IBM Условия за употреба – Специфични условия на оферта SaaS

IBM Watson Health Core

Условията за употреба ("УУ") се състоят от настоящите Условия за употреба на IBM – Специфични условия на офертата SaaS ("Специфични условия на офертата SaaS") и документ със заглавието Условия за употреба на IBM – Общи условия ("Общи условия"), достъпен на следния URL адрес: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

В случай на противоречие, Специфичните условия на офертата SaaS имат предимство пред Общите условия. Чрез поръчване, осъществяване на достъп или използване на IBM SaaS Клиентът се съгласява с тези Условия за употреба.

Условията за употреба (УУ) се регулират от Международния договор на IBM за Passport Advantage, Международния договор на IBM за Passport Advantage Express или Международния договор на IBM за избрани IBM SaaS оферти, както е приложимо ("Договор") и заедно с Условията за употреба (УУ) съставляват пълният договор.

1. IBM SaaS

Следните IBM SaaS оферти са предмет на тези Специфични условия за оферта SaaS:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Метрики за фактуриране

IBM SaaS се продава при една от следните метрики за фактуриране, както е указано в Документа по сделката:

a. **Достъп** – е единица-мярка, чрез която IBM SaaS може да бъде придобит. Достъпът представлява правата за използване на IBM SaaS. Клиентът трябва да получи единично Пълномощие за достъп, за да използва IBM SaaS по време на измервателния период, указан в Лицензионния сертификат (ЛС) или Документа по сделката на Клиента.

b. **Индивид** – е единица-мярка, чрез която IBM SaaS може да бъде придобит. Индивид може да бъде отделен предмет или лице. Трябва да бъде получен достатъчен брой пълномощия, за да се покрие всеки Индивид, обработена или управляване от IBM SaaS пред периода на измерване, посочен в Лицензионния сертификат на Клиента или в Документа по сделката.

   За целите на този IBM SaaS, Индивид включва лице, устройство или мобилно приложение, чиито данни се управляват от IBM SaaS.

c. **Потребителски модел** – е единица мярка, чрез която IBM SaaS може да бъде придобит. Потребителски модел представлява достъп до специфична конфигурация на IBM SaaS. Трябва да бъдат получени достатъчно пълномощия за всеки потребителски модел на IBM SaaS, наличен за достъп и употреба по време на измервателния период, указан в Лицензионния сертификат (ЛС) или Документа по сделката.

3. Цени и фактуриране

Платимата сума за IBM SaaS е указана в Документа по сделката.

3.1 Частични месечни цени

Частична месечна цена, както е указано в Документа по сделката, може да бъде определена по размер на пропорционална база.

3.2 Цени за надвишаване

Ако действителната употреба от страна на Клиента на IBM SaaS по време на измервателния период надвишава пълномощието, посочено в Лицензионния сертификат, тогава на Клиента ще бъде издавана фактурира за надвишаването, както е посочено в Документа по сделката.

4. Опции за срокове и подновяване

Срокът на IBM SaaS започва на датата, на която IBM извести Клиента, че му е предоставен достъп до пилотната оперативна среда на IBM SaaS, както е описано в Документа за поръчка. Абонаментният период за отделните пълномощия започва, когато IBM извести Клиента, че му е предоставен достъп до производствената оперативна среда. Документът за поръчка ще укаже дали IBM SaaS ще бъде подновен автоматично, ще продължи непрекъснато или ще бъде прекратен в края на периода.

За автоматично подновяване, освен ако Клиентът не предостави писмено известие да не се подновява поне 90 дни преди датата на изтичане на срока, IBM SaaS автоматично ще се поднови за срока, посочен в Лицензионния сертификат.

За дългосрочна употреба, IBM SaaS ще продължи да бъде достъпен на базата месец за месец, докато Клиентът не предостави писмено 90-дневно предизвестие за прекратяване. IBM SaaS ще остане достъпен до края на календарния месец след този 90-дневен срок.

5. Техническа поддръжка

IBM ще предостави Наръчника за поддръжка на IBM Софтуер като услуга, който предоставя информация за контакт за техническа поддръжка, време за поддръжка и друга информация и процеси. Информация за контакти за техническа поддръжка и други подробности по отношение на операциите по поддръжка могат да бъдат намерени на: Наръчник за поддръжка на IBM SaaS: https://support.ibmcloud.com.

Техническата поддръжка и простите конфигурационни заявки за IBM SaaS се предоставят чрез електронно подаване. Техническата поддръжка се предлага заедно с IBM SaaS и не е достъпна като отделна оферта.

В документацията или информацията при докладването на проблем не трябва да се включват лична информация (PI), включително защитена здравна информация (PHI) и чувствителна лична информация (SPI).

6. Определения

Приложимо законодателство – означава всички закони, законодателни актове или укази, правила, разпоредби, наредби мандати, декрети или други изисквания, издадени от правителствен орган или общопризнати индустриални стандарти, които са приложими за изпълнението на тези Условия за употреба

API – означава интерфейс на приложна програма, който представлява набор от рутинни процедури, протоколи и инструменти за изграждане на софтуерни приложения. API указва как софтуерните компоненти трябва да си взаимодействат и API се използват при програмирането на компоненти на графичен потребителски интерфейс (GUI).

Оторизиран администратор – представлява служител на Клиент, одобрен доставчик на Клиент, отделно лице или група, отговорни за управление на поддържането и надеждното функциониране на платформата. Отговорностите могат да включват конфигуриране, поддръжка и управление на потребители и акаунти. Администраторът може също така да бъде клиничен изследовател, отговорен за създаване на проучване в здравната система Watson.

Оторизирано лице – представлява всяко разпознато лице, мобилно приложение или устройство, на което е предоставени права за достъп за изпращане на данни до Watson Health Core. Това може да включва Клиента; или участници в изследвания, клиенти или пациенти на Клиенти.

Законодателство, приложимо за данните на Клиента – означава законодателството по отношение на данните, приложимо за изпълнението на задълженията на Клиента по Договора, Свързани документи и приложими Описания на услуги, Документи за поръчка и Поръчки за/Предмет на работа между страните.

Данни на Клиента – означават всички въведени данни в IBM SaaS от или за Клиента, без значение дали тези данни са собствени данни на Клиента или данни, въведени от името или за сметка на клиент на Клиента или трета страна и включително всички данни от устройство на трета страна за наблюдение на здравно състояние.

Законодателство, свързано с данните – означава всички приложими закони, които са свързани със защита на данните, поверителност или сигурност.

Обект на данни – означава идентифицирано лице или лице, което може да се идентифицира, за което се отнасят Личните данни.

Обозначен център за данни – означава център за данни, указан в Документа по сделката като първичен център и център за възстановяване на данни след срив, който работи на потребителски модел на IBM SaaS на Клиента, ако е приложимо.

Здравни данни – означават всички данни или информация, включително изображения, които представляват Лична информация, свързана със здравно състояние.

Активирани здравни данни – по отношение на IBM SaaS означава възможността на IBM SaaS да отговори на приложимите стандарти, закони и наредби за защита и поверителност в областите на управление на здравните данни, включително въвеждането на спецификации, изложени в част 164, подчасти A и C на разпоредбите прилагащи HIPAA (както са изменени от HITECH Act) и други приложими закони, свързани със Здравните данни, но това не означава, че IBM действа в ролята си на Бизнес сътрудник или Администратор на данни.

HIPAA – означава Закон за преносимост и отчетност на здравните осигуровки от 1996 г., изменен, включващ от Закона за здравните информационни технологии за икономическо и клинично здраве на Закона за американско възстановяване и реинвестиране от 2009 г. ("HITECH Act"), определени разпоредби, обнародвани в съответствие с HIPAA от Министерството на здравеопазването и социалната политика на САЩ в 45 C.F.R. Части 160 и 164, и определени наредби, обнародвани съгласно закон HITECH.

Законодателство, приложимо за данните на IBM – означава законодателството по отношение на данните, приложимо за изпълнението на задълженията на IBM по Договора, Свързани документи и приложими Описания на услуги, Документи за поръчка и Поръчки за/Предмет на работа между страните.

Персонал на IBM – означава (a) IBM, неговите филиали и неговите изпълнители, и по отношение на горепосоченото, неговите служители; и (b) доставчици на трети страни; във всеки случай лицата, които изпълняват услугите от името на IBM съгласно Договора и приложимите Свързани документи или за които IBM по друг начин предостави достъп до Личните данни на Клиента.

Държави в областта на действие – означава 28-те държави-членки на Европейския съюз и Швейцария и държавите, които IBM може да добавя към този списък от време на време.

Лични данни или **Лична информация** – означава информация във всеки тип средство или формат, включително електронни и хартиени досиета, която е свързана с идентифицирано лице или лице, което може да се идентифицира, като "лице, което може да се идентифицира" е лице, което може да се идентифицира пряко или непряко, по-конкретно чрез референция към идентификационен номер или един или повече фактори, специфични за неговата/нейната физическа, физиологическа, психична, икономическа, културна или социална идентичност.

Обработка и варианти от него, например **обработване** (с или без обозначаване с главна буква) – означава всяка операция или набор от операции, които се извършват върху данни, автоматично или не, например събиране, записване, организиране, съхранение, адаптиране или промяна, извличане, консултиране, използване, разкриване чрез предаване, разпространение или по друг начин предоставяне, присъединяване или комбиниране, блокиране, изтриване или унищожаване.

Обработени данни – означават всички данни, поверителни или собствена информация или материали, включително Здравни данни и Лични данни, които се обработват от IBM съгласно Договора, Свързан документ и/или Описание на услуга, Документ за поръчка, и/или Поръчка за/Предмет на работа.

Инцидент, свързан със сигурността – има значението, изложено в SBCA.

7. Управление на акаунт

IBM SaaS е достъпен само за оторизираните потребители на Клиента ("**Оторизирани администратори**" или "**Оторизирани лица**"). Клиентът ще извършва контрол върху оторизираните акаунти с цел осъществяване на достъп до IBM SaaS, което може да включва оторизирани приложения, персонал на Клиента, трети страни-доставчици на услуги и изпълнители на Клиента, и носи единствен отговорност за (i) осъществяване на контрол върху всички оторизирани потребители, включително без ограничение, проверка на идентичността на всеки оторизиран потребител; и (ii) уверяване, че само оторизирани потребители осъществяват достъп до IBM SaaS.

Оторизираните лица, които са клиенти, пациенти или участници в изследвания на Клиента ще получат достъп единствено за целите по качване на данни в IBM SaaS, в който случай тези Оторизирани лица няма да имат друг достъп до IBM SaaS.

8. Поверителност

8.1 Общи изисквания

Между Страните, Клиентът е единственият администратор на всички Лични данни на Клиента и Клиентът посочва IBM като обработващ данните. В съответствие с приложимото законодателство относно данните, Клиентът има правото да инструктира IBM във връзка с обработването от страна на IBM на Лични данни на Клиенти.

До степента, до която IBM обработва Лични данни на Клиента, IBM:

a. ще спазва всички приложими закони, свързани с данни на IBM; и

b. няма да смесва Лични данни на Клиента с данни от други източници с изключение:

- ако това е необходимо за предоставяне на IBM SaaS и след това за никаква друга цел освен конкретно посочената от Клиента; или
- в съответствие с условията на тези Условия за употреба и Приложението SBCA.

До степента, до която IBM обработва Лични данни на Клиента, Клиентът:

a. ще спазва всички приложими закони, свързани с данни на Клиента;

b. ще носи отговорност за всички комуникации от Клиента с неговите филиали, пациенти, крайни потребители, обекти на данни и/или други трети страни на Клиента;

c. ще сключи споразумения за обработка на данни със своите администратори, от които се изисква да позволят на IBM като обработващ данни и на неговите подобработващи да обработват всички Лични данни на Клиента; и

d. ще служи като единствено лице за контакт за IBM и носи единствен отговорност за вътрешната координация, преглед и предаване на инструкции или заявки от филиалите на Клиента, които са други администратори по отношение на IBM. IBM ще бъде освободен от задължението да информира или известява филиал на Клиента, който представлява администратор, ако е предоставил подобна информация или известие на Клиента. IBM има право да откаже инструкции, предоставени директно от филиал на Клиента, който е администратор, но не е Клиента.

Никоя от страните няма да действа в нарушение на приложимите закони, свързани с данните, важащи за тази страна.

