Sygnatura sprawy: **32/ZP/22**

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

ZAMAWIAJĄCY:

Akademia Marynarki Wojennej
im. Bohaterów Westerplatte
ul. inż. Śmidowicza 69
81-127 GDYNIA
www.amw.gdynia.pl

ROCZNICA POWSTANIA ARMII KRAJOWEJ

ZAPRASZA DO ZŁOŻENIA OFERTY W POSTĘPOWANIU

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego

TRYB UDZIELENIA ZAMÓWIENIA**:** tryb podstawowy bez negocjacji

Podstawa prawna: Ustawa z dnia 11.09.2019 r. - Prawo zamówień publicznych
(Dz. U. z 2021 r. poz. 1129 z późn. zm.)

ZATWIERDZAM

Rektor-Komendant
wz. kmdr Paweł PODGÓRNY

Signature Not Verified
Dokument podpisany przez Paweł Podgórny
Data: 2022.06.08 08:32:24 CEST

dnia …… …….. 2022 r.

Opracowała: Sekcja Zamówień Publicznych

100 lat Akademii Marynarki Wojennej

ROZDZIAŁ 1 Nazwa oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania

Nazwa:	Akademia Marynarki Wojennej im. Bohaterów Westerplatte
Adres:	**ul. inż. Śmidowicza 69** **81 – 127 GDYNIA**
Numer telefonu:	**261262537**
Godziny urzędowania:	**od godz. 7.30 do godz. 15.30**
NIP:	**586-010-46-93**
REGON:	**190064136**
Adres poczty elektronicznej:	przetargi@amw.gdynia.pl
Adres strony internetowej:	www.amw.gdynia.pl
Adres strony internetowej prowadzonego postępowania	platforma zakupowa https://platformazakupowa.pl/

Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, zobowiązany jest posiadać konto na platformie zakupowej.
Zarejestrowanie i utrzymanie konta na platformie zakupowej oraz korzystanie z platformy jest bezpłatne.

ROZDZIAŁ 2 Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

platforma zakupowa
https://platformazakupowa.pl/

ROZDZIAŁ 3 Tryb udzielenia zamówienia

Postępowanie o udzielenie zamówienia prowadzone jest w **trybie podstawowym** na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych oraz zgodnie z wymogami określonymi w niniejszej Specyfikacji Warunków Zamówienia, zwanej dalej „SWZ".

ROZDZIAŁ 4 Informacja, czy Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji

Zamawiający **nie przewiduje negocjacji**.

ROZDZIAŁ 5 Opis przedmiotu zamówienia

1. Wspólny Słownik Zamówień (CPV):
   Część I: **CPV** 48760000-3 Pakiety oprogramowania do ochrony antywirusowej
   CPV 72000000-5 Usługi informatyczne
   Część II: **CPV** 48210000-3 Pakiety oprogramowania dla sieci

2. Przedmiotem zamówienia jest:
   Część I – odnowienie subskrypcji na system ochrony antywirusowej i antyspamowej zasobów sieci komputerowej;
   – wsparcie techniczne systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego;

   Część II - certyfikat ssl wildcard z roczną subskrypcją;

   Przedłużenie subskrypcji i certyfikat w formie elektronicznej, wsparcie techniczne – usługa świadczona na miejscu lub zdalnie.
   Szczegółowy OPZ zawiera (załącznik nr 2 SWZ)

3. **Zamawiający informuje, że podstawą do wstępu cudzoziemców na teren Akademii przed przystąpieniem do realizacji umowy jest otrzymanie pozwolenia jednorazowego na wjazd w wyniku uzyskania pozytywnej opinii Dyrektora Zarządu Operacyjnego Służby Kontrwywiadu Wojskowego poprzez Szefa Agencji Bezpieczeństwa Wewnętrznego lub otrzymanie jednorazowego pozwolenia wydanego przez Dowództwo Generalne Rodzajów Sił Zbrojonych** *(wymóg uzyskania zgody SKW zgodnie z zasadami wynikającymi z decyzji nr 19/MON Ministra Obrony Narodowej z dnia 24.01.2017r. w sprawie organizowania współpracy międzynarodowej w resorcie obrony narodowej (Dz. Urz. MON poz. 18).*
   Zamawiający zastrzega, że procedura wyrażenia zgody na realizację umowy przez pracowników nieposiadających obywatelstwa polskiego może potrwać około miesiąca.
   Z powyższego Wykonawcy nie przysługują żadne roszczenia związane ze zmianą terminu wykonania przedmiotu zamówienia.

