Ogłoszenie

Numer

2022-36060-101275

Id

101275

Powstaje w kontekście projektu

POPC.05.01.00-22-0000/00 - Cyfrowa Gmina – Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym- „Granty PPGR”

Tytuł

Cyfrowa Gmina – Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym- „Granty PPGR”

Zamówienia uzupełniające

Zamawiający nie przewiduje zamówień uzupełniających

Warunki zmiany umowy

1. Zmiana postanowień zawartej umowy może nastąpić za zgodą obu stron wyrażoną na piśmie pod rygorem nieważności takiej zmiany w niżej wymienionych przypadkach:
1) zmiany terminu realizacji:
a) z powodu okoliczności siły wyższej, np. wystąpienia zdarzenia losowego wywołanego przez czynniki zewnętrzne, którego nie można było przewidzieć z pewnością, w szczególności zagrażającego bezpośrednio życiu lub zdrowiu ludzi lub grożącego powstaniem szkody w znacznych rozmiarach,
b) z powodu uzasadnionych zmian w zakresie sposobu wykonywania przedmiotu zamówienia proponowanych przez Zamawiającego lub Wykonawcę, jeżeli te zmiany są korzystne dla Zamawiającego,
c) z powodu zaistnienia okoliczności leżących po stronie Zamawiającego, w szczególności spowodowanych sytuacją finansową, zdolnościami płatniczymi lub warunkami organizacyjnymi lub okolicznościami, które nie były możliwe do przewidzenia w chwili zawarcia umowy,

Załączniki

Dodane do ogłoszenia w obowiązującej wersji z dn. 2022-03-29
1. Zapytanie ofertowe z załącznikam

Czy dopuszczalna oferta częściowa?

NIE

Data opublikowania ogłoszenia

2022-03-29

Data ostatniej zmiany

2022-03-29

Termin składania ofert

2022-04-06 08:00:00

Planowany termin podpisania umowy

2022-04

Dane adresowe ogłoszeniodawcy

> Miasto Kwidzyn
> Warszawska 19
> 82-500 Kwidzyn
> NIP: 5811956166

Osoby do kontaktu

> Iwona Milewska
> tel.: 556464760
> e-mail: im@kwidzyn.pl

Części zamówienia

Część: 1

Tytuł części 1

Systemy operacyjne

Czy dopuszczalne oferty wariantowe

NIE

Przedmioty zamówienia do części 1

> **Typ**
> Dostawa
>
> **Podkategoria**
> Sprzęt IT

Opis

1. Przedmiotem zamówienia jest zakup i instalacja na wskazanych przez Zamawiającego komputerach systemu operacyjnego klasy PC typu Windows 10 Home 64 bit Home lub równoważnego w ilości 232 licencji.
2. Instalację wykona Wykonawca, na własny koszt, w siedzibie Wykonawcy lub Zamawiającego (wg. uznania Wykonawcy). Koszty ewentualnego transportu komputerów poniesie Wykonawca.
3. Zamawiający zastrzega, że wszystkie licencje muszą być oryginalne, nowe i nieużywane, nie dopuszcza się tzw. licencji „refurbished”. Zamawiający zastrzega sobie prawo do sprawdzenia legalności każdej z dostarczonych licencji.
4. Na potwierdzenie instalacji systemu Wykonawca umieści na każdym z komputerów naklejkę z hologramem i numerem seryjnym systemu.
5. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
1) Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
2) Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
3) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
4) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
5) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
6) Wbudowany system pomocy w języku polskim.
7) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
8) Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
9) System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:
a) wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
b) wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
c) stosowanie kwarantanny,
d) wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
e) skanowanie urządzeń USB natychmiast po podłączeniu,
f) automatyczne odłączanie zainfekowanej końcówki od sieci,

g) skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
h) Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.
i) Musi posiadać moduł ochrony IDS/IPS
j) Musi posiadać mechanizm wykrywania skanowania portów
k) Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
l) Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
10) Szyfrowanie danych:
a) Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
b) Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.
11) Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
12) Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
13) Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.
14) Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przed niezamierzonymi manipulacjami – ataki ransomware
15) Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.
16) System musi umożliwiać co najmniej:
a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
b) funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
c) funkcje regulowania połączeń WiFi i Bluetooth
d) funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
e) funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi

f) funkcje blokowania dostępu dowolnemu urządzeniu
g) możliwość tymczasowego dodania dostępu do urządzenia przez administratora
h) zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
i) możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
j) możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
k) możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry
l) możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
m) funkcję wirtualnej klawiatury
n) możliwość blokowania każdej aplikacji
o) możliwość zablokowania aplikacji w oparciu o kategorie
p) możliwość dodania własnych aplikacji do listy zablokowanych
q) dodawanie innych aplikacji
r) dodawanie aplikacji w formie portable
s) możliwość wyboru pojedynczej aplikacji w konkretnej wersji
t) dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
u) kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
v) możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
w) możliwość zablokowania funkcji Printscreen
x) funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
y) funkcje monitorowania i kontroli przepływu poufnych informacji
z) możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
aa) możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
bb) możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
cc) ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
dd) ochrona zawartości schowka systemu
ee) ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
ff) możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
gg) ochrona plików zamkniętych w archiwach
hh) Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
ii) możliwość tworzenia profilu DLP dla każdej polityki
jj) wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania

kk) ochrona przez wyciekiem plików poprzez programy typu p2p
17) Monitorowanie zmian w plikach:
a) Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
b) Funkcje monitorowania określonych rodzajów plików.
c) Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
d) Generator raportów do funkcjonalności monitora zmian w plikach.
e) możliwość śledzenia zmian we wszystkich plikach
f) możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
g) możliwość definiowana własnych typów plików
18) Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa
19) Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
20)Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
21) Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:
a) Microsoft Internet Explorer
b) Microsoft Edge
c) Mozilla Firefox
d) Google Chrome
e) Safari
22) Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
23) Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
24) Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:
a) Windows 2008 R2
b) Windows 2012
c) Windows 2012 R2
d) Windows 2016
25) Portal zarządzający musi umożliwiać:
a) przegląd wybranych danych na podstawie konfigurowalnych widgetów
b) zablokowania możliwości zmiany konfiguracji widgetów
c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności

e) eksport wszystkich skanów podatności do pliku CSV
3. Wykonawca powołujący się na rozwiązania równoważne jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego.

Kody CPV

48620000-0 Systemy operacyjne

Miejsca realizacji

adres

Kraj

Polska

Województwo

pomorskie

Powiat

kwidzyński

Gmina

Kwidzyn

Miejscowość

Kwidzyn

Kryteria oceny do części 1

Czy kryterium cenowe?

TAK

Opis

Cena 100%

Podsumowanie

Oś czasu związana z ogłoszeniem i ofertowaniem

-> 2022-03-29 - data opublikowania

-> 2022-04-06 08:00:00 - termin składania ofert

-> 2022-04 - planowany termin podpisania umowy

Oś czasu realizacji przedmiotów zamówienia

Brak zdefiniowanych etapów dla przedmiotów zamówienia.