IBM „Cloud Service“ aprašas:

„IBM Kenexa Prove It! Add-ons on Cloud“

Toliau pateiktas jūsų Užsakymo Paslaugų aprašas:

1. „Cloud Services“ aprašas

Toliau pateikiamas „Cloud Service“ pasiūlymas, kurį galite užsisakyti. Šiame Paslaugų apraše pateiktas pasiūlymas laikomas priedo pasiūlymu, todėl prieš užsakydami bet kurį 1.1 skyriuje aprašytą priedą privalote užsiprenumeruoti „IBM Kenexa Prove It!“. Jūsų užsisakyti pasiūlymai nurodyti Užsakymo dokumente. Su šia „Cloud Services“ susijusį Užsakymo dokumentą sudarys jums pateiktas IBM Pasiūlymas ir Teisių suteikimo dokumentas (TSD), kurį gausite iš IBM, patvirtinantis „Cloud Services“ teikimą, informuojantis apie sąskaitų išrašymą ir nustatantis „Cloud Services“ pradžios ir pabaigos terminus.

1.1 „IBM Kenexa Prove It! Add-ons on Cloud“

„IBM Kenexa Prove It!“ – tai internetinis sprendimas, skirtas „IBM Kenexa Skills Assessments“ administruoti ir palaikyti bei „IBM Kenexa Behavioral Assessments“ pasirinkti. „IBM Kenexa Prove It!“ suteikia toliau nurodytas konfigūravimo paslaugas, skirtas tinkinti „Prove It!“ svetainę pagal pasirinktus Kliento reikalavimus:

a. „IBM Kenexa Prove It! Custom Web Site“

   Naudodamas šį priedo pasiūlymą Klientas gali keisti Pradinio skyriaus spalvas, logotipus ir turinį. Struktūros, reklamjuostės arba išdėstymo Pradinėje arba likusioje svetainės dalyje keisti negalima.

b. „IBM Kenexa Prove It! Corporate Custom Web Site“

   Naudodami šį priedo pasiūlymą Pradiniame skyriuje galite keisti spalvas, logotipus, turinį, reklamjuostę ir išdėstymą. Struktūros arba išdėstymo likusioje svetainės dalyje keisti negalima.T

2. Saugos aprašas

2.1 Saugos politikos

IBM palaiko privatumo ir saugos politikas, kurios yra pateikiamos IBM darbuotojams. IBM reikalauja, kad privatumo ir saugos mokymo kursai būtų taikomi IBM duomenų centrų darbą palaikantiems asmenims visame pasaulyje. Mes turime saugos komandą, kurį savo pagrindinį dėmesį skiria informacijos saugai. IBM saugos politikos ir standartai kasmet peržiūrimi ir iš naujo įvertinami. IBM saugos incidentai nagrinėjami pagal išsamią reagavimo į incidentus procedūrą.

2.2 Prieigos kontrolė

Prieiga prie kliento duomenų, laikantis pareigų atskyrimo principo, leidžiama tik įgaliotiesiems IBM palaikymo atstovams. IBM pagalbiniai darbuotojai naudoja dviejų veiksnių tarpinio šliuzo valdymo pagrindinio kompiuterio autentifikavimą. Kliento duomenys pasiekiami tik šifruoto ryšio kanalais. Registruojamos visos prieigos prie kliento duomenų ir visi duomenų perkėlimai į pagrindinio kompiuterio aplinką arba iš jos.IBM duomenų centruose, kuriuose palaikomas „Cloud Service“, WIFI ryšys nenaudojamas.

2.3 Paslaugos vientisumas ir pasiekiamumas

Operacinės sistemos išteklių taikomųjų programų programinės įrangos modifikavimus reguliuoja IBM keitimų valdymo procesas. Be to, užkardos taisyklių keitimus, kuriuos reguliuoja keitimų valdymo procesas, prieš realizuojant atskirai peržiūri IBM saugos darbuotojai. IBM 24x7 stebi duomenų centro išteklius. Siekiant nustatyti ir pašalinti galimas sistemos saugos spragas, vidaus ir išorės pažeidžiamumo tikrinimą reguliariai atlieka įgaliotieji administratoriai ir trečiosios šalies teikėjai. Visuose IBM duomenų centruose veikia kenkėjiškų programų aptikimo (antivirusinė, įsilaužimo aptikimo, pažeidžiamumo tikrinimo ir įsilaužimo prevencijos) sistemos. IBM duomenų centro tarnybos palaiko įvairius duomenų perdavimo viešaisiais tinklais informacijos pateikimo protokolus. Pavyzdžiui, HTTPS / SFTP / FTPS / S/MIME ir tiesioginio svetainių VPN. Atskiroje saugykloje skirta saugoti atsarginė duomenų kopija prieš transportavimą užšifruojama.

