

PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest udzielenie 51 szt. licencji oprogramowania Microsoft 365 Business Basic na okres 12 miesięcy

Specyfikacja ilościowa przedmiotu zamówienia:

LP.	Nazwa produktu	Numer katalogowy	Ilość	Model
1.	Microsoft 365 Business Basic	CFQ7TTC0LH18	51	subskrypcja roczna

Zamawiający wymaga dostaw licencji oprogramowania przeznaczonych do wykorzystania przez jednostki administracji publicznej.

Zamawiający oświadcza, że po podpisaniu umowy z Wykonawcą wskaże nazwę środowiska chmurowego (tenant) na platformie Microsoft, pod które należy podpiąć licencje.

WYMAGANIA W ZAKRESIE WYKONAWCY

Zamawiający wymaga, aby Wykonawca, składając ofertę na realizację przedmiotu zamówienia, posiadał status Partnera Microsoft.

Zamawiający żąda złożenia, wraz z ofertą przedmiotowego środka dowodowego, dokumentu potwierdzającego posiadanie statusu Partnera Microsoft w postaci wydruku ze strony Microsoft lub wskazania w Formularzu oferty adresu strony internetowej, umożliwiającej weryfikację posiadanego przez Wykonawcę statusu.

MINIMALNE WYMAGANIA W ZAKRESIE DOSTAW

1. Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2. Zamawiający wymaga dostawy Produktów na warunkach przewidzianych przez producenta Produktów lub jego spółek zależnych (Dostawcy).
3. Zamawiający wymaga dostawy Produktów, które umożliwiają na warunkach przewidzianych przez Dostawcę udzielenie licencji dla jednostek pozostających w strukturze Zamawiającego.
4. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:
 - a) Aktywację pakietów subskrypcji,
 - b) Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.
5. Oferowane pakiety subskrypcji usług hostowanych w chmurze publicznej jej producenta (Dostawcy) muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i norm potwierdzonych aktualnymi wynikami niezależnych audytów, oraz list kontrolnych w szczególności:
 - a) PN-ISO/IEC
 - i. 27001,
 - ii. 27002,
 - iii. 27017,
 - iv. 27018,
 - v. 20000-1:2011,
 - vi. 22301,
 - b) SOC 1, SOC 2, SOC 3,
 - c) Open Authentication Standard – OAuth,

- d) CIS Benchmark.
- 6. Zgodność algorytmów zabezpieczających dane usług platformy hostowanej Dostawcy z FIPS 140.
- 7. Oferowane pakiety subskrypcji powszechnie dostępnych, standardowych usług muszą zapewniać lub umożliwiać zapewnienie:
 - a) Dostępność usług na poziomie 99,9% (lub wyższym),
 - b) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach.
 - c) Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO posiadanymi przez Dostawcę.
 - d) Możliwość automatycznej, niewpływającej na ciągłość pracy systemów instalacji poprawek dla wybranych składników pakietów usług,
 - e) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
 - f) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi zarządzania tożsamością będącej składową pakietów usług oferowanych przez Dostawcę.
 - g) Możliwość realizacji bezpiecznego uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
 - h) Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
 - i) Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
 - j) Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
 - k) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).
 - l) Możliwość zestawienia (za dodatkową opłatą) dedykowanego połączenia pomiędzy lokalną infrastrukturą sprzętową Zamawiającego, a Centrami przetwarzania Dostawcy,
 - m) Możliwość korzystania w ramach pakietów usług Dostawcy z dedykowanych urządzeń typu HSM zgodnych z FIPS 140-2 poziomu 3.
 - n) Wbudowane w platformę Dostawcy mechanizmy zabezpieczające przed atakami DDoS,
 - o) Możliwość zastrzeżenia miejsca uruchomienia usług i składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego (EOG).
 - p) Możliwość korzystania z przynajmniej dwóch równorzędnych centrów przetwarzania danych Dostawcy, składających się z przynajmniej trzech redundantnych ośrodków przetwarzania i położonych na obszarze EOG.
 - q) Dostępność zapisów umownych Dostawcy zawierających tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
 - r) Zobowiązania umowne Dostawcy potwierdzające zgodność z rozp. RODO i potwierdzające rolę Dostawcy jako przetwarzającego dane,
 - s) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
 - t) Gwarancję usunięcia danych Zamawiającego z usług i centrów przetwarzania Dostawcy po zakończeniu umowy.
 - u) Gwarancję braku dostępu do danych Zamawiającego przez Dostawcę, z wyłączeniem działań serwisowych i wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy.