Toruń, dn. 26.04.2022

Urząd Miasta Torunia
Biuro Projektów Informatycznych
Ul. Wały gen. Sikorskiego 8
e-mail: zp_bpi@um.torun.pl
BPI.271.14.1.2022

--- Wg. rozdzielnika ---

Zapytanie ofertowe poniżej 130 000 zł
nr BPI/3400/08/2022

postępowanie o udzielenie zamówienia publicznego o wartości nieprzekraczającej 130 000 zł prowadzone jest poza przepisami ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, (Dz.U. z 2021 r., poz. 1129 z późn. zm.) zgodnie z zarządzeniem nr 247 PMT z dnia 22.09.2021 r w sprawie zasad udzielania zamówień publicznych w Urzędzie Miasta Torunia

Biuro Projektów Informatycznych
Urząd Miasta Torunia
87-100 Toruń
ul. Wały gen. Sikorskiego 8

zwraca się z uprzejmą prośbą o przesłanie w trybie badania rynku propozycji cenowej na

- Udzielenie **250 licencji** na system DLP do ochrony przed wyciekiem danych zgodnie ze specyfikacją załączoną w załączniku 2. Okres licencjonowania – bezterminowo (licencje wieczyste)

1. Proszę podać jako kryterium 1: ryczałtową cenę **netto i brutto w złotych**.
2. Wraz z ofertą Oferent złoży wypełniony formularz oferty – załącznik nr 1.
3. Wraz z ofertą Oferent złoży aktualny pełny odpis z KRS bądź z CEiDG.
4. Termin realizacji: Zamawiający oczekuje realizacji zadania w terminie do 14 dni od dnia podpisania umowy
5. Kryterium wyboru ofert: Dla porównania ofert zostaną zastosowane kryteria:
   a) Kryterium 1: Cena – 100%
   Za korzystniejszą ofertę zostanie uznana oferta, która otrzyma największą liczbę punktów stanowiących sumę punktów za kryterium a)
   Każda oferta może uzyskać za dane kryterium określoną liczbę punktów przy zastosowaniu wzorów:
   a) Kryterium 1:

$$\text{cena oferty} = \frac{\textit{najniższa oferowana cena spośród złożonych ofert}}{\textit{cena oferty badanej}} \times \text{znaczenie kryterium tj. 100 \%}$$

6. Miejsce składania ofert: Ofertę proszę dostarczyć do Biura Projektów Informatycznych UMT ul. Wały gen. Sikorskiego 8 pok. 62, osobiście lub na adres e-mail (np. w formacie PDF): zp_bpi@um.torun.pl
7. Warunki płatności: przelew, **21 dni od dnia dostarczenia faktury**.
8. Termin składania ofert: do **06.05.2022r. do godz. 12:00 (decyduje godzina otrzymania oferty przez Zamawiającego)**
9. Wymagania i warunki Zamawiającego:
   a) Zamawiający nie dopuszcza składania ofert wariantowych, chyba, że zostało wskazane inaczej.
   b) Zamawiający nie dopuszcza składania ofert częściowych, chyba, że zostało wskazane inaczej.
   c) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Oferentami w celu uzupełnienia lub doprecyzowania ofert.
   d) Z wyłonionym Wykonawcą zostanie zawarta pisemna umowa zgodnie z procedurami obowiązującymi w UMT. Umowa do podpisania zostanie wysłana do Wykonawcy w formie elektronicznej i papierowej.
   e) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu sporządzania niniejszego zapytania Ofertowego.
   f) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny na każdym etapie postępowania do zawarcia umowy.
   g) Ze względu na założenia budżetowe i ograniczenia finansowe, w przypadku, gdy kwoty przedstawione w ofertach na zapytanie będą wyższe od zaplanowanych w budżecie na ww. zadanie Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez negocjacji z Oferentami.
   h) Oferent może złożyć wyłącznie jedną ofertę.
   i) Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
   j) Oferty złożone po terminie nie zostaną rozpatrzone.
   k) Oferenci uczestniczą w postępowaniu ofertowym na własne ryzyko i koszt, nie przysługują im żadne roszczenia z tytułu odstąpienia przez Zamawiającego od postępowania ofertowego.
   l) Oferenci biorący udział w postępowaniu zostaną poinformowani o wynikach postępowania pisemnie (drogą elektroniczną).
   m) Zamawiający zastrzega sobie możliwość wyboru kolejnej wśród najkorzystniejszych ofert, jeżeli oferent, którego oferta zostanie wybrana jako najkorzystniejsza, uchyli się od zawarcia umowy w przedmiocie realizacji niniejszego zamówienia.
   n) Oferenci mogą zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego drogą elektroniczną na adres e-mail: zp_bpi@um.torun.pl
   o) Ewentualne pytania dotyczące postępowania wraz z odpowiedziami Zamawiającego będą publikowane na BIP Zamawiającego.
10. Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.
11. Zaproszenie nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert. Zamawiający zastrzega sobie prawo do rezygnacji z zamówienia bez wyboru którejkolwiek ze złożonych ofert.
12. Zamawiający, w przypadku wpłynięcia jednej oferty, zastrzega sobie prawo do negocjacji warunków zamówienia oraz ceny za jego wykonanie, a także do rezygnacji z zamówienia bez podania przyczyny.