8.2 Права, свързани с клиентски данни

Клиентът представя и гарантира, че (a) притежава данните, които ще въведе в IBM SaaS, или (b) че е получил и носи отговорност за поддържането на всички права, позволения, съгласия и оторизации, за да предостави на IBM правата за достъп, използване и разкриване на Клиентски данни в съответствие с условията, посочени в тези Условия за употреба или във Договора, или ако е необходимо по друг начин за IBM за предоставяне на IBM SaaS. Освен това Клиентът представя и гарантира, че Клиентските данни ще бъдат (a) или свързани само лица, пребиваващи в САЩ и след това ще бъдат въведени в IBM SaaS в център за данни в САЩ, или (b) свързани с лица, пребиваващи в една или повече от държавите от областите на управление и ще бъдат въведени в IBM SaaS само в Посочените центрове за данни.

8.3 Услуги, свързани с данни, и отговорности

a. Клиентът се съгласява, че ще извършва анализи или ще заяви IBM да извършва анализи по Клиентските данни във връзка с дейностите, които съставляват "операции по здравни грижи" или "изследвания" на Клиента, както са определени съгласно HIPAA и/или подобни условия по други приложими за данните закони, и че Клиентът ще използва Клиентските данни или ще нареди на IBM да използва Клиентските данни само в съответствие с всички свързани изисквания (напр. определяне на Институционален ревизиращ борд или отказ от право, където е необходимо) съгласно тези или други приложими закони за данните на Клиента.

b. Клиентът е единствено отговорен да си набави всички регистрации, съгласия, оторизации и разрешения, както се изисква съгласно приложимите за Клиента закони във всяка държава от областите на управление, включително, но без ограничение, HIPAA и други приложими закони, правила и наредби, свързани с поверителност и защита на данни, за да могат Клиентските данни да бъдат въведени в IBM SaaS и използвани и планирано разкривани съгласно тези Условия за употреба, и Договора с Клиента и от IBM и разрешените изпълнители на IBM. IBM няма да носи отговорност за наблюдение дали подобни регистрации, съгласия, оторизации и разрешения са получени или необходими.

c. Клиентът е единствен отговорен за гарантирането, че всички Клиентски данни, въведени в IBM SaaS са ограничени само до данните, свързани с отделните лица, пребиваващи в САЩ или в държава от областите на управление.

d. IBM няма да поддържа центрове с персонал, обучен по HIPAA и други приложими закони, свързани с данни на IBM по отношение на данните от държавите от областите на управление.

8.4 Мерки за сигурност и инциденти, свързани със сигурността

a. IBM ще въведе, поддържа и спазва техническите и организационни мерки, включително организационните процеси и процедури и всички специфични задължения, свързани със сигурността, изложени или посочени в тези Условия за употреба и SBCA, с цел защита на Личните данни на Клиента от неоторизирана употреба или достъп, случайна загуба, повреда, промяна, унищожаване, кражба или неоторизирано разкриване.

b. В случай че IBM научи за инцидент, свързан със сигурността (както е определено от SBCA), включващ Обработени данни на Клиент, IBM ще информира Клиента в съответствие с условията на SBCA и приложимите закони за данни на IBM, а подобно известяване ще включва информация относно всяко възможно въздействие върху Клиента или обекти на данни (ако има такива), засегнати от този инцидент, свързан със сигурността, и ще бъдат предприети или предложени корективни действия, които да бъдат предприети от IBM.

8.5 Получаване на запитвания и оплаквания

IBM ще извести Клиента писмено и навременно и до степента, позволена от приложимите за IBM закони, свързани с данните, не по-късно от пет (5) работни дни след получаването на запитването, съобщението или оплакването на служителя по поверителност на данните в IBM Watson Health от IBM във връзка с Личните данни на Клиента от:

a. всеки обект на данни, свързан с Личните данни относно подобен обект на данни, обработван от IBM. Клиентът ще отговори на подобни заявки от обектите за данни и IBM ще спази разумните инструкции на Клиента при оказването на съдействие за Клиента при отговаряне на тези заявки. Ако се изисква съгласно приложимите за IBM закони, IBM може да отговори директно на подобни заявки, при положение че IBM извести Клиента предварително за това и разумно си сътрудничи с Клиента по отношение на формата и съдържанието на тоиз отговор, когато това е позволено съгласно приложимите за IBM закони или по друг начин, както е възможно;

b. всяки юридическо лице и регулаторен орган, свързани с обработката от страна на IBM на Лични данни на Клиента, при положение че IBM може да отговори на подобни заявки, получени от правителствена агенция чрез призовка или подобен законен документ, налагащ разкриване от IBM или по друг начин изискан съгласно приложими закони, свързани с данните, при положение че IBM извести Клиента предварително за подобно разкриване и разумно си сътрудничи с Клиента по отношение на формата и съдържанието на този отговор, където е това е позволено от закона или по друг начин възможно.

8.6 Обработване на Лични данни на Клиент

IBM ще ограничи разкриването на Лични данни на Клиента само до персонала на IBM, който може да се наложи да съдейства при предоставянето на Услугите.

IBM ще отговори на всяка разумна заявка, получена от Клиента и изискваща IBM да промени, коригира, изтрие или блокира Лични данни на Клиента в съответствие с приложимото законодателство.

При заявка от една от страните, IBM, Клиентът или техните филиали ще сключат стандартни споразумения, изисквани от закона, с цел защита на Личните данни на Клиента. Страните се

съгласяват (и ще се погрижат техните съответни филиали да се съгласят също), че подобни споразумения ще бъдат предмет на ограничения и изключения по отношение на отговорността по този Договор във връзка с претенции между страните. Страните ще си сътрудничат при сключването (или ще се погрижат съответните им филиали да сключат) и при спазването на взаимно договорените условия или споразумения, което може да се изисква съгласно приложимите закони, свързани с данни.

8.7 Връщане на Лични данни на Клиент

При изтичане или прекратяване на Договора, IBM ще спре да използва и ще изиска целият персонал на IBM да спре да използва или обработва Собствена информация на Клиента и Лични данни на Клиента, при възможността за тази опция от Клиента и при негова заявка:

a. навременно връщане във формат и на носител за съхранение, който Клиентът разумно изиска, на пълната собствена информация и Лични данни на Клиента, които IBM съхранява в електронен вид и при потвърждаване от страна на Клиента на получаването, ще изтрие, унищожи или по друг начин направи трайно нечетливи или не дешифриращи се собствената информация и Личните данни на Клиента, включително копия и архиви. IBM може да таксува цена за медийния носител за съхранение и за определени дейности, извършени по заявка на Клиента (например доставяне на собствената информация и Личните данни на Клиента в определен формат или тяхното унищожаване по конкретен начин); и

b. директно изтриване и унищожаване или по друг начин трансформирането на собствената информация и Личните данни на Клиента в нечетливи или не дешифриращи се, включително копия и архиви.