   Wykonawca przed przystąpieniem do realizacji Umowy zapozna się z procedurami wstępu na teren Akademii Marynarki Wojennej obowiązujących u Zamawiającego.

ROZDZIAŁ 6 Termin wykonania zamówienia

Termin realizacji zamówienia:

Część I: Do 29.06.2022 r. – odnowienie subskrypcji,
Od 30.06.2022 r. – przez 12 miesięcy – wsparcie techniczne
Część II: 20.08.2022 r. – certyfikat

ROZDZIAŁ 7 Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy

1. Zamawiający wymaga, aby wybrany Wykonawca zawarł z nim umowę na warunkach określonych w projekcie umowy stanowiącym **załącznik nr 3** do SWZ.
2. Zamawiający zastrzega sobie, iż ostateczna treść umowy w stosunku do projektu umowy może ulec zmianie, jednakże wyłącznie w przypadku, gdy zmiana ta nie jest istotna w rozumieniu art. 454 ustawy Prawo Zamówień Publicznych i w zakresie przewidzianym w treści projektu umowy, zgodnie z art. 455 ust. 1 ustawy Prawo Zamówień Publicznych.

ROZDZIAŁ 8 Informacja o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformy zakupowej (dalej jako „Platforma") pod adresem:

   https://platformazakupowa.pl/

2. W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między Zamawiającym a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były w formie elektronicznej za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do Zamawiającego".
   Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do Zamawiającego", po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.
3. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji "Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem platformazakupowa.pl do konkretnego Wykonawcy.
4. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

5. Zamawiający, zgodnie z art. 67 ustawy Prawo Zamówień Publicznych, określa wymagania techniczne i organizacyjne sporządzania, wysyłania i odbierania korespondencji elektronicznej, tj.:
   a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć RAM min. 2 GB, procesor Intel Pentium IV 2 GHZ lub nowszy, jeden z systemów operacyjnych - MS Windows wersja 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,
   c) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10.0,
   d) włączona obsługa JavaScript,
   e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   f) Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
   g) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
6. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   a) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
   b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.
7. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl**, w szczególności za sytuację, gdy Zamawiający zapozna się z treścią oferty przed upływem terminu otwarcia ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do Zamawiającego").
   Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek określony w art. 221 Ustawy Prawo Zamówień Publicznych.
8. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
9. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

ROZDZIAŁ 9 Informacja o sposobie komunikowania się Zamawiającego z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej w przypadku zaistnienia jednej z sytuacji określonych w art. 65 ust. 1, art. 66 i art. 69

Nie dotyczy.

ROZDZIAŁ 10 Wskazanie osób uprawnionych do komunikowania się z Wykonawcami

Sekcja Zamówień Publicznych
Anna PARASIŃSKA, Beata ŁASZCZEWSKA-ADAMCZAK, Rafał FUDALA.

ROZDZIAŁ 11 Termin związania ofertą

1. Wykonawca jest związany złożoną ofertą od dnia upływu terminu składania ofert do dnia **17.07.2022 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

ROZDZIAŁ 12 Opis sposobu przygotowania oferty

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny Wykonawca może złożyć bezpośrednio na dokumencie, który następnie przesyła do systemu[1] przez **platformazakupowa.pl** oraz dodatkowo dla całego pakietu dokumentów w kroku 2 **Formularza składania oferty lub wniosku** (po kliknięciu w przycisk **Przejdź do podsumowania**).
2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
3. Oferta musi być:
   a) sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
   b) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
   c) podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną.
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".
5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny Zamawiający wymaga dołączenia odpowiedniej ilości plików, czyli podpisywanych plików z danymi oraz plików XAdES.
6. Zgodnie z art. 18 ust. 3 ustawy Prawo zamówień publicznych, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Prawo zamówień publicznych. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
7. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
8. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje, że podlegać będzie odrzuceniu.
9. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością.
10. Opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego Wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, albo przez Podwykonawcę.
11. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB, natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

[1] rozporządzenie Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. poz. 2452).

12. Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z "OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".
13. Zalecenia:
    a) *Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf*
    b) *W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:*
        - *.zip*
        - *.7Z*
    c) *Wśród formatów powszechnych a NIE występujących w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.*
    d) *Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.*
    e) *Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, Zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.*
    f) *Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.*
    g) *Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.*
    h) *Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.*
    i) *Zaleca się, aby komunikacja z Wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do Zamawiającego", nie za pośrednictwem adresu email.*
    j) *Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.*
    k) *Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na kilka godzin przed terminem składania ofert/wniosków.*
    l) *Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.*
    m) *Jeśli Wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.*
    n) *Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.*
    o) *Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.*

14. Dokumenty stanowiące ofertę **(dotyczy wszystkich części)**, które należy złożyć:
    a) **Formularz ofertowy**- sporządzony według wzoru **(załącznik nr 1).**
    b) **Oświadczenie Wykonawcy o niepodleganiu wykluczeniu z postępowania** – w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepodleganiu wykluczeniu składa każdy z Wykonawców - sporządzony według wzoru **(załącznik nr 5).**
    c) **Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu – w** przypadku wspólnego ubiegania się o zamówienia przez Wykonawców, oświadczenie o spełnianiu warunków udziału w postępowaniu składa ich pełnomocnik - sporządzone według wzoru **dotyczy części I (załącznik nr 9);**
    d) **Oświadczenie** podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby o którym mowa w art. 118 - sporządzony według wzoru **dotyczy części I (załącznik nr 10 - jeżeli dotyczy);**

e) **Oświadczenia podmiotu udostępniającego zasoby** z art. 125 ust. 5 ustawy Pzp **dotyczy części I (załącznik nr 11 - jeżeli dotyczy);**
f) **Oświadczenie wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia** z art. 125 ust. 1 ustawy Pzp **dotyczy części I (załącznik nr 12 - jeżeli dotyczy);**
g) **Pełnomocnictwo** upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik;
h) **Pełnomocnictwo dla pełnomocnika** do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia **– jeżeli dotyczy**;
i) **Oświadczenie o którym mowa w art. 117 ust 4 (załącznik nr 6) – jeżeli dotyczy.**
j) **Oświadczenie RODO** - sporządzone według wzoru **(załącznik nr 7)**.

15. Dokumenty i oświadczenia, które Wykonawca będzie zobowiązany złożyć na wezwanie Zamawiającego, którego oferta została najwyżej oceniona. Zamawiający wezwie wykonawcę, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, aktualnych na dzień złożenia oświadczenia o braku podstaw do wykluczenia i następujących podmiotowych środków dowodowych:
    a) **Oświadczenie** o przynależności bądź braku przynależności do grupy kapitałowej **(dla części I i II – załącznik nr 4)**
    b) **Oświadczenie** o aktualności informacji **(dla części I i II – załącznik nr 8)**
    c) **Wykaz dostaw i usług wraz z referencjami** (**dla części I – załącznik nr 13)**
    d) **Wykaz osób (załącznik nr 14) - (dotyczy części I)**
    e) **Oświadczenie o dysponowaniu osobami (załączniki nr 15-19) - (dotyczy części I)**
    f) **Oświadczenie** o dysponowaniu punktem serwisowym **(załącznik nr 20) - (dotyczy części I).**
    g) **Oświadczenie** o dysponowaniu portalem/systemem serwisowym **(załącznik nr 21) - (dotyczy części I).**
16. Oferta, oświadczenie o niepodleganiu wykluczeniu z udziału w postępowaniu muszą być złożone w oryginale.
17. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (t.j. Dz.U.2020.1192 z późn.zm.), które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.
18. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
19. Postanowień ust. 18 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzaniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
20. Oferty składane wspólnie (konsorcjum, spółka cywilna itp.).
21. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
22. Wykonawcy składający ofertę wspólną ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy.
23. Do oferty wspólnej Wykonawcy dołączają pełnomocnictwo.
24. Pełnomocnik pozostaje w kontakcie z Zamawiającym w toku postępowania i do niego Zamawiający kieruje informacje, korespondencję, itp.
25. Oferta wspólna, składana przez dwóch lub więcej Wykonawców, powinna spełniać następujące wymagania:
    a) oferta wspólna powinna być sporządzona zgodnie z SWZ;
    b) sposób składania dokumentów w ofercie wspólnej:

