MUZEUM GÓRNICTWA WĘGLOWEGO W ZABRZU
41-800 Zabrze, ul. Georgiusa Agricoli 2
tel: +48 32 630 30 91
fax: +48 32 277 11 25
biuro@muzeumgornictwa.pl
www.muzeumgornictwa.pl

KOPALNIA GUIDO
ul. 3 Maja 93,
41-800 Zabrze,
kopalniaguido.pl

SZTOLNIA KRÓLOWA LUIZA
ul. Wolności 410,
41-800 Zabrze,
sztolnialuiza.pl

MGW.DI.271.2.2026.DP Zabrze, dnia 20.03.2026 r.

Zapytanie o cenę z jednoczesnym zastrzeżeniem zawarcia umowy do realizacji

Muzeum Górnictwa Węglowego w Zabrzu zaprasza do złożenia oferty na realizacje zamówienia pn.:
„Dostawa oprogramowania antywirusowego na potrzeby MGW"

Postępowanie prowadzone na podstawie regulaminu udzielania zamówień publicznych o wartości nieprzekraczającej kwoty wskazanej w art. 2 ust1 pkt 1 ustawy – prawo zamówień publicznych.
Ofertę prosimy przesłać :
pocztą na adres – Muzeum Górnictwa Węglowego w Zabrzu, ul. Georgiusa Agricoli 2, 41-800 Zabrze,
lub pocztą elektroniczną: oferty@muzeumgornictwa.pl
Termin składania ofert : do 27.03.2026 r. godzina 14:00

Opis przedmiotu zamówienia:

Przedmiotem rozeznania ofertowego jest dostawa oprogramowania celem kontynuacji zgodnie z zaistniałymi potrzebami MGW na okres 3 lat.

Termin realizacji zamówienia:

1. Termin wykonania przedmiotu zamówienia: dwa tygodnie od daty podpisania umowy.
2. Wykonawca jest zobowiązany do zawarcia umowy w ciągu 7 dni od powiadomienia drogą telefoniczną/e-mail przez Zamawiającego o wyborze oferty Wykonawcy.

Termin związania ofertą:

Termin związania ofertą wynosi 30 dni kalendarzowych od daty złożenia oferty.

Wymagania Zamawiającego:

1. Zamówienie będzie realizowane po cenach jednostkowych zadeklarowanych przez Wykonawcę w Formularzu Cenowym wg. potrzeb do wysokości środków zabezpieczonych w budżecie na ten cel. Ilości wskazane w formularzu cenowym są ilościami szacunkowymi. Zamawiający nie jest zobowiązany do zamówienia wszystkich pozycji wymienionych w ofercie.
2. Zamawiający posiada oprogramowanie antywirusowe Bitdefender i wymaga dostarczenia rozwiązania tego samego lub równoważnego. Przez rozwiązanie równoważne rozumie się oprogramowanie, które spełnia co najmniej poniższe wymagania techniczne i funkcjonalne:
   Wspierane systemy operacyjne:
   - Windows 11, Windows 10, Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows 2016 oraz wersje Windows Server Core
   - Linux oparte o RPM, oparte o Debian oraz SUSE,

   Ochrona antywirusowa i antyspyware
   - Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
   - Interfejs oraz pomoc techniczna świadczona w języku polskim.
   - Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

- Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
- Możliwość dodawania wykluczeń na podstawie:
    a) Plik
    b) Folder
    c) Rozszerzenie
    d) Proces
    e) Hash pliku
    f) Hash certyfikatu
    g) Nazwa zagrożenia
    h) Wiersz poleceń
    i) IP/maska
- Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.
- Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
- W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
- Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
- Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
- Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
- Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
- Możliwość dezaktywacji funkcji zapory sieciowej.
- Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
- Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
- Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
- Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
- Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
- Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
- Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
- Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
- Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows. Zmiana ustawień zabezpieczona jest hasłem.
- Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
- Ochrona Exchange

- Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
- Konsola zdalnej administracji
- System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
- Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
- Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
- Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
- Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
- Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
- Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
- Możliwość ręcznego i automatycznego generowania raportów oraz wyeksportowanie ich do formatu: pdf i csv.
- Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
- Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
- Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie m.in:
  a) Zakres adresów IP/IP.
  b) Adres bramy.
  c) Nazwa hosta.
- Możliwość naprawy instalacji agenta z poziomu konsoli.
- Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej,
- Możliwość wyświetlenia informacji o zainstalowanym systemie operacyjnym,
- Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania.
- Filtrowanie wykrytych incydentów bezpieczeństwa
- Możliwość wygenerowania i wyeksportowania incydentów do pliku .csv.