8.8 Споразумение с бизнес сътрудник

До подходяща степен и както се изисква от HIPAA, IBM и Клиента ще сключат Споразумение за с бизнес сътрудник ("BAA"), което ще регулира задълженията на IBM като бизнес сътрудник на Клиента при предоставянето на IBM SaaS. Без ограничаване на изричните задължения на IBM по Договора и BAA, ако е приложимо, Клиентът приема и се съгласява, че носи отговорност за определяне на приложимостта и за спазването на всички приложими закони и изисквания за лицензиране, които се прилагат спрямо употребата от страна на Клиента, както и други дейности във връзка с IBM SaaS (включително употреба или други дейности от Оторизираните потребители).

8.9 Допълнение относно обработването на данни в Европейския съюз

Ако Клиентът установи, че IBM обработва Лични данни в рамките на Европейския съюз, IBM и Клиентът ще сключат Допълнение по отношение на обработването на данни, включващо, ако е приложимо, примерните клаузи на ЕС, като опционалните клаузи бъдат премахнати.

9. Допълнителни условия на офертата IBM SaaS

9.1 Защита

Този IBM следва принципите на IBM за защита и поверителност на данните за IBM SaaS, които са налични на http://www.ibm.com/cloud/data-security, както и допълнителните условия, изложени по-долу и в Допълнението по отношение на защитата и непрекъснатост на бизнес процесите към тези Условия за употреба. Всяка промяна по принципите за защита и поверителност на данните на IBM няма да наруши качеството на защитата на IBM SaaS.

IBM Watson Health Core прилага политики за защита, стандарти и процеси, базирани на ISO 27001 рамката, както са описани допълнително в Описанието за защита. Освен възможностите за защита, решението прилага следното:

a. Сигурни оперативни зони

   IBM Watson Health Core прилага задълбочена стратегия за защита, използваща множество защитени зони за управление на точките на интегриране на облака, например добавяне на данни и разработване на персонализирани приложения.

b. шифроване

   Всички клиентски данни се шифроват както при работа с тях, така и при неизползване. Всички данни, преминаващи от и към IBM Watson Health Core, се шифроват. Споделената услуга предоставя управление чрез ключове за шифроване. Клиентът носи отговорност за

цялата мрежова свързаност и качеството между услугата на IBM Watson Health и прокси сървъра на Клиента.

c. Наблюдение на събитие за защита

IBM използва своята платформа за наблюдение на защитата за управление на информация и събития за защита, управление на журнали, проучвания на инциденти, засичане на заплахи и управление на уязвимостта.

d. Управление на самоличност

- Watson Health Core поддържа открити стандарти по отношение на идентичността на доставчиците за мащабни групи от пациенти и потребители, като използва OpenID Connect.
- За потребителски групи, при които IBM е доставчикът на идентичност, Watson Health Core използва подходящите възможности за услугите по управление на директории и идентичност, за да се справя с процесите по разпознаване.

e. Сигурно разпознаване и достъп въз основа на роли

- Watson Health Core поддържа разпознаване посредством SAML като механизъм за Клиентите за интегриране на опцията за единично влизане (SSO) или услуги за директории.
- Watson Health Core използва решение за управление на достъпа и свързани компоненти за управление на политиките по защита, където това се изисква.
- Watson Health Core поддържа софтуерно двуфакторно разпознаване.
- Watson Health Core предоставя основен контрол на достъпа, базиран на роли, както се изисква; Watson Health Core поддържа конфигурация за проучване, потребителски профили, роли и потребителски групи чрез програмиращи интерфейси на програмните приложения ("API"), които позволяват достъп въз основа на дадена роля.

9.2 Бисквитки

Клиентът е наясно и се съгласява, че IBM може като част от нормалната работа и поддръжка на IBM SaaS да събира лична информация от Клиента (Вашите служители и изпълнители), свързана с употребата на IBM SaaS чрез проследяване и други технологии. IBM прави това, за да натрупва статистика за потребление и информация относно ефективността на нашия IBM SaaS с цел подобряване на практическата работа на потребителите и/или персонализиране на взаимодействията с Клиента. Клиентът потвърждава, че ще получи или е получил съгласие за позволяване на IBM да обработва събраната лична информация за горепосочената цел в рамките на IBM, други компании на IBM и техните подизпълнители, независимо от мястото, на което ние или нашите подизпълнители осъществяваме стопанска дейност, в съответствие с приложимия закон. IBM ще се съобрази със заявките от служителите и подизпълнителите на Клиента за достъп, обновяване, поправяне или изтриване на тяхната събрана лична информация.

9.3 Местоположения на извлечени ползи

Когато е приложимо, се начисляват данъци въз основа на местоположенията, които Клиентът идентифицира като такива за извличане на ползи от IBM SaaS. IBM ще начисли данъци въз основа на бизнес адреса, посочен при поръчването на IBM SaaS като основното местоположение за извличане на полза, освен ако Клиентът не предостави на IBM допълнителна информация. Клиентът е задължен да поддържа тази информация актуална и да информира IBM за всички промени.

9.4 Непрекъснато осигуряване

Клиентът има право на възможности и подобрения, направени по решението и внедрявани от IBM в модел от непрекъснато осигуряване в облака.

9.5 Архивиране и възстановяване

IBM Watson Health Core предоставя архивиране на Клиентски данни в производствената среда (включително хранилищата Data Lake и Data Reservoir) към момента на последното добро състояние, с цел възстановяване на услугата в случай на срив на системата.

9.6 Висока достъпност

IBM Watson Health Core компонентите в производствената среда се въвеждат в конфигурации на висока достъпност, с клъстеризирани сървъри на бази данни за дублиране, с цел предоставяне на разпределение на натоварванията и елиминиране на единични сривове.

9.7 Възстановяване след срив

Подходът на IBM за възстановяване след срив се състои от множество центрове за данни в разпръснати в географско отношение зони за постигане на целите по непрекъснатост на бизнес процесите за производствената среда, както следва:

- RTO – в рамките на 36 часа след декларирането на срив
- RPO – не повече от 24 часа след загуба на съдържание на Клиента

9.8 Инструменти за измерване

IBM SaaS използва синтетично решение за наблюдение, измерване и докладване относно достъпност и прекъсвания спрямо приложените нива на обслужване. Това решение симулира и проследява потребителските реакции и потребителския опит на глобално равнище – както за статична достъпност, така и за транзакции.

IBM SaaS също така използва вътрешна система за наблюдение за метрика, събития и сигнализиране в цялото решение.

9.9 Публичност

Клиентът се съгласява, че IBM може публично да посочи Клиента като абонат на IBM SaaS в обществено или маркетинг съобщение.

Приложение A

1. IBM Watson Health Core

IBM Watson Health Core е платформа за здравни данни като услуга (PaaS), платформа за разработки и оперативна подсреда за съхраняване, комбиниране и обработване на Защитена здравна информация (PHI), както е определено от HIPAA, и други Здравни данни, в съответствие с приложимите за IBM закони относно данните, намираща се в притежаван и контролиран от IBM център за данни. Клиентът трябва да се сдобие с подходящите пълномощия за IBM Watson Health Core и IBM Watson Health Core Access, за да позволи характеристиките и възможностите, описани по-долу.

1.1 Оперативни среди на Watson Health Core

Пълномощието за Watson Health Core се състои от три оперативни среди в облак за здравните данни, проектирани да позволят на Клиента да обработва здравни данни:

- Пилотна среда

  Предоставя ограничена среда, където Клиентите могат да разработват и тестват приложения, изградени с помощта на IBM SaaS. Пилотната среда въвежда всички контролни мерки за защита на HIPAA с изключение на възстановяване след срив, висока достъпност и архивиране на системите за записи.

- Производствена среда

  Предоставя пълномащабна среда, където Клиентите могат да внедряват потоци от здравни данни. Производствената среда е високодостъпна, балансиране среда за зареждане и може да бъде преместена при отказ до местоположение за възстановяване след срив.

- Възстановяване след срив

  Предоставя огледално копие на производствената среда; и се намира на отделно местоположение в център за данни.

1.2 Разработване на приложения

IBM Watson Health Core позволява разработване на приложения и защита на колекции от данни от устройствата на Клиента или устройствата на оторизираните потребители на Клиента. API предоставят програмни интерфейси и документация, които оторизираните потребители на Клиента, включително трети страни-доставчици на услуги на Клиента могат да използват за разработване на приложения и за обмен на данни с IBM SaaS. Използването на API от Клиента или неговите разработчици е предмет на съответствие с изискванията за разработчици на API.

- REST API

  Watson Health Core предоставя серия от REST API и услуги за платформата Watson Health Core. Възможностите на API включват, но не са ограничени само до, механизми за осъществяване на достъп до хранилищата за данни, услуги по комбиниране на данни, управление на потребители и журнали от одити.

- Apple HealthKit и Apple ResearchKit

  Watson Health Core поддържа интегрирането с рамката Apple ResearchKit API за iOS въз основа на изследователски проучвания и с Apple HealthKit за прихващане на данни относно състояние.

1.3 Управление на данни

- Управление на съгласие

  Watson Health Core предоставя рамка за събиране на съгласие, предоставена от пациенти или участници в изследвания и може защитено да съхранява записи на съгласие, отделно от данните, когато лицето се впише в приложение на Клиента, изискващо предоставянето на съгласие.

- Маскиране на данни

  Watson Health Core предоставя възможността за разделяне на идентификаторите за имена от структурираните данни. Watson Health Core получава данните в облака посредством програмни API. API позволяват разделянето на идентификаторите за пациент и личното име от останалите данни, които да бъдат съхранени в отделно шифровано хранилище за данни. Към данните се приписва анонимен токен, който може да бъде използван при бъдещото проследяване на произход.

1.4 Услуги, свързани със здравни данни

Watson Health Core осигурява събиране, съхранение, синхронизиране на данни, включително екзогенни здравни данни или друга Лична информация, както в структуриран, така и в неструктуриран вид.

- Поемане на данни

  Watson Health Core предоставя възможността за поемане на данни от приложения или устройства на пациенти посредством програмни API. Watson Health Core предоставя право на всяко от оторизираните лица на Клиента да качва до 25 MB данни в Health Core през всяка година от договорния срок. Услугата може да поеме до 10 броя качвания за лице на ден.

- Оперативно езеро от данни

  Необработените данни на Клиент или на пациент се съхраняват в Watson Health Core в тяхната първоначална форма, докато това е необходимо за анализиране и моделиране.

- Зареждане на трансформирани извадки (ETL)

  Данните се трансформират в нормален формат за операционната подсистема. Базирана на индустриалните стандарти шина за корпоративни услуги за здравни учреждения позволява интегрирането сред различните приложения и протоколи на Клиента.

- Data Reservoir

  След бъдат комбинирани, данните се преместват в Data Reservoir. Watson Health Core използва аспектите на унифицирания модел за данни на IBM за здравеопазването, за да нормализира бизнес данни и технически данни в областта на здравеопазването, за да се използват в анализи.

- Индекс Master Person

  Watson Health предоставя инструменти за управление на основни данни с цел консолидирането на данни от множество източници, с цел създаване на Longitudinal Person Record (LPR).

2. Опционални характеристики

2.1 IBM Watson Health Core Terminology Service

Тази добавена услуга улеснява интегрирането на данни и интероперативността между отделните здравни системи, като предоставя съгласувано използване на клинична терминология сред всички приложения на Watson Health Cloud. Тази услуга предоставя функционалната платформа за всички задачи, включително терминологии, кодови системи и структурирано съдържание, например:

- създаване на нови кодови системи;
- превод на международни кодови системи; и
- преобразуване между местните кодови списъци и международните стандарти.

Приложение Б

IBM предоставя следното Споразумение за ниво на обслужване ("СНО") за достъпност за IBM SaaS, както е указано в Лицензионния сертификат на Клиента. СНО не представлява гаранция. Споразумението за ниво на обслужване е достъпно само за Клиента и се прилага само за употреба в производствени среди.

1. Кредити за достъпност

Отстъпките, свързани с достъпност са приложими само до степента на абонаментните такси за пълномощията за отделните лица.

Клиентът трябва да подаде към помощния център за техническа поддръжка на IBM билет за поддръжка с Ниво на сериозност 1 в рамките на 24 часа след първото узнаване, че дадено събитие е имало ефект върху достъпността на IBM SaaS. Клиентът трябва да подпомогне IBM при всяка диагностика и разрешаване на даден проблем.

Претенция за билет за поддръжка при неуспех за спазването на Споразумението за ниво на обслужване трябва да бъде подадена в рамките на три работни дни след края на договорния месец. Компенсация за валиден иск спрямо Споразумението за ниво на обслужване ще бъде кредит за бъдеща фактура за IBM SaaS, въз основа на времетраенето, по време на което обработката на работната система за IBM SaaS не е достъпна ("Престой"). Престоят се измерва от момента, в който Клиентът докладва събитието, до момента, в който IBM SaaS е възстановен и не включва време, свързано с планирано или оповестено прекъсване на работата поради профилактика; причини извън контрола на IBM; проблеми със съдържание или технология, дизайни или инструкции на Клиента или трета страна; неподдържани системи конфигурации и платформи или други грешки на Клиента; или причинен от Клиента инцидент със сигурността или тестване на сигурността от Клиента. IBM ще приложи най-високата приложима компенсация, въз основа на кумулативната достъпност на IBM SaaS през всеки договорен месец, както е показано в таблицата по-долу. Общата компенсация по отношение на даден договорен месец не може да надвишава 20 процента от една дванадесета (1/12) от годишната такса за IBM SaaS.

2. Нива на обслужване

Достъпност на IBM SaaS през даден договорен месец

Достъпност по време на договорен месец	**Компенсация (% от месечната абонаментна цена* за договорен месец, който е предмет на претенцията)**
< 99,95%	10%
< 99,0%	20%

* Ако IBM SaaS е бил придобит от Бизнес партньор на IBM, месечната абонаментна такса ще се изчисли спрямо актуалния към момента ценоразпис за IBM SaaS, който е в сила за договорния месец, който е предмет на претенцията, с отстъпка в размер на 50%. IBM ще предостави на Клиента директна отстъпка.

Достъпността, изразена като процент, се изчислява като: общ брой минути в договорен месец минус общ брой минути престой в договорен месец, разделено на общ брой минути в договорния месец.

Пример: 108 минути общ Престой през договорен месец

Общо 43 200 минути в Договорен месец с 30 дни - 108 минути Престой = 43,092 минути _____ 43 200 общо минути	= 10% кредит за достъпност за 99.75% достъпност през договорен месец

3. Изключения

Това Споразумение за ниво на обслужване не се прилага при следните:

- Отделно от наблюдението на сървъри, СНО не се прилага за хоствани виртуални машини за поддръжка на потребителски или клиентски приложения.
- Ако Клиентът е нарушил съществено задължение по настоящия Договор.

Приложение C

Това приложение за защита и непрекъснатост на бизнес процесите (това "SBCA") налага известни изисквания и задължения за IBM при предоставянето на IBM SaaS за Клиента. Изискванията и задълженията, посочени тук, са в допълнение на изложените в описанието на принципите за защита на данните за IBM SaaS, които са достъпни на http://www.ibm.com/cloud/data-security. Понятията, посочени с главни букви, които не са определени тук, ще имат значението, посочено в Договора или в Условията за употреба.

1. Програма за защита на информацията

IBM има въведени вътрешни политики за защита, стандарти и процеси, базирани на рамката ISO 27001 и области на контрол. В допълнение към управлението на IBM Corporate Security Organization, тези политики, стандарти и процеси редовно подлежат на вътрешни одити.

IBM поддържа програма за защита на информацията от организационни, оперативни, административни, физически и технически мерки за защита, регулираща обработването, съхранението и предаването на съдържание на Клиента, които са съгласувани най-малко с изискванията на това SBCA.

IBM ще сподели с Клиента по негова заявка, информация относно програмата за защита на информацията IBM Watson Health, така че Клиентът да може разумно да определи нейната непрекъсната годност, адекватност и ефективност. Програмата за защита на информацията IBM Watson Health ще бъде актуализирана от време на време, за да бъде поддържана актуална с общоприети индустриални практики и приложимите за IBM закони.

2. Средства за контрол на достъпа

IBM ще разкрие съдържанието на Клиента само пред своите служители, изпълнители или трети страни, които имат доказана законно необходимост във връзка със своя бизнес да осъществяват достъп до съдържанието на Клиента, за да се подпомогне IBM при изпълняването на задълженията пред Клиента, или други лица, ако е необходимо, за осигуряването на IBM SaaS в съответствие с приложимото законодателство, Договора или Свързан документ, ако е приложимо. В случай че IBM е Бизнес сътрудник на Клиента, IBM и Клиентът ще разкрият Личната здравна информация само в съответствие с условията на приложимото споразумение с бизнес сътрудник, сключено между страните.

IBM има въведен процес по формално управление на достъпа на вътрешните потребители, при който достъпът на потребителите се заявява официално, одобрява се след проверка на идентичността и се предоставя на информативна база, като използва концепцията за най-ниски привилегии. Достъпът до съдържанието на Клиента ще бъде ограничено само до активните потребители и активните потребителски акаунти. IBM има въведен формален процес за периодично повторно валидиране на вътрешния достъп за активните потребителски акаунти.

IBM използва защитени протоколи за разпознаване на потребители, включително приписване на уникални идентификатори и сигурни пароли за активните потребителски акаунти в системите, използване за предоставяне на услуги на Клиента в съответствие с корпоративните стандарти и политики за сигурност на IBM:

a. Паролите няма да бъдат пароли по подразбиране, предоставяни от доставчиците, и ще бъдат съхранявани на местоположение и/или във формат, който няма да застраши сигурността на данните, която те защитават.

b. Изобразяването и отпечатването на пароли трябва да бъде маскирано, премахнато или по друг начин възпрепятствано, за да не могат неоторизирани страни да ги видят и впоследствие възпроизведат. Паролите не трябва да бъдат завеждани или съхранявани при тяхното въвеждане. Потребителските пароли не трябва да бъдат съхранявани като текст.

c. Паролите за всяка технология, обхващащи IBM SaaS, са избрани така, че да намаляват рисковете, свързани с известни уязвимости по отношение на дължината на паролите, и трябва да бъдат документирани.

d. Когато се изисква използването на вътрешни, привилигировани, споделени функционални идентификатори поради оперативни причини, IBM управлява споделените, функционални и/или системни идентификатори, изискващи изписване на пароли за поддържане на отделна отчетност.

Настъпва таймаут поради неактивност за всички системи и приложения, които съхраняват съдържание на Клиента.