- dokumenty, dotyczące własnej firmy, takie jak np.: oświadczenie o braku podstaw do wykluczenia składa każdy z Wykonawców składających ofertę wspólną we własnym imieniu;
- dokumenty wspólne takie jak np.: formularz ofertowy, formularz cenowy, dokumenty podmiotowe i przedmiotowe składa pełnomocnik Wykonawców w imieniu wszystkich Wykonawców składających ofertę wspólną;

c) kopie dokumentów dotyczących każdego z Wykonawców składających ofertę wspólną muszą być poświadczone za zgodność z oryginałem przez osobę lub osoby upoważnione do reprezentowania tych Wykonawców.

26. Przed podpisaniem umowy (w przypadku wygrania postępowania) Wykonawcy składający ofertę wspólną będą mieli obowiązek przedstawić Zamawiającemu umowę konsorcjum, zawierającą, co najmniej:
   a) zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,
   b) określenie zakresu działania poszczególnych stron umowy,
   c) czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia oraz czas trwania gwarancji jakości i rękojmi.

ROZDZIAŁ 13 Sposób oraz termin składania ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: **https://platformazakupowa.pl/** w myśl Ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych na stronie internetowej prowadzonego postępowania do dnia **17.06.2022 r. o godz. 09:00**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
3. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.
4. Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 1 oraz ust. 2 ustawy Prawo zamówień publicznych, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 tej ustawy sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
5. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
7. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

ROZDZIAŁ 14 Termin otwarcia ofert

1. Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert, tj. **17.06.2021 r. o godz. 09:15**
2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. **Otwarcie ofert jest niejawne.**
6. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
2) cenach lub kosztach zawartych w ofertach.

7. Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji „Komunikaty" .
8. W przypadku ofert, które podlegają negocjacjom, Zamawiający udostępnia informacje, o których mowa w ust. 6 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.
9. Zgodnie z Ustawą Prawo Zamówień Publicznych Zamawiający nie ma obowiązku przeprowadzania jawnej sesji z otwarcia ofert, z udziałem wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line a ma jedynie takie uprawnienie.

ROZDZIAŁ 15 Podstawy wykluczenia

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:
   1) w art. 108 ust. 1 pkt 1 - 6 ustawy;
   2) w art. 109 ust. 1 pkt 1 i od 3 do10 ustawy, tj.:

   Z postępowania o udzielenie zamówienia zamawiający może wykluczyć wykonawcę:

   1) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
   ~~2) który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:~~
      ~~a) będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego,~~
      ~~b) będącego osobą fizyczną prawomocnie skazanego~~ **ukaranego** ~~za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny,~~
      ~~c) wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;~~
   3) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub **ukarano za** wykroczenie, o którym mowa w pkt 2 lit. a lub b;
   4) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
   5) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;
   6) jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie wykonawcy;
   7) który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;

8) który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w po-stępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
9) który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
10) który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.

