Załącznik nr 1 do Zapytania ofertowego

Nr postępowania: **ZP.271.2.37.2024**

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

I. PRZEDMIOT ZAMÓWIENIA:

1. Nazwa: Zakup i dostawa oprogramowania do ochrony przed wyciekiem danych, zapewnienia poufności danych oraz zapobiegania przed ich nieupoważnionym udostępnieniem (DLP).

2. Szczegółowy opis przedmiotu zamówienia:

Licencje (ilość: 55 sztuk):

1. System operacyjny:

a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,

b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,

c. MacOS 12 lub nowszy;

2. Serwer administracyjny musi obsługiwać instalację na systemach: Windows Server 2016 (64-bit) i nowszych;

3. Serwer administracyjny musi obsługiwać bazy danych:

a. MS SQL Server 2016 lub nowsze,

b. MS SQL Express,

c. AzureSQL S3 lub nowsze;

4. Pomoc i dokumentacja programu musi być dostępna w języku angielskim;

5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim;

6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta;

7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych;

8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym;

9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia;

10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli;

11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit;

12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania;

13. Administrator musi mieć możliwość, aby tworzyć, usuwać konta administratorów w konsoli programu;

14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu);

15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory;

16. Administrator powinien potrafić wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym;

17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa;

18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak: uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach;

19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików;

20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych;

21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości e-mail;

22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu;

23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania;

24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików;

25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie: aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku;

26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak: zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami, itp.;

27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak: numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN;

28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym;

29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM;

30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP;

31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwiać aktualizację do nowej wersji lub dezaktywację tego oprogramowania;

32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365;

33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams;

34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach;

35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.);

36. System musi zapewniać możliwość zarządzania szyfrowaniem dysków twardych oraz urządzeń wymiennych;

37. Licencja – czas nieokreślony;

38. Okres wsparcia - przez okres min. 12 miesięcy.

3. Termin realizacji (dostawy) przedmiotu zamówienia: 30 dni od dnia udzielenia zamówienia (od dnia wystawienia zlecenia).

4. Zamawiający nie dopuszcza składania ofert częściowych.

5. Zamawiający nie dopuszcza składania ofert wariantowych.

6. Przedmiot zamówienia jest realizowany w związku z:

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23.

II. WYMAGANE DOKUMENTY, KTÓRE ZOBOWIĄZANY BĘDZIE ZŁOŻYĆ WYKONAWCA:

1) Formularz oferty (wg załączonego wzoru) – załącznik nr 2 do zapytania ofertowego;

2) Oświadczenie Wykonawcy – załącznik nr 4 do zapytania ofertowego;

3) Odpis lub informacja z Rejestru Przedsiębiorców Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

III. WSPÓLNY SŁOWNIK ZAMÓWIEŃ (CPV):

CPV: 48730000-4 - Pakiety oprogramowania zabezpieczającego.

IV. KRYTERIUM OCENY OFERT: Cena brutto oferty (waga-100 %).

Klembów, dnia 06.11.2024 r.

/-/Rafał Mathiak
Wójt Gminy Klembów

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