключений из этих требований. Оценка рисков должна включать:

- причину потребности в соответствующих действиях, а также обоснования всех случаев нарушений этих Требований;
- статус любого нарушения (например, постоянный или временный);
- если нарушение временное, дата, до которой внедрены средства контроля, и дата завершения деятельности;
- функция/роль индивидов и причина приемлемости соответствующей деятельности для этой роли (и причина их исключения из контролей);
- минимизирование рисков средств контроля, возникающих в рамках деятельности;
- обоснование внедрения и/или невнедрения отдельных средств контроля; и
- доказательство утверждения со стороны высшего руководства.

12. Глоссарий

Термин	Объяснение
Контактный центр обслуживания клиентов	Контактный центр (также именуемый «центр взаимодействия с клиентами» или «электронный контактный центр») - центральная точка предприятия, из которой осуществляется управление отношениями со всеми клиентами. Как правило, в контактном центре находятся один или несколько он-лайн колл-центров, однако он может включать другие типы контакта с клиентами, включая новостные рассылки по электронной почте, каталоги, запросы по веб-сайту и чаты, а также данные, получаемые от клиентов в процессе покупок в магазинах. Как правило контактный центр является элементом общего управления отношениями с клиентом.
Специальные локеры	Персоналу, работающему в помещениях контактного центра, не разрешается иметь личные вещи, которые могут обеспечить запись клиентской информации, такие как мобильные телефоны, на своих рабочих местах. Эти вещи запираются в персональных локерах (маркированных как таковые) за пределами зоны контактного центра.
Работник(и) / работник(и)	Работник – любое лицо, работающее в зоне контактного центра, включая постоянных и временных работников Поставщика, персонал агентства, подрядчиков и рабочих.

Сопровождаемый	Для предотвращения случаев непопадания в нужное место или нахождения в местах, где им нельзя находится, необходимо внедрить процедуру работы с посетителями, обеспечивающую, как минимум, постоянное сопровождение посетителей.
Матрица внедрения	Матрица с изменениями, включающая, как минимум, результаты и стандарты, достижение и соблюдение которых должен обеспечить Поставщик при внедрении определенных политик или процедур, упоминаемых в Требованиях.
Работа в одиночестве	Следует внедрить процедуру, не позволяющую одиночную работу в зоне контактного центра после завершения стандартного рабочего дня без разрешения руководства. Это включает уборщиков и других лиц, не работающих в компании, таких как эксплуатационный персонал.
Программы Microsoft Office	Программы Microsoft Office включают, но без ограничений, программы Word, PowerPoint, Excel, Outlook и OneNote. Для исключения эксфильтрации данных взаимодействия с клиентами с использованием он-лайн систем не должны регистрироваться в этих приложениях (кроме случаев, когда это разрешено), поскольку информация из этих программ может быть легко скопирована и извлечена.
Личные вещи	Все личные вещи, которые могут использоваться для перехвата или записи клиентских данных (это включает, но без ограничений, мобильные телефоны, смарт-часы, устройства iPod, iPad, фотоаппараты, флэш-накопители USB, ручки и бумагу).
Средства физического контроля	Используемые средства физического контроля будут зависеть от расположения контактного центра. Средства физического контроля доступа могут быть техническими (например контактная карта, консоль, биометрика) или процедурными (например, ключи с проверяемой аудитом процедуры пропуска или процедура допуска, в рамках которой лицо, контролирующее доступ, проверяет идентификатор), при этом используемые средства физического контроля должны соответствовать типу месторасположения.
Физический актив	Для целей настоящего документа термин «физический актив» означает любой актив, способный обрабатывать или хранить клиентские данные или информацию.
Физическое отделение	Для целей настоящего документа термин «физически отделенные» означает невозможность подслушать разговор или увидеть данные из других бизнес-подразделений. Необходимо установить физический барьер (стены, отдельные здания и т.д.) со средствами физического контроля, регулирующие доступ в соответствующее помещение.
Нарушение безопасности	Нарушение безопасности – это изменение в обычных деловых операциях, влияющее на конфиденциальность, целостность или наличие информационных активов, указывающее на возможный случай нарушения безопасности или стандарта, требования по безопасности, или отказ гарантий безопасности. Примеры: Использование системы не по