3. W przypadku zastosowania produktu równoważnego Wykonawca zobowiązuje się wykonać pełne wdrożenie systemu antywirusowego na wszystkich wskazanych przez Zamawiającego serwerach oraz komputerach użytkowników. Po wdrożeniu wymagane jest przeprowadzenie pełnego szkolenia z obsługi administracyjnej dostarczonego oprogramowania.
4. Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego przez cały okres obowiązywania licencji, obejmującego w szczególności:
   - pomoc w rozwiązywaniu problemów technicznych i konfiguracyjnych,
   - dostarczanie aktualizacji oprogramowania oraz sygnatur zagrożeń,
   - dostęp do dokumentacji, bazy wiedzy i portalu wsparcia technicznego,
   - możliwość kontaktu z pomocą techniczną w języku polskim
5. Zamawiający dopuszcza stosowanie jedynie licencji nieużywanych.
6. Zamawiający nie dopuszcza stosowania licencji tzw. refurbished.

7. Cennik powinien zawierać ceny jednostkowe oraz wartości netto i brutto.
8. Dostawy przedmiotu zamówienia mogą być wykonywane w godzinach pomiędzy 7:00 a 15:00 w terminie do 3 dni roboczych od daty złożenia zamówienia.

Cena i warunki płatności za usługi objęte zakresem oferty

1. Podane ceny będą obowiązywały przez cały rok 2026 w przypadku wyboru Wykonawcy.
2. Warunki płatności: faktura – po wykonaniu dostawy

Dodatkowe wymagania:
Wykonawca zobowiązany będzie do dostarczenia licencji na własny koszt, w dniach roboczych, tj. od poniedziałku do piątku, w godzinach 7:00 – 15:00.

Osoba do kontaktu:
Dariusz Parysek tel. **728 406 117** / (32)**630 30 91** wew. **2000**

Kryteria oceny ofert:
Cena - 100% (najniższa zaoferowana cena).

Podpis Dyrektora:

……

Załączniki:
1. Formularz ofertowy
2. Wzór umowy

Uwaga:

Zamawiający zastrzega sobie prawo do odstąpienia od udzielenia zamówienia bez podania przyczyny i bez zwrotu kosztów przygotowania i złożenia oferty.

Ochrona danych osobowych:
W przypadku złożenia oferty Pani/Pana dane osobowe będą przetwarzane - na podstawie art. 6 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – RODO (Dz. Urz. UE L 2016, Nr 119, s. 1) - wyłącznie na potrzeby przeprowadzenia tegoż postepowania. Nie jest Pani/Pan zobowiązana/zobowiązany do podania swych danych osobowych. Jednakże konsekwencją nie podania tych danych będzie odrzucenie Pani/Pana oferty, co z góry wyklucza ewentualne podpisanie z Panią/Panem umowy. Jeżeli złoży Pani/Pani ofertę to administratorem Pani/Pana danych osobowych będzie Muzeum Górnictwa Węglowego w Zabrzu z siedzibą przy ul. Georgiusa Agricoli 2 w Zabrzu. Kontakt do inspektora ochrony danych Zamawiającego: iod@muzeumgornictwa.pl. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania w oparciu o przepisy prawa lub w oparciu o obowiązujące u Zamawiającego procedury. Decyzje, w oparciu o podane przez Panią/Pana dane, nie będą podejmowane w sposób zautomatyzowany. Dane osobowe będą przechowywane do przedawnienia ewentualnych roszczeń, wykonania obowiązków archiwalnych i wynikających z przepisów prawa. Po złożeniu oferty będzie Pani/Pan mieć prawo żądania dostępu do swych danych osobowych; ich sprostowania, przeniesienia oraz ograniczenia przetwarzania (z zastrzeżeniem przypadku, o którym mowa w art. 18 ust. 2 RODO). Będzie Pani/Pan również mieć prawo do wniesienia skargi do organu nadzorczego w rozumieniu przepisów o ochronie danych osobowych w każdym przypadku zaistnienia podejrzenia że przetwarzanie Pani/Pana danych osobowych następuje z naruszeniem powszechnie obowiązujących przepisów prawa. W zakresie określonym w art. 17 ust. 3 lit. d) oraz e) RODO nie będzie Pani/Panu przysługiwać prawo do usunięcia danych osobowych. Uwaga: Punkt ma zastosowanie jeśli oferent jest osobą fizyczną lub osobą fizyczną prowadząca działalność gospodarczą lub działa przez pełnomocnika będącego osobą fizyczną lub członków organu zarządzającego będących osobami fizycznymi.