**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**na zakup wraz z dostawą i konfiguracją serwera wraz z oprogramowaniem do szyfrowania i zabezpieczenia poczty przed atakami phishing**

w ramach projektu grantowego pn. „Cyfrowa Gmina” realizowanego w ramach Programu Operacyjny Polska Cyfrowa na lata 2014–2020, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

ZAMAWIAJĄCY:

**Gmina ORCHOWO**

**ul. Kościuszki 6, 62-436 Orchowo**

**tel. 63 26 84 090**

1. **OFERTA NA SERWER Z OPROGRAMOWANIEM – specyfikacja sprzętu i oprogramowania:**

|  |  |  |
| --- | --- | --- |
| **OPROGRAMOWANIE serwera** | | |
|  | Oprogramowanie serwera wsparcie techniczne i prawo do aktualizacji na 2 lata. | **Spełnia/nie spełnia** |
|  | Oprogramowanie serwera Windows Server Standard 2019 64Bit Polish DVD 16 | **Spełnia/nie spełnia** |
|  | Oprogramowanie dostarczone razem z serwerem musi dodatkowo zapewnić funkcjonalność: | **Spełnia/nie spełnia** |
|  | realizowanie usług FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS zarządzanych przez przeglądarkę WEB, | **Spełnia/nie spełnia** |
|  | nadawanie uprawnień do plików i katalogów dla użytkowników serwera przez przeglądarkę WEB | **Spełnia/nie spełnia** |
|  | systemu antywirusowego zarządzanego przez przeglądarkę WEB , | **Spełnia/nie spełnia** |
|  | generowania certyfikatów SSL przez przeglądarkę WEB, | **Spełnia/nie spełnia** |
|  | importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB, | **Spełnia/nie spełnia** |
|  | centralnego zarządzania bazą haseł przez przeglądarkę WEB | **Spełnia/nie spełnia** |
|  | centralnego sterowania, zarządzania i wprowadzania konfiguracji przez przeglądarkę WEB | **Spełnia/nie spełnia** |
| 4. | W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność: | **Spełnia/nie spełnia** |
|  | Administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB, | **Spełnia/nie spełnia** |
|  | Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny. | **Spełnia/nie spełnia** |
|  | Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny. | **Spełnia/nie spełnia** |
|  | Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token, | **Spełnia/nie spełnia** |
|  | Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny, | **Spełnia/nie spełnia** |
|  | Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0, | **Spełnia/nie spełnia** |
|  | Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u, | **Spełnia/nie spełnia** |
|  | współpracy z klientami Windows 7,8,8.1,10,11 w wersji professional. | **Spełnia/nie spełnia** |
| Specyfikacja wdrożenia: | | |
|  | Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami: | **Spełnia/nie spełnia** |
|  | jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne, | **Spełnia/nie spełnia** |
|  | jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne. | **Spełnia/nie spełnia** |
|  | W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne. | **Spełnia/nie spełnia** |
| **Serwer główny – parametry techniczne** | | |
|  | Obudowa: RACK 2U | **Spełnia/nie spełnia** |
|  | Procesor: Jeden procesor min. sześciordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 13000 punktów w teście PassMark CPU Benchmarks dostępnym na stronie <http://www.cpubenchmark.net/high_end_cpus.html>. Procesor z obsługą wirtualizacji. | **Spełnia/nie spełnia** |
|  | Pamięć: min. 128GB dedykowane do pracy serwerowej | **Spełnia/nie spełnia** |
|  | 8 kieszeni HotSwap SATA3 | **Spełnia/nie spełnia** |
|  | 1 dysk systemowy o poj. min. 1TB zamontowany wewnątrz serwera | **Spełnia/nie spełnia** |
|  | 4 dyski na dane o poj. min. 1TB zamontowane w kieszeniach HotSwap | **Spełnia/nie spełnia** |
|  | 4 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap. | **Spełnia/nie spełnia** |
|  | Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s | **Spełnia/nie spełnia** |
|  | Wsparcie KVM przez LAN | **Spełnia/nie spełnia** |
|  | Panel przedni chroniący kluczem dostępu do dysków | **Spełnia/nie spełnia** |
|  | Czujnik otwarcia obudowy | **Spełnia/nie spełnia** |
|  | Komplet szyn montażowych w zestawie | **Spełnia/nie spełnia** |
|  | Gwarancja: 2 lata gwarancji producenta. | **Spełnia/nie spełnia** |