2. W przypadkach, o których mowa w ust. 1 pkt 1–5 lub 7, zamawiający może nie wykluczać wykonawcy, jeżeli wykluczenie byłoby w sposób oczywisty nieproporcjonalne, w szczególności gdy kwota zaległych podatków lub składek na ubezpieczenie społeczne jest niewielka albo sytuacja ekonomiczna lub finansowa wykonawcy, o którym mowa w ust. 1 pkt 4, jest wystarczająca do wykonania zamówienia.
3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy.
4. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
5. W związku z ustawą z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, **wyklucza się z postępowania wykonawców rosyjskich** w rozumieniu przepisów rozporządzenia 833/2014 zmienionego rozporządzeniem 2022/576. **Zakaz obejmuje również podwykonawców, dostawców i podmioty, na których zdolności wykonawca polega**, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.

Weryfikacji braku zaistnienia tej podstawy wykluczenia w stosunku do wykonawcy zamawiający dokona wszelkimi dostępnymi środkami np.: za pomocą ogólnodostępnych rejestrów takich jak Krajowy Rejestr Sądowy, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Centralny Rejestr Beneficjentów Rzeczywistych itd.

ROZDZIAŁ 16 Sposób obliczenia ceny

1. Cena oferty musi uwzględniać wszystkie zobowiązania wynikające z umowy, tj. wszystkie koszty i składniki związane z wykonaniem zamówienia oraz warunkami SWZ i uwzględniać cały zakres przedmiotu zamówienia (w tym podatki i narzuty). Cena oferty uwzględnia wszystkie zobowiązania, musi być podana w PLN cyfrowo i słownie, z wyodrębnieniem należnego podatku VAT - jeżeli występuje.
2. Cenę należy określić z dokładnością do dwóch miejsc po przecinku. Kwoty wykazane w ofercie zaokrągla się do pełnych groszy, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się do 1 grosza.
3. Cena ustalona przez Wykonawcę zostanie ustalona na okres ważności umowy i nie będzie podlegała zmianom.
4. Cenę za wykonanie przedmiotu zamówienia należy wpisać do „Formularza ofertowego" stanowiącego załącznik do niniejszej specyfikacji warunków zamówienia.
5. Wynagrodzenie za przedmiot umowy jest wynagrodzeniem ryczałtowym.

ROZDZIAŁ 17 Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów, i sposobu oceny

1. **CZĘŚĆ I**

Przy wyborze oferty Zamawiający będzie kierował się **następującymi kryteriami:**

Lp.	Kryterium	Znaczenie kryterium (%)	Liczba możliwych do uzyskania punktów

1.	Cena oferty	**90**	do 90 punktów
2.	Polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę (oprócz Wykonawcy)	**10**	do 10 punktów

1) Cena – **90%**
sposób przyznania punktów

Cn / Cb x 100 x 90% = ilość punktów

gdzie:
Cn – najniższa cena spośród ofert nie odrzuconych
Cb – cena oferty badanej (rozpatrywanej)
100 – wskaźnik stały
90% – procentowe znaczenie kryterium „ceny"

2) Polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę (oprócz Wykonawcy) – **10%**

sposób przyznania punktów:

Polskojęzyczne wsparcie – 10 pkt
Brak polskojęzycznego wsparcia – 0 pkt

3) **Całkowita liczba punktów** jest sumą punktów uzyskanych w poszczególnych kryteriach.

2. **<u>CZĘŚĆ II</u>**
Przy wyborze oferty Zamawiający będzie kierował się **następującymi kryteriami:**

Lp.	Nazwa kryterium	Znaczenie kryterium (%)	Liczba możliwych do uzyskania punktów
1.	Cena oferty /**C**/	100	do 100 punktów

Cena wykonania zamówienia /C/ – obejmuje cenę wykonania przedmiotu zamówienia w zakresie rzeczowym określonym w niniejszej SWZ.
Oferta z najniższą ceną otrzyma maksymalną ilość punktów = **100 pkt**, oferty następne będą oceniane na zasadzie proporcji w stosunku do oferty najtańszej wg wzoru:

$$C = [C_{min} / C_{bad}] \times 100$$

gdzie: C - liczba punktów za cenę
C_{min} - najniższa cena ofertowa
C_{bad} - cena oferty badanej

3. Ocenie będą podlegać wyłącznie oferty niepodlegające odrzuceniu.
4. Za najkorzystniejszą zostanie uznana oferta z najwyższą liczbą punktów.
5. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej ilości punktów, wezwie on Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
6. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.
7. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania z ofertą określonym w SWZ.

7. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
8. W przypadku braku zgody, o której mowa w ust. 7, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.
9. Cenę należy podać w PLN i wyliczyć na podstawie indywidualnej kalkulacji wykonawcy, uwzględniając termin realizacji, doświadczenie i wiedzę zawodową wykonawcy, jak i wszelkie koszty niezbędne do wykonania całości lub części przedmiotu zamówienia, podatki oraz rabaty, upusty itp., których wykonawca zamierza udzielić. Cena oferty musi obejmować pełny zakres przedmiotu zamówienia lub jego części. W okresie realizacji umowy cena nie podlega waloryzacji.
10. Wynagrodzenie za przedmiot umowy jest wynagrodzeniem ryczałtowym. Sumaryczna cena wyliczona w indywidualnej kalkulacji wykonawcy winna odpowiadać cenie podanej przez wykonawcę w formularzu oferty dla całości lub części przedmiotu zamówienia.
11. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu umowy, a płatność nastąpi zgodnie z zapisem umowy i ofertą wykonawcy.

ROZDZIAŁ 18 Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 ustawy Prawo zamówień publicznych, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią załącznik do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postepowanie.

ROZDZIAŁ 19 Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówieniá oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Pzp.
2. Odwołanie przysługuje na:
   2.1. niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postepowanių o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2.2. zaniechanie czynnoścí w postepowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy;
   2.3. zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy Prawi zamówień publicznych , stronom oraz uczestnikom postepowanią odwoławczego przysługuje skarga do sadu. Skargę wnosi się do Sadu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.

5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX ustawy Prawo zamówień publicznych - „Środki ochrony prawnej".

ROZDZIAŁ 20 Informacje o warunkach udziału w postępowaniu, jeżeli Zamawiający je przewiduje

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy **spełniają warunki udziału w postępowaniu** dotyczące:
   1) **zdolności do występowania w obrocie gospodarczym**
      Opis spełnienia warunku:
      Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.
   2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów**
      Opis spełnienia warunku:
      Dokument wystawiony przez producenta lub dystrybutora oferowanego oprogramowania potwierdzający, że jest on autoryzowanym partnerem producenta oferowanego oprogramowania uprawnionym do sprzedaży licencji i wdrażania oferowanego oprogramowania **(dotyczy części I)**.
   3) **sytuacji ekonomicznej lub finansowej**
      Opis spełnienia warunku:
      Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.
   4) **zdolności technicznej lub zawodowej**
      Opis spełnienia warunku:
      a) **Wykonawca musi wykazać się doświadczeniem (załącznik nr 13) – dotyczy części I** tj. wykaz dostaw i usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy– w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów- oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonanie powinny być wystawione w okresie ostatnich 3 miesięcy.

         Za spełnienie tego warunku Zamawiający uzna wykonanie minimum 1 zamówienia obejmującego łącznie (nie dopuszcza się przedłożenia kilku dokumentów (referencji) na cząstkowe zakresy wymienione poniżej):
         - Dostarczenie subskrypcji oprogramowania antywirusowego do ochrony serwerów i stacji roboczych z konsolą centralnego zarządzania dla minimum 500 urządzeń,
         - Świadczenie wsparcia technicznego dla systemu ochrony antywirusowej ESET lub innego, oferowanego przez wykonawcę systemu antywirusowego w przypadku oferowania systemu równoważnego do ESET dla minimum 500 urządzeń
         - Świadczenie wsparcia technicznego dla środowiska serwerowego opartego o Windows Serwer składającego się z minimum dwóch serwerów poczty Exchange 2016 skonfigurowanych w DAG, serwera plików opartego o system minimum Windows Server 2016, serwera wydruków, serwera aktualizacji WSUS, klastra środowiska wirtualnego Hyper-V, systemu zarządzania maszynami wirtualnymi System Center Virtual Machine Manager 2019, serwera backupu System Center Data Protection Manager 2019, kontrolerów domeny opartych o system minimum Windows Serwer 2016, serwerów fizycznych i macierzy dyskowych.

