Требования к внешнему размещению данных сторонних лиц

В случаях, когда данные компании BT

- размещены во внешней среде (центр данных, не принадлежащий BT);
- передаются между центрами данных (ЦД) (центр данных, не принадлежащий BT);
- передаются между центрами данных и резервным оборудованием (центр данных, не принадлежащий BT),

необходимо соблюдать следующие условия.

Это касается всех данных BT под грифом «Конфиденциально» (К) и «Совершенно конфиденциально» (СК), а также персональных данных BT. Определения терминов приведены в разделе «Положения о классификации и обращении с информацией сторонних лиц» по ссылке http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm. Существуют дополнительные меры контроля для секретных персональных данных.

Код	Меры контроля	Причина
EDH20	В случае несанкционированного доступа к внешнему серверу и кражи или изменения данных BT, должен быть принят алгоритм уведомления о произошедшем компании BT согласно контракту, с достаточной степенью подробности в соответствии с Требованиями к минимальной безопасности BT, а также должен быть обеспечен переход в состояние «защита персональных данных», в случае обработки персональных данных.	Для быстрого доведения до сведения BT о потенциальном инциденте/краже данных.
EDH30	Центр данных должен иметь действительный сертификат в соответствии со стандартом ISO 27001 по информационной безопасности (или сертификат(ы), которые описывают эквивалентные меры контроля, поддерживаемые независимым аудиторским заключением)	В стандарте ISO27001 описана наиболее эффективная структура управления рисками в области защиты информации, состоящая из принятых мер контроля.
EDH60	Система управления использованием криптографических ключей должна соответствовать требованиям Криптографического стандарта, изложенного в разделе «Положения о классификации и обращении с информацией сторонних лиц» http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Наиболее эффективный криптографический метод
EDH70	Логический доступ пользователя в целях администрирования должен быть основан на ролевой модели и предусматривать использование стандартизованной двухфакторной аутентификации, например, одноразовые маркеры пароля или сертификаты, выданные уполномоченными доверенными корневыми центрами сертификации. Перечни и файлы доверенных корневых центров сертификации можно найти по ссылке: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Недостаточный контроль доступа может привести к несанкционированному доступу.
EDH90	Администрирование приложений или данных, размещенных на внешнем сервере, должно осуществляться по защищенному (шифрованному) соединению и предусматривать использование двухфакторной аутентификации, как и для кода EDH70.	Для обеспечения той же степени надежности для удаленного доступа, что и для локального.
EDH100	Любой непосредственный удаленный доступ к данным в случаях, когда данные BT находятся в состоянии передачи или хранения, должен осуществляться из той же страны, в которой расположен центр данных, или из страны или региона, которые могут гарантировать надлежащий уровень защиты данных BT. Удаленное хранилище должно находиться в той же стране, в которой расположен центр данных, или в стране или регионе, которые могут гарантировать надлежащий уровень защиты данных BT.	Для сведения к минимуму риска несоблюдения законов страны о защите данных или обработки данных под грифом «Конфиденциально» в ключевых для BT областях.

Издание: версия 3.0, июль 2017 г.

EDH110	Любой доступ (физический или логический) для контроля изменений или исследования причин возникновения/исправления ошибок должен предусматривать отправку запроса на внесение изменений или заявки на устранение ошибки. Такой доступ должен быть предоставлен только на период внесения изменений/работы с ошибками и прекращен сразу после завершения.	Для сведения к минимуму риска внесения несанкционированных изменений.
EDH130	Резервное хранилище данных должно быть зашифровано на уровне носителей, например, ленточных носителей, дисков и т. п. в соответствии со Стандартом шифрования, описанным в разделе «Положения о классификации и обращении с информацией сторонних лиц» http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Для защиты данных BT и сведения к минимуму риска несоблюдения законов страны о защите данных