	назначению, несанкционированный доступ, потеря или кража оборудования, установка вредоносных программ.
Утверждение со стороны высшего руководства	В случае необходимости согласования любого исключения из этих требований, соответствующие обстоятельства следует оценить на предмет уровня риска, при этом лицо, утверждающее исключение, должно быть работником, отвечающим за управление соответствующим подразделением или направлением, имеющим надлежащие полномочия.
Ответственный за систему	Это должностное лицо, несущее общую ответственность за закупку, разработку, интеграцию, модификацию и поддержку информационной системы.
Следование в хвосте	Практика следования за другим лицом или практика, позволяющая лицу, не имеющему прав доступа, получить доступ в помещение, пройдя контрольно-пропускной барьер/дверь; неиспользование собственного пропуска для получения доступа к служебному помещению Поставщика для целей выполнения контрактов BT/EE.
Временные пропуска, выданные службой безопасности	Эти пропуска должны выдаваться в рамках проверяемой аудитом процедуры (с регистрацией в книге, журнале или в электронной таблице), при этом необходимо фиксировать все случаи выдачи временных пропусков, а также даты выпуска, фамилию, департамент, контактный номер, и основание для выдачи, фамилию принимающего лица и дату возврата временного пропуска. Компания должна внедрить процедуру действий в случае невозврата карточек пропуска.
Идентификатор пользователя	Принтеры и факс-аппараты, находящиеся в зоне контактного центра, должны требовать от пользователей ввода уникального идентификационного номера и кода безопасности, что должно обеспечивать мониторинг их использования пользователями на индивидуальной основе. Кроме того, работники обязаны вводить свой уникальный идентификатор во время просмотра учетных записей клиентов в соответствии с разделом 5.1.

Таблица	**Общее описание**	**Минимальные результаты, считающиеся соответствующими законодательству.**
1.2	Проверяемая аудитом процедура доступа	Электронная таблица или журнал данных с названиями, включая детальную информацию о предоставлении доступа, обоснование причины доступа, дату аннулирования доступа и его причины.
2.1	Легко опознаваемый	Работники, имеющие разрешение на ношение и использование мобильных телефонов, переносных компьютеров, устройств iPads и/или планшетных компьютеров при выполнении ими своих обязанностей, должны быть легко опознаваемы с использованием таких методов, как значки другого цвета или иные отличимые средства идентификации.
2.4	Журналы регистрации посетителей	Следует фиксировать следующую информацию: i) ФИО посетителя, ii) организация, которую они представляют, iii) дата и время входа и выхода, iv) цель визита, v) ФИО посещаемого лица, vi) регистрационные номера всех транспортных средств, прибывающих на объект, vii) номер мобильного телефона, viii) идентификационный номер пропуска посетителя.
3.5	Система неотложной связи	Необходимо внедрить систему, которая позволит родственникам и друзьям связываться с работниками в неотложных случаях. Эта система может использовать специальный выделенный номер или номер руководителя, который может выполнять функцию центрального контактного лица.
3.7	Надежное хранение или утилизация	Если работники в ходе выполнения служебных обязанностей делают заметки, примеры безопасного хранения или утилизации включают, но без ограничений, использование уничтожителей бумаг, конфиденциальные (и потенциально запертые) мусорные баки, и/или хранение в разрешенных местах, которые могут запираться работниками.
3.7	Политика чистого стола	Все материалы должны безопасно храниться или утилизироваться немедленно после их использования, запрещается присутствие каких-либо материалов на рабочих столах на момент завершения рабочего дня. Необходимо проводить регулярные выборочные проверки персонала и внедрить процедуру применения дисциплинарных санкций за нарушения.

3.10	Аудит досок/бумаг	В отношении процедур, описанных в этом разделе 3, следует вести записи (например, в форме электронной таблицы) для демонстрации проведения выборочных проверок, а также обеспечивать соблюдение требований.
4.1	Защищенные компьютерные экраны	Следует обеспечить невозможность видеть экраны консультантов в помещении контактного центра, а также невозможность чтения информации лицами, не уполномоченными на это (такими, как уборщики и обслуживающий персонала). Клиентские данные, хранящиеся на компьютерах должны быть постоянно скрыты за счет размещения мониторов или использования экранов, защищенных от считывания информации посторонними лицами.
4.6	Инвентарный перечень материальных активов	Для целей аудита следует вести инвентарный перечень всех материальных активов и других предметов, выдаваемых работникам, таких как пропуска, ключи от локеров, переносные компьютеры, настольные компьютеры или жетоны удаленного доступа. Когда консультант увольняется или лишается права допуска в контактный центр, необходимо выполнять процедуры, обеспечивающие немедленные шаги, направленные на аннулирование логического и физического доступа и возврат им всех материальных активов, ключей, паролей доступа. Эти процедуры должны быть включены в контрольный перечень вопросов в связи с увольнением.
4.7	Требования к безопасной утилизации	Во время утилизации материальных активов в конце срока их полезного использования, надлежит использовать защищенное программное обеспечение, такое как ‘Tabernus’ или ‘Blanco’, обеспечивающее полное удаление конфиденциальной или клиентской информации из оборудования (когда это необходимо), а также выполнение стандарта, утвержденного ВТ и/или ЕЕ. Если такое программное обеспечение не обеспечивает безопасное удаление данных, оборудование должно быть безопасно уничтожено с использованием процедуры, утвержденной ВТ и/или ЕЕ. Дополнительную помощь в этой сфере может оказать контактное лицо ВТ и/или ЕЕ, отвечающее за безопасность. После удаления конфиденциальной или клиентской информации из оборудования материальные активы могут быть либо повторно использованы в других местах, либо утилизированы, в зависимости от обстоятельств.