b) **Wykonawca musi dysponować osobami (załącznik nr 14) (dotyczy części I),** które zostaną skierowane przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami;.

Za spełnienie tego warunku zamawiający uzna dysponowanie przez wykonawcę osobami:

- Minimum 1 osobą, posiadającą certyfikat potwierdzający umiejętność instalowania i konfigurowania oferowanego oprogramowania. Certyfikat musi być wystawiony przez producenta lub autoryzowanego dystrybutora oferowanego oprogramowania lub autoryzowany przez niego ośrodek szkoleniowy. **(na część I załącznik nr 15).**
- Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Windows Serwer 2008 lub nowszego **(na część I załącznik nr 16).**
- Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Microsoft Exchange 2010 lub nowszego **(na część I załącznik nr 17).**
- Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność wdrażania i administrowania środowiskiem wirtualnym opartym o Microsoft Hyper-V **(na część I załącznik nr 18).**
- Minimum 1 osobą posiadającą certyfikat potwierdzający umiejętność świadczenia usług serwisowych zgodnie z ITIL (np. ITIL Foundation) **(na część I załącznik nr 19).**

c) Dysponować punktem serwisowym umożliwiającym dotarcie do siedziby Zamawiającego w ciągu 1 godziny od zgłoszenia serwisowego **(na część I załącznik nr 12).**

d) Dysponować portalem/systemem serwisowym w którym Zamawiający będzie mógł dokonywać zgłoszeń serwisowych i widzieć szczegóły ich realizacji **(na część I załącznik nr 13).**

Ocena spełnienia warunków będzie dokonywana metodą 0-1, tj. spełnia/nie spełnia w oparciu o oświadczenia i dokumenty dołączone do oferty bądź po ich uzupełnieniu na wezwanie Zamawiającego.

2. Wykonawca może w celu potwierdzenia spełnienia warunków udziału w postępowaniu, polegać na zdolnościach technicznych lub zawodowych lub sytuacji ekonomicznej lub finansowej podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
5. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   a) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   b) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   c) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

6. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 3 i 4 ustawy Prawo zamówień publicznych oraz, jeżeli to dotyczy, kryteriów selekcji, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
7. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z Wykonawcą, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.
8. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
9. Wykonawca nie może, po upływie terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania wniosków o dopuszczenie do udziału w postępowaniu albo ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

ROZDZIAŁ 21	**Informacje o podmiotowych środkach dowodowych, jeżeli Zamawiający będzie wymagał ich złożenia**

1. Zamawiający nie będzie wymagał złożenia podmiotowych środków dowodowych **do oferty** innych, z wyjątkiem oświadczeń wymienionych w art. 125 ust. 1 ustawy Prawo zamówień publicznych.
2. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w pkt 1, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

ROZDZIAŁ 22	**Opis części zamówienia, jeżeli Zamawiający dopuszcza składanie ofert częściowych**

Zamawiający **dopuszcza** możliwość składania ofert częściowych.

Część I

- **ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**
- **WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO;**

Część II

- **CERTYFIKAT SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ.**

ROZDZIAŁ 23	**Liczba części zamówienia, na którą Wykonawca może złożyć ofertę, lub maksymalna liczbę części, na które zamówienie może zostać udzielone temu samemu Wykonawcy, oraz kryteria lub zasady, mające zastosowanie do ustalenia, które części zamówienia zostaną udzielone jednemu Wykonawcy, w przypadku wyboru jego oferty w większej niż maksymalna liczbie części**

Wykonawca może złożyć ofertę na wszystkie części zamówienia

ROZDZIAŁ 24	**Informacje dotyczące ofert wariantowych, w tym informacje o sposobie przedstawiania ofert wariantowych oraz minimalne warunki, jakim muszą odpowiadać oferty wariantowe, jeżeli Zamawiający wymaga lub dopuszcza ich składanie**

Zamawiający **nie dopuszcza** możliwości składania ofert wariantowych.