DYREKTOR
Biura Projektów Informatycznych
Mariusz Szefera

Załącznik 1

PRZEDMIOT ZAMÓWIENIA	**250 licencji** na system DLP do ochrony przed wyciekiem danych .....
ZAMAWIAJĄCY	Gmina Miasta Toruń - wydział prowadzący – Biuro Projektów Informatycznych UMT .....
WYKONAWCA **Adres** **Numer telefonu / fax** **Internet http: //** **e-mail**	
Kryterium 1. CENA OFERTY NETTO / BRUTTO (z obowiązującym podatkiem VAT)	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Osoba uprawniona do podpisania umowy	.....
Osoba uprawniona do podpisania protokołu odbioru	.....
Adres e-mail służący do zgłaszania reklamacji	.....
Data **Podpis**	

Załącznik 2

Specyfikacja

DLP – ochrona przed wyciekiem danych

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim lub angielskim
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
    a) Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
    b) Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
    a) logowanie oraz wylogowanie użytkownika,
    b) włączenie oraz wyłączenie stacji roboczej,
    c) blokada oraz odblokowanie stacji roboczej,
    d) przejście w stan bezczynności stacji roboczej.
19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.

21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29.
30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
    a) aplikacje, z której zostały utworzone,
    b) lokalizację,
    c) adres URL,
    d) format pliku,
    e) zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
    a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
    b) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    c) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    d) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej w tym blokowaniem oraz zezwalaniem na przesyłanie plików na strony internetowe w kategorii hosting plików
    e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
    f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
    g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
        - Dropbox,
        - Google Drive,
        - SharePoint,
        - OneDrive Business,
        - OneDrive Personal.
    h) blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
    i) blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,

j) blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty oraz wirtualnego drukowania,
k) uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,

35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów email oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
    a) numery kart kredytowych,
    b) numer PESEL,
    c) numer polskiego dowodu osobistego,
    d) polski numer paszportu,
    e) wyrażenia regularne,
    f) określone ciągi znaków,
    g) numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości email, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy").
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
52. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
    a) Bezpieczeństwo danych:
        - Przegląd informacji o incydentach bezpieczeństwa.
        - Przegląd danych przychodzących.
        - Przegląd danych wychodzących.
        - Podłączane/odłączane urządzenia przenośne.
    b) Produktywność:
        - Przegląd informacji na temat produktywności użytkowników.

- Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
- Trendy.

c) Eksploatacja sprzętu:
- Przegląd informacji na temat eksploatacji sprzętu komputerowego.
- Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
- Eksploatacja drukarek.
- Eksploatacji sieci.

53. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
54. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
55. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku który zawiera informacje nt:
    - plików przenoszonych na nośniki USB i inne urządzenia przenośne,
    - plików przesłanych za pomocą wiadomości e-mail,
    - plików przesłanych za pomocą poczty webowej,
    - plików przesłanych do Internetu,
    - plików wysłanych za pomocą komunikatorów,
    - plików przesłanych na dyski chmurowe,
    - analiza sposobu korzystania z aplikacji,
    - analiza korzystania z Internetu,
    - analiza wykorzystania porali do poszukiwania pracy.

Wdrożenie (na miejscu u Zamawiającego lub zdalnie):

- Zamawiający udostępni na potrzeby instalacji system Windows Serwer
- Instalacja maksymalnie na 10 komputerach
- Plan wdrożenia:
  · Instalacja serwera.
  · Instalacja klientów na maksymalnie 10 stacjach.
  · Włączenie funkcji audytora.
  · Ustawienie tagowania jednej przykładowej ścieżki lokalnej (tagowanie w oparciu o maksymalnie 10 plików tekstowych).
  · Ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe.
  · Ustawienie reguły (jednej)
    - DLP.Omówienie funkcji konsoli.
- Roczne wsparcie techniczne producenta rozwiązania zapewniające między innymi kontakt telefoniczny w godzinach 8-15 (pn-pt),