Popis služeb IBM Cloud Service:

IBM Kenexa Prove It! Add-ons on Cloud

Níže je uveden Popis služeb pro Vaši Objednávku:

1. Popis služeb Cloud Service

Níže je uvedena nabídka Cloud Service, kterou si můžete objednat. Nabídka uvedená v tomto Popisu služeb se považuje za doplňkovou nabídku ("add-on"), to znamená, že si musíte zaregistrovat IBM Kenexa Prove It! ještě před objednáním jakýchkoli doplňků popsaných v článku 1.1 níže. Vámi objednané nabídky jsou uvedeny ve Vašem Dokumentu objednávky. Pro účely této služby Cloud Service bude Dokument objednávky obsahovat Cenovou nabídku, kterou Vám IBM předloží, a dokument o oprávnění (Proof of Entitlement), který obdržíte od IBM jako potvrzení o poskytování služby Cloud Service. Tento dokument Vás bude informovat o datu zahájení fakturace a bude uvádět počáteční a koncové datum období poskytování služby Cloud Service.

1.1 IBM Kenexa Prove It! Add-ons on Cloud

IBM Kenexa Prove It! je online řešení určené k administraci a podpoře produktu IBM Kenexa Skills Assessments a výběru IBM Kenexa Behavioral Assessments. IBM Kenexa Prove It! poskytuje níže uvedené konfigurační služby pro přizpůsobení webového serveru Prove It!, aby byl v souladu s vybranými požadavky Zákazníka:

a. IBM Kenexa Prove It! Custom Web Site

   Tato doplňková nabídka Vám umožňuje změnit barvy, loga a obsah v uvítací sekci Welcome. Nelze provádět žádné změny struktury, banneru nebo rozvržení uvítací stránky nebo zbývající části webového serveru.

b. IBM Kenexa Prove It! Corporate Custom Web Site

   Tato doplňková nabídka Vám umožňuje změnit barvy, loga, obsah, banner a rozvržení v uvítací sekci Welcome. Nelze provádět žádné změny struktury nebo rozvržení zbývající části webového serveru.

2. Popis zabezpečení

2.1 Zásady zabezpečení

IBM dodržuje zásady v oblasti zabezpečení a ochrany soukromí a seznamuje s nimi své zaměstnance. IBM vyžaduje, aby osoby na celém světě, které poskytují podporu datovým střediskům IBM, byly proškoleny v oblasti zabezpečení a ochrany soukromí. IBM disponuje vlastním bezpečnostním týmem, který se specializuje na zabezpečení informací. Zásady a standardy IBM v oblasti zabezpečení jsou každoročně přezkoumávány a přehodnocovány. Bezpečnostní incidenty IBM jsou zpracovávány v souladu s komplexním postupem reagování na incidenty.

2.2 Řízení přístupu

Přístup k datům zákazníka je umožněn pouze oprávněným zástupcům podpory IBM v souladu s principy segregace rolí. Ve vztahu k hostiteli mezilehlého správce "brány" používají pracovníci podpory IBM dvouúrovňové ověření. Při přístupu k datům zákazníka se pro všechna připojení používají šifrované kanály. Veškeré přístupy k datům zákazníka a přesuny dat z nebo do hostitelského prostředí jsou zapisovány do protokolů. V rámci datových středisek IBM podporujících tuto službu Cloud Service nejsou využívány WIFI.

2.3 Integrita a dostupnost služeb

Úpravy prostředků operačního systému a úpravy aplikačního softwaru se řídí procesem řízení změn IBM. Změny v pravidlech brány firewall rovněž podléhají procesu řízení změn a před implementací jsou jednotlivě přezkoumávány bezpečnostními pracovníky IBM. IBM monitoruje prostředky v datových střediscích 24 hodin denně, 7 dní v týdnu. Na podporu detekce a řešení potenciálního ohrožení zabezpečení systému je oprávněnými administrátory a dodavateli, kteří jsou třetími stranami, prováděno pravidelné interní i externí skenování ohrožení zabezpečení. Ve všech datových střediscích IBM jsou

používány systémy na detekci malwaru (antivirové programy, detekce neoprávněného vniknutí a ochrana před ním, skenování ohrožení zabezpečení). Služby datových středisek IBM podporují řadu doručovacích protokolů pro přenos dat prostřednictvím veřejných sítí. Jedná se například o HTTPS/SFTP/FTPS/S/MIME a site-to-site VPN. Zálohovaná data určená pro uložení mimo pracoviště jsou před přenosem šifrována.