1. **OFERTA NA OPROGRAMOWANIE DO SZYFROWANIA I ZABEZPIECZENIA POCZTY PRZED ATAKAMI PHISHING – specyfikacja oprogramowania:**

|  |  |  |
| --- | --- | --- |
| 30 Licencji oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na 2 lata. | | |
|  | Oprogramowanie musi zapewnić funkcjonalność: | **Spełnia/nie spełnia** |
|  | szyfrowanie algorytmem AES256 treści wiadomości, | **Spełnia/nie spełnia** |
|  | szyfrowanie algorytmem AES256 załączników, | **Spełnia/nie spełnia** |
|  | szyfrowanie algorytmem AES256 plików, | **Spełnia/nie spełnia** |
|  | szyfrowanie algorytmem AES256 katalogów, | **Spełnia/nie spełnia** |
|  | do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego. | **Spełnia/nie spełnia** |
|  | do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe. | **Spełnia/nie spełnia** |
|  | do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego. | **Spełnia/nie spełnia** |
|  | do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego. | **Spełnia/nie spełnia** |
|  | odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0 | **Spełnia/nie spełnia** |
|  | szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki | **Spełnia/nie spełnia** |
|  | generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania, | **Spełnia/nie spełnia** |
|  | opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność, | **Spełnia/nie spełnia** |
|  | zabezpieczenia każdego emaila dedykowanym unikalnym hasłem, | **Spełnia/nie spełnia** |
|  | posiadania wewnętrznej bazy haseł, która umożliwia: | **Spełnia/nie spełnia** |
|  | export haseł do pliku, | **Spełnia/nie spełnia** |
|  | import haseł z pliku | **Spełnia/nie spełnia** |
|  | generowania ponownie haseł w bazie | **Spełnia/nie spełnia** |
|  | posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich, | **Spełnia/nie spełnia** |
|  | posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym, | **Spełnia/nie spełnia** |
|  | posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów, | **Spełnia/nie spełnia** |
|  | pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows. | **Spełnia/nie spełnia** |
|  | integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym, | **Spełnia/nie spełnia** |
|  | zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe, | **Spełnia/nie spełnia** |
|  | wykrywania fałszywych emaili - Antiphishing, | **Spełnia/nie spełnia** |
|  | wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING, | **Spełnia/nie spełnia** |
|  | wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych, | **Spełnia/nie spełnia** |
|  | wykrywanie niebezpiecznych dokumentów MS Office, | **Spełnia/nie spełnia** |
|  | wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email, | **Spełnia/nie spełnia** |
|  | definiowania alarmów informujących o niebezpiecznych mailach i załącznikach, | **Spełnia/nie spełnia** |
|  | współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia, | **Spełnia/nie spełnia** |
|  | alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc, | **Spełnia/nie spełnia** |
|  | współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11. | **Spełnia/nie spełnia** |
|  | Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy. | **Spełnia/nie spełnia** |
|  | Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy. | **Spełnia/nie spełnia** |
|  | Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami. | **Spełnia/nie spełnia** |
|  | Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows. | **Spełnia/nie spełnia** |
|  | Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne **przez 2 lata.** | **Spełnia/nie spełnia** |

Oświadczam, że zapoznałem się z opisem przedmiotu zamówienia i nie wnoszę do niego zastrzeżeń.

W przypadku wyboru mojej oferty zobowiązuję się, do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.

.......................................................

(podpis i pieczęć Wykonawcy)