Ако е необходимо, ще бъде установен отдалечен достъп до мрежата, системите и приложенията на IBM, които съхраняват съдържание на Клиента, при заявка за това от Клиента и при официалното одобрение от страна на IBM, а всички отдалечени свързвания ще бъдат защитени чрез сигурни протоколи за разпознаване и шифроване. Активността по отдалечен достъп трябва да бъде регистрирана и наблюдавана.

До степента, до която осигуряването на IBM SaaS налага на IBM да използва отдалечен достъп до система в рамките на вътрешните мрежи на Клиента, този отдалечен достъп ще бъде осъществяван единствено като се ползват защитените системи и протоколи за отдалечен достъп на Клиента и като се ползват идентификационните данни за достъп, предоставени на IBM от Клиента. Отдалеченият достъп до мрежата на Клиента ще бъде осъществяван само при заявка от IBM и одобрението на Клиента, и в съответствието с актуалните към момента политики на Клиента, които ще бъдат предоставени предварително на IBM. Използването от страна на IBM на вътрешните мрежи на Клиента ще бъде предмет на политиките на Клиента, свързани с използването на IT и политиките за защита, които ще бъдат предоставени на IBM предварително.

IBM използва разделяне на задълженията, свързани с администриране на сигурността, преглед на достъпа и проучването на нарушения сигурността.

Съхраняването, хостването и обработването на специфично съдържание на Клиента е логически разделено от това на другите клиенти, обслужвани от IBM. В потребителските модели, където от Клиента е оторизирано споделено хранилище, хостване или обработваща работна площ, IBM ще въведе процедури и стандарти, съгласувани с изискванията, посочени в това SBCA, които са предназначени да предотвратят неоторизирано разкриване на съдържание на Клиента.

IBM прилага политики за изчистване на работната площ/екран, за да се увери, че съдържанието на Клиента в никакъв случай не е оставено без надзор на публично място.

3. Прехвърляне и шифроване

IBM ще предприеме необходимите мерки при прехвърлянето на съдържание на Клиента (по факс, имейл, куриер и т.н.), за да се увери, че се използва правилната информация за контакт за получателя, преди да уреди договореностите с въпросния получател за подсигуряване получаването на подобна информация.

IBM използва, и ще наложи на своя персонал да използва, съответните начини за шифроване или други технологии за защита по всяко време, във връзка с обработването на съдържанието на Клиента, включително във връзка с прехвърляне, съобщаване, отдалечен достъп или съхранение (включително архивно съхраняване) на съдържание на Клиента. Например IBM ще шифрова в съответствие с приетите индустриални стандарти всички записи и файлове, съдържащи съдържание на Клиента:

a. съхранени на преносими компютри на IBM, преносими устройства или преносими електронни носители, включително архивни касети, при прехвърлянето във външен обект за съхранение;

b. съхранени или транспортирани от IBM извън физическите защитени офиси на Клиента или на IBM, с изключение на документи, отпечатани на хартия;

c. при преминаването сред публичните мрежи от IBM;

d. при прехвърлянето от системите на IBM към Клиента;

e. при безжичното предаване от IBM; и

f. съхранени от IBM на сървъри и бази данни.

4. Мрежова сигурност

IBM използва разумни и актуални версии на софтуер за защита, например защитни стени, прокси, защитни стени и интерфейси на уеб приложения. Подобен софтуер трябва да включва защита от злонамерен софтуер и разумни и актуални пакети и определения за вируси. В съответствие с корпоративните стандарти, антивирусният софтуер трябва да бъде инсталиран на работни

станции, сървъри и свързани крайни точки, където е технически възможно, и софтуерът се управлява в съответствие с корпоративната политика с вътрешни решения за управление.

IBM наблюдава IBM SaaS, за да открие и идентифицира инциденти, свързани със сигурността, възможно най-скоро. IBM ще поддържа като минимално изискване, индустриални инструменти за засичане и предотвратяване на нарушения, процеси по наблюдение и реагиране, по начин, предназначен да идентифицира както вътрешната, така и външната уязвимост и рискове, които могат да възникнат от неоторизирано разкриване, злоупотреба, промяна или унищожаване на системи за съдържание и информация на Клиента, които се използват за осигуряване на услуги за Клиента.

IBM се абонира за услуги, свързани с проучване на уязвимостта, или за консултации, свързани със сигурността на информацията, както и други свързани източници, предоставящи актуална информация относно уязвимост на системите. IBM извършва редовни оценки на уязвимостта и ще разрешава проблеми по своята мрежа.

IBM наблюдава IBM SaaS, за да засича, идентифицира, изолира и разрешава инциденти, свързани със сигурността.

IBM проверява достъпността, цялостта и ефективността на инфраструктурата за мрежова сигурност, чрез която IBM SaaS се предоставя, чрез процесите по управление на издания на IBM.

5. Управление на инциденти и известия

IBM Watson Health работи в екип в тясна връзка с екипа за реагиране в областта на киберсигурността на IBM, глобален екип, който управлява получаването, проучването и вътрешното координиране на инциденти за сигурност, свързани с офертите на IBM и за въвеждане на превантивни мерки, необходими за намаляване на проблемите, свързани със сигурността на софтуера. "Инцидент, свързан със сигурността" представлява успешно осъществяване на неоторизиран достъп, употреба, разкриване, промяна или взаимодействие с системни операции или данни в дадена информационна система, използвана от IBM за предоставяне на IBM SaaS. Ако е открит инцидент, свързан със сигурността (чрез рутинно сканиране, сигнали, прагови събития и други), IBM ще информира и извести Клиента:

a. относно потвърден инцидент, свързан със сигурността, включващ съдържанието на Клиента, възможно най-бързо и не по-късно от 2 работни дни след проучването и потвърждаването на такъв Инцидента със сигурността;

b. навременно след всяка заявка за достъп до или информация за съдържание на Клиента от държавен служител (включително агенция по защита на данните или агенция за правоприлагане) освен ако това не е забранено по закон или съответна наредба; и

c. с изключение на позволените и посочени в раздел Средства за контрол на достъпа в това SBCA, предварително за всяко разкриване или прехвърляне, или достъп до съдържание на Клиента или от трета страна.

6. Регистриране

IBM поддържа, в съответствие с политиките и практиките на IBM, общоприети индустриални практики, разумно наблюдение на системите за неоторизирана употреба или достъп до данни, обработвани от Клиента. Нарушения на достъпа или опити за такива ще бъдат документирани.

IBM поддържа записи за всички заявки за достъп и журнали от активностите по влизане за всички системи, които съхраняват, осъществяват достъп, обработват или предават данни на Клиента или здравни данни, за колкото време се изисква от HIPAA или съгласно други приложими за IBM закони, свързани с данни.