2.4 Protokolování aktivity

IBM uchovává protokoly aktivity pro systémy, aplikace, datová úložiště, middleware a zařízení síťové infrastruktury, které umožňují protokolovat aktivitu a jsou pro tento účel nakonfigurovány. Aktivita je protokolována v reálném čase do centrálních úložišť protokolů, což umožňuje minimalizovat pravděpodobnost neoprávněných zásahů, centrální provádění analýzy, zasílání výstražných zpráv a tvorbu sestav. Aby se zabránilo neoprávněným zásahům, jsou data opatřena podpisem. Analýza protokolů se provádí v reálném čase prostřednictvím pravidelných analytických sestav, v nichž je vyhledáváno jakékoli abnormální chování. Operátoři jsou upozorňováni na anomálie a v případě potřeby mohou 24 hodin denně, 7 dní v týdnu telefonicky kontaktovat bezpečnostního specialistu.

2.5 Fyzické zabezpečení

IBM dodržuje standardy v oblasti fyzického zabezpečení, jejichž účelem je omezení neoprávněného fyzického přístupu k prostředkům v datových střediscích. Přístup do datových středisek IBM je možný pouze omezenými přístupovými body, pro něž platí režim dvouúrovňového ověření a které jsou monitorovány sledovacími kamerami. Přístup je umožněn pouze oprávněným pracovníkům s povoleným přístupem. Operátoři ověří povolení k přístupu a vydají přístupovou kartu umožňující nezbytný přístup. Zaměstnanci, jimž byly vydány takové přístupové karty, musí odevzdat ostatní přístupové karty a po dobu jejich činnosti smí mít u sebe pouze přístupové karty pro přístup do datového střediska. Používání přístupových karet je evidováno. Návštěvníci, kteří nejsou pracovníky IBM, jsou při vstupu do budovy zaregistrováni a po budovách se pohybují v doprovodu. Zásobovací a nakládací oblasti a další místa, jimiž mohou do prostor vniknout neoprávněné osoby, jsou hlídány a izolovány.

2.6 Dodržování požadavků

IBM certifikuje své postupy v oblasti ochrany soukromí vždy jednou ročně z hlediska souladu se zásadami U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement.Vždy jednou ročně je v našich produktivních datových střediscích prováděn odvětvový audit dle SSAE 16 (dříve SAS 70) nebo ekvivalentní audit. IBM přezkoumává činnosti související se zabezpečením a ochranou soukromí z hlediska dodržování obchodních požadavků IBM. IBM pravidelně provádí hodnocení a prověřování, jejichž cílem je ověřit dodržování zásad zabezpečení informací. Zaměstnanci IBM a dodavatelů každoročně absolvují školení pracovních sil zaměřené na vzdělávání a získání povědomí v oblasti zabezpečení. Každý rok je personál upomínán, aby jeho pracovní cíle a povinnosti byly v souladu s principy etického obchodního chování, ochrany důvěrných informací a závazků IBM v oblasti zabezpečení.

3. Informace o oprávnění, fakturaci a smluvním období

3.1 Metriky poplatků

Nabídka Cloud Service se prodává na základě níže uvedené metriky poplatků, jak je uvedena v Dokumentu objednávky:

a. Instance je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Instance je přístup ke specifické konfiguraci služby Cloud Service. Pro každou Instanci Cloud Service zpřístupněnou a používanou během období měření uvedeného v dokumentu o oprávnění (Proof of Entitlement) nebo v Dokumentu objednávky je nutno získat dostatečný počet oprávnění.

3.2 Poplatky a fakturace

Výše platby za nabídky Cloud Service je specifikována v Dokumentu objednávky.

3.2.1 Nastavení

Poplatky za nastavení budou uvedeny v Dokumentu objednávky.

3.2.2 On-Demand

Volby On-Demand budou fakturovány v měsíci, kdy si objednáte volbu On Demand, a to za sazbu uvedenou v Dokumentu objednávky.