5.5	Средства удаленного доступа	Для предотвращения случаев несанкционированного доступа к клиентским данным необходимо внедрить официальные процедуры, которые будут гарантировать, что доступ к устройствам клиента можно получить только с использованием средств удаленного доступа, предварительно утвержденных ВТ и/или ЕЕ. Необходимо внедрить решения для выявления случаев несанкционированного удаленного доступа, при этом такие решения должны регулярно анализироваться, с тем чтобы обеспечить невозможность использования неутвержденных инструментов или убедиться в отсутствии случаев использования неутвержденных инструментов. Кроме того, право на использование утвержденных средств удаленного доступа должно предоставляться ограниченному кругу работников, при этом разрешение таким работникам должно предоставляться в рамках официальной процедуры, включающей оценку рисков, связанных с потребностью в удаленном доступе.
6.1	Передача записей разговоров	Важно передавать записи разговоров с клиентами с ПК на серверы в зашифрованном виде, при этом шифроваться должны как голосовые записи, так и информация на экране.
7.1	Идентификация клиента	Все консультанты обязаны выполнять процедуры идентификации клиентов, утвержденные ВТ/ЕЕ, с тем чтобы убедиться, что клиент является тем, за кого он себя выдает. Эта процедура должна быть сообщена Поставщикам и консультантам, при этом она может быть различной в зависимости от функции (функций) контактного центра.
7.4	Дополнительные проверки по вопросам идентификации	Перед тем как начать процесс изменения ПИНа или пароля клиентов, консультанты обязаны дополнительно получить достаточный объем информации от клиентов, чтобы убедиться, что они являются лицами, за которые себя выдают. Это достигается за счет постановки определенных обеспечивающих безопасность вопросов об их личности дополнительно к просьбе указать фамилию и адрес, например, может быть задан вопрос о последних операциях на счете клиента, о сумме последнего выставленного счета или о длительности периода сотрудничества клиента с ВТ или ЕЕ. При этом выше указаны лишь примеры, и этот перечень не является исчерпывающим.

7.8	Помощь работников клиентам в ходе сброса	Чтобы оказать помощь клиентам, не способным осуществить сброс пароля или персонального идентификационного кода в режиме онлайн или через систему интерактивного речевого ответа, возможность сброса должна быть предоставлена работнику колл-центра. При этом следует внедрить официальную процедуру, позволяющую осуществлять сброс пароля или персонального идентификационного кода ограниченному количеству работников, а также наличие средств обеспечения безопасности, гарантирующие физическое отделение всех работников, имеющих возможность осуществлять сброс пароля или персонального идентификационного кода клиентов, от других работников контактного центра, а также внедрить надлежащие средства контроля. Перечень ответственных за утверждение следует регулярно пересматривать, с тем чтобы обеспечить потребность в таких утверждениях и их применение с надлежащим уровнем дискреционной безопасности.
9.1	Проверка качества мониторинга звонков	Менеджеры должны проводить проверки качества, включая ежедневный мониторинг случайного выбора телефонных звонков клиентов (входящих и исходящих), обрабатываемых консультантами, а также ежемесячный обзор всех записей Поставщиком. Это должно обеспечить соответствие Поставщика этим Требованиям, в частности, использование работниками корректной процедуры идентификации клиентов и ведение правильных записей.
10.1	Внезапные проверки на предмет выполнения требований	Необходимо внедрить проверяемую аудитом процедуру проведения и управления проверками безопасности на местах и внезапных проверок на предмет выполнения всех Требований. Одновременно с обязанностью Поставщика проводить такие проверки, компания BT и/или EE также могут в любое время проводить внезапные выборочные проверки. Внезапные проверки включают, в частности, проверки следующих данных: • идентификационный номер, используемый системой защиты / пропуск, выданный службой безопасности • требования политики чистого стола/чистого экрана • правила использования персональных запирающихся шкафчиков • персональные мобильные устройства • использование досок • вынос или утилизация напечатанной или переданной по факсу конфиденциальной информации

		• идентификация клиента • проверки качества мониторинга звонков • сброс пароля и аудиторские следы • использование текстовых сообщений • прохождение обучения на предмет защиты и безопасности данных и выполнение соответствующих требований Любая внезапная аудиторская проверка должна включать детальное описание действий, которые надлежит предпринимать в случае обнаружения отклонений или нарушений. Необходимо отслеживать процесс выполнения устранения всех нарушений, обнаруженных ВТ и/или ЕЕ, вплоть до момента завершения их выполнения.