Журналите и докладите могат да включва като минимално изискване: (i) всички опити за влизане, било то успешни или не, включително идентификационната информация; (ii) всички промени по системни или мрежови конфигурации, включително инсталирания на приложения, промени по управлението на потребители и известия за позволения за достъп до файлове; (iii) опити за достъп до ресурси, било то успешни или не, включително опити за достъп до файлове, споделяния в мрежа, журнали или други ресурси; и (iv) изтегляния на данни, включително типа на съдържанието и протокола за достъп, които са използвани за осъществяването на изтеглянето.

7. Разработване на софтуерни приложения и управление на промените

IBM следва сигурни практики за разработване на приложения и кодиране, които защитават цялостта на производствените приложения и свързания изходен код от неоторизирани и нетествани модификации.

IBM следва процес по управление на промените, който включва (a) записване и формално одобрение на промените и обратни процедури; и (b) подходящо тестване на подобни промени, включително тестване на начина на приемане от страна на потребителите, където е приложимо, както и тестване на сигурността.

IBM следва процес по управление на пакети, който включва тестване на пакети преди инсталация на всички системи, използвани за съхранение, достъп и предаване на съдържание на Клиента или използвани за предоставяне на услуги, включително IBM SaaS, на Клиента.

IBM изисква системните администратори да поддържат пълна, точна и актуализирана информация относно конфигурирането на всички информационни системи, използвани за съхраняване, достъп и предаване на съдържание на Клиента.

8. Физическа сигурност и сигурност на средата

Платформата IBM Watson Health Core е внедрена в инфраструктура за данни IBM SoftLayer. IBM SoftLayer поддържа физическа сигурност и сигурност на среда, контрол на достъпа, средства за контрол и процеси за защита на данните на Клиента от нарушение и влияние от страна на лица, на средата и технически влияния.

Общият достъп до обектите, в които IBM SaaS се хоства, се контролира чрез използване на система за достъп с карти. Във всички обекти за инсталирани камери за видео наблюдение и се наблюдават от охранителен. Избрани врати за достъп са снабдени с аларми и охранителният персонал следи тези аларми.

Достъпът до контролираните зони е ограничен посредством използване на карти и/или допълнителни проверки на биометрия. Всички лица без оторизиран достъп до контролираните зони, трябва да се регистрират и да бъдат придружени от лице с одобрен достъп до контролирана зона. Всички аварийни изходи на контролираните зони имат звукови аларми и охранителният персонал следи тези аларми. Извършва се периодична проверка дали алармите функционират, която се документира и запазва. Правата за достъп до контролираните зони се проверява повторно на всяко тримесечие. Достъпът до контролираните зони се отнема при прекратяване на договора за заетост.

Обектите са защитени и срещу природни бедствия, като например пожар, наводнение, прегряване, с помощта на противопожарни системи, пожарогасители, системи за засичане на дим и системи за изолиране и гасене на пожари. Обектите за защитени от прекъсване на електрозахранването и от сривове посредством системи за непрекъсваемо захранване (UPS) и резервни генератори, които се поддържат и тестват редовно.

Информацията и докладите относно съответствие на IBM SoftLayer може да бъде намерена на: http://www.softlayer.com/compliance.

9. Непрекъснатост на бизнес операциите

IBM има планове за непрекъснатост на бизнес процесите и възстановяване след срив, които са предназначени да поддържат ниво на обслужване, което е в съответствие със задълженията по Договора. Тези планове за непрекъснатост на бизнес процесите и възстановяване след срив ще бъдат актуализирани и тествани периодично (поне веднъж на година). IBM ще въведе всички съответни промени по плановете за непрекъснатост на бизнес процесите и възстановяване след срив, които са необходими за поддържане на съответствието с общоприетите индустриални практики, във всеки случай без неразумна намеса в IBM SaaS или производствената среда, която се използва от Клиента.

В случай че възникне даден срив, който направи IBM SaaS недостъпен за Клиента, IBM ще извести навременно Клиента и ще активира план за непрекъснатост на бизнес процесите и възстановяване след срив. Когато е деклариран срив, целта за непрекъснатост по отношение на работата на IBM SaaS, е възстановяването на достъпа на Клиента до IBM SaaS, както следва: в случай на прекъсване, Recovery Time Objective (RTO) (цел за време на възстановяване) за възстановяване на производствената среда на IBM Watson Health в рамките на 36 часа след деклариране на срив. Recovery Point Objective (RPO) (цел за момент на възстановяване) е не

повече от 24 часа от загубата на съдържание на Клиента в рамките на производствената среда. Специфичните решения на Watson Health за непрекъснатост на бизнес процесите могат да варират.

Подходът на IBM за възстановяване след срив се състои от множество центрове за данни в разпръснати в географско отношение зони.

Всички центрове за данни IBM SoftLayer поддържат множество електрозахранвания, оптични връзки, специализирани генератори и резервни акумулатори. Те са произведени от водещи в индустрията хардуер и оборудване, предоставящи най-високото равнище на производителност, надеждност и интероперативност. Всички компоненти в центровете за данни, които включват например допълнително n+1 захранване и охлаждане, се проверяват, за да се поддържа стабилност в рамките на центровете за данни.

10. Съвместимост

Практиките на IBM по отношение на сигурността са базирани на ISO 27001-27002. Тези практики предоставят структури за контрол, но не са ограничени само до Анализ на риска, Физическа сигурност, Планиране на непредвидени ситуации, Проучвания, Защита на информацията, Обучения, Защита на данните и Операции.

IBM преглежда дейностите, свързани със защита и поверителност за съответствие с практиките за сигурност на IBM.

IBM спазва приложимите за IBM закони, свързани с данните в съответните юрисдикции.

Изисква се също така подходящо боравене с поверителната информация на Клиентите съгласно Насоките за извършване на стопанска дейност на IBM, които всички служители трябва да прегледат веднъж годишно (и удостоверят, че са запознати с тях).

11. Други

IBM ще гарантира, че всички споразумения с всички изпълнители и/или включени трети страни при осигуряването на IBM SaaS имат условия, които защитават съдържанието на Клиента най-малко по начин, подобен на описания в това SBCA, и всички приложими Свързани документи, всеки до степента на тези условия, са приложими спрямо услугите, които трябва да бъдат изпълнени от изпълнителите и/или третите страни.