Nr postępowania: **ZP.271.2.14.2022** *Załącznik nr 4 do Zapytania ofertowego*

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

I. PRZEDMIOT ZAMÓWIENIA:

Nazwa: Zakup 29 licencji na oprogramowanie do szyfrowania poczty e-mail i dokumentów z modułem antyphishing oraz modułem do pracy zdalnej.

Zamówienie realizowane w projekcie pt. „Cyfrowa Gmina" w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina".

1. Szczegółowy opis przedmiotu zamówienia:

Specyfikacja na oprogramowanie do szyfrowania poczty e-mail i dokumentów z modułem antyphishing oraz modułem do pracy zdalnej

1) Oprogramowanie musi zapewnić funkcjonalność:

- szyfrowania algorytmem AES256 treści wiadomości;

- szyfrowania algorytmem AES256 załączników;

- szyfrowania algorytmem AES256 plików;

- szyfrowania algorytmem AES256 katalogów;

- do odszyfrowania treści wiadomości, plików, katalogów, załączników e-mail, nie wymagana jest dodatkowo płatna lub bezpłatna licencja (oprogramowanie, usługa, chmura, hosting) lub dostęp do portalu internetowego;

- do odszyfrowania treści wiadomości, plików, katalogów, załączników e-mail, nie wymagane jest połączenie internetowe;

- odszyfrowanie treści wiadomości, plików, katalogów, załączników e-mail, 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;

- generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania;

- opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność;

- zabezpieczenia każdego e-maila dedykowanym unikalnym hasłem;

- posiadania wewnętrznej bazy haseł, która umożliwia:

* export haseł do pliku,

* import haseł z pliku,

* generowanie ponownie haseł w bazie;

- posiadania wewnętrznego raportu informującego Administratora o szyfrowaniu e-mail przy włączonej opcji generowania hasła dla każdej z nich;

- posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym;

- posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości e-mailowych, plików i katalogów;

- 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;

- integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie SMS z hasłem i docelowym kontaktem smsowym;

- zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe;

- wykrywania fałszywych e-maili Antyphishing;

- wykrywania prób podszycia się pod dowolnego adresata (mechanizm ANTISPOOFING);

- wykrywania fałszywych linków i odsyłaczy w wiadomościach e-mailowych;

- wykrywania niebezpiecznych dokumentów MS Office;

- wykrywania niebezpiecznych rozszerzeń plików przesyłanych przez pocztę e-mail;

- definiowania alarmów informujących o niebezpiecznych mailach i załącznikach;

- współpracy z serwerem Producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest na minimum 4 lata;

- współpracy z klientem Microsoft Outlook 2021 dla systemów 32Bit i 64Bit, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.

2) Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa, np. antywirusy.

3) Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa, np. antywirusy.

4) Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.

5) Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

6) Wsparcie techniczne i prawo do aktualizacji oraz bazy dla modułu ANTYPHISHING na 4 lata.

Wykonawca musi dostarczyć Zamawiającemu licencję nową w takiej formie, aby nie podlegała wątpliwości jej legalność. Zamawiający wskazuje jednocześnie, że będzie weryfikował legalność oprogramowania.

2. Okres gwarancji, w tym wsparcie techniczne i prawo do aktualizacji na cały przedmiot zamówienia: 4 lata.

3. Termin wykonania przedmiotu zamówienia: do 30 dni od dnia udzielenia zamówienia (zlecenia).

4. Miejsce dostarczenia przedmiotu zamówienia: Urząd Gminy w Klembowie, ul. Gen. Fr. Żymirskiego 38, 05-205 Klembów.

5. Zamawiający nie dopuszcza składania ofert częściowych.

6. Zamawiający nie dopuszcza składania ofert wariantowych.

7. Zamawiający dopuszcza możliwość zastosowania produktów równoważnych, tj. produktów o cechach, parametrach technicznych i jakościowych nie gorszych niż określone w Opisie Przedmiotu Zamówienia (OPZ), stanowiącym załącznik nr 4 do zapytania ofertowego.

II. WSPÓLNY SŁOWNIK ZAMÓWIEŃ (CPV):

CPV 48761000-0 - Pakiety oprogramowania antywirusowego;

CPV 48731000-1 - Pakiety oprogramowania zabezpieczającego pliki;

CPV 48811000-6 - System poczty elektronicznej.

III. KRYTERIUM OCENY OFERT: cena 100%.

Klembów, dnia 13.09.2022r.

/-/Rafał Mathiak
Wójt Gminy Klembów

.....
(data i podpis Kierownika Zamawiającego lub osoby upoważnionej)