2.4 Veiklos registravimas

IBM laiko savo veiklos sistemose, taikomosiose programose, duomenų saugyklose, tarpinėje įrangoje ir tinklo infrastruktūros įrenginiuose, kuriuose galima konfigūruoti ir kurie yra konfigūruoti registruoti veiklą, žurnalus. Siekiant sumažinti piktavališko pakeitimo galimybę ir įgalinti centrinę analizę, įspėjimus ir ataskaitų kūrimą, centrinio žurnalo saugyklose realiuoju laiku registruojama veikla. Siekiant išvengti piktavališko pakeitimo, duomenys pasirašomi. Ieškant elgesio anomalijų žurnalai analizuojami realiuoju laiku ir periodinėse analizės ataskaitose. Eksploatacijos personalas įspėjamas apie anomalijas ir, jei reikia, kreipiasi į 24x7 pagal iškvietimą pasiekiamą saugos specialistą.

2.5 Fizinė sauga

IBM laikosi fizinės saugos standartų, skirtų apriboti neteisėtą fizinę prieigą prie duomenų centro išteklių. IBM duomenų centruose yra tik ribotos prieigos vietos, kurios kontroliuojamos taikant dviejų veiksnių autentifikavimą ir stebimos stebėjimo kameromis. Įeiti leidžiama tik įgaliotajam personalui, turinčiam patvirtintą įėjimo leidimą. Eksploatacijos personalas patikrina patvirtinimą ir išduoda prieigos leidimą, suteikiantį reikiamą prieigą. Tokius leidimus gavę darbuotojai privalo atiduoti kitus prieigos leidimus ir lankydamiesi gali turėti tik duomenų centro prieigos leidimą. Leidimų naudojimas registruojamas. Ne IBM lankytojai registruojami įeinantys į patalpas ir lydimi visose patalpose. Pristatymo vietos, krovimo rampos ir kitos vietos, per kurias į patalpas gali patekti asmenys be leidimų, kontroliuojamos ir izoliuotos.

2.6 Laikymasis

IBM kasmet atestuoja privatumo praktikas, kad atitiktų JAV Prekybos departamento „Saugaus uosto“ programos principus dėl pranešimų, pasirinkimo, tolimesnio perdavimo, prieigos ir tikslumo, saugos ir priežiūros bei reikalavimų vykdymo. Mūsų gamybos duomenų centruose kasmet atliekamas pramonės standarto SSAE 16 (anksčiau – SAS 70) arba atitinkamo tipo auditas. IBM peržiūri, ar su sauga ir privatumu susijusios veiklos atitinka IBM verslo reikalavimus. Siekiant laikytis informacijos saugos politikų, IBM reguliariai atlieka vertinimus ir auditus. Kasmet IBM darbuotojai ir tiekėjai dalyvauja darbuotojų saugos ir žinių apie sukčiavimo mokymuose. Darbuotojams kasmet primenami jų darbo tikslai ir atsakomybė laikytis verslo etikos, konfidencialumo ir IBM saugos įsipareigojimų.

3. Teisių suteikimas, sąskaitų išrašymas ir terminas

3.1 Mokesčio apskaičiavimas

„Cloud Service“ pasiūlymas parduodamas pagal šią mokesčių apskaičiavimo metriką, kaip nurodyta Užsakymo dokumente:

a. Egzempliorius yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Egzempliorius yra prieiga prie konkrečios „Cloud Service“ konfigūracijos. Reikia įsigyti pakankamas teises, skirtas kiekvienam „Cloud Service“ Egzemplioriui pasiekti ir naudoti matavimo laikotarpiu, nurodytu Teisių suteikimo dokumente (TSD) arba Užsakymo dokumente.

3.2 Mokesčiai ir sąskaitų išrašymas

Mokėtina suma už „Cloud Service“ pasiūlymus nurodoma Užsakymo dokumente.

3.2.1 Nustatymas

Nustatymo išlaidos nurodomos Užsakymo dokumente.

3.2.2 Pagal poreikį

Už parinktis pagal poreikį sąskaitos bus išrašomos tą mėnesį, kai užsakote parinktį pagal poreikį, apmokant tarifu, nustatytu Užsakymo dokumente.