ROZDZIAŁ 25	**Wymagania w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95**

Nie dotyczy.

ROZDZIAŁ 26	**Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2, jeżeli Zamawiający przewiduje takie wymagania**

Nie dotyczy.

ROZDZIAŁ 27	**Informacje o zastrzeżeniu możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94, jeżeli Zamawiający przewiduje takie wymagania**

Zamawiający **nie zastrzega** możliwości ubiegania się o udzielenie zamówienia wyłącznie wykonawców, o których mowa w art. 94 ustawy Prawo zamówień publicznych.

ROZDZIAŁ 28	**Wymagania dotyczące wadium, w tym jego kwotę, jeżeli Zamawiający przewiduje obowiązek wniesienia wadium**

Zamawiający **nie przewiduje** konieczność złożenia wadium.

ROZDZIAŁ 29	**Informacje o przewidywanych zamówieniach, o których mowa w art. 214 ust. 1 pkt 7 i 8, jeżeli Zamawiający przewiduje udzielenie takich zamówień**

Zamawiający **nie przewiduje** możliwości udzielenia zamówień z wolnej ręki o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Prawo zamówień publicznych.

ROZDZIAŁ 30	**Informacje dotyczące przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Prawo zamówień publicznych, jeżeli Zamawiający przewiduje możliwość albo wymaga złożenia oferty po odbyciu wizji lokalnej lub sprawdzeniu tych dokumentów**

Zamawiający **nie wymaga** odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia.

ROZDZIAŁ 31	**Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między Zamawiającym a wykonawcą, jeżeli Zamawiający przewiduje rozliczenia w walutach obcych**

1. Zamawiający **nie przewiduje** możliwości prowadzenia rozliczeń w walutach obcych.
2. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
3. Zamawiający nie przewiduje możliwości udzielenia zaliczek na poczet wykonania zamówienia.

ROZDZIAŁ 32	**Informacje dotyczące zwrotu kosztów udziału w postępowaniu, jeżeli Zamawiający przewiduje ich zwrot**

Zamawiający **nie przewiduje** zwrotu kosztów udziału w postępowaniu, z zastrzeżeniem art. 261.

ROZDZIAŁ 33	**Informację o obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań, jeżeli Zamawiający dokonuje takiego zastrzeżenia zgodnie z art. 60 i art. 121 ustawy Prawo zamówień publicznych**

Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań.

ROZDZIAŁ 34	**Maksymalna liczba wykonawców, z którymi Zamawiający zawrze umowę ramową, jeżeli Zamawiający przewiduje zawarcie umowy ramowej**

Zamawiający **nie przewiduje** zawarcia umowy ramowej.

ROZDZIAŁ 35	**Informacja o przewidywanym wyborze najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Prawo zamówień publicznych, jeżeli Zamawiający przewiduje aukcję elektroniczną**

Zamawiający **nie przewiduje** aukcji elektronicznej.

ROZDZIAŁ 36	**Wymóg lub możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93ustawy Prawo zamówień publicznych**

Zamawiający **nie wymaga** złożenia oferty w postaci katalogu elektronicznego.

ROZDZIAŁ 37	**Informacje dotyczące zabezpieczenia należytego wykonania umowy, jeżeli Zamawiający je przewiduje**

Zamawiający **nie wymaga** wniesienie zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ 38	**Klauzula informacyjna z art. 13 RODO do zastosowania przez Zamawiających w celu związanym z postępowaniem o udzielenie zamówienia publicznego**

Zgodnie z art. 13 ust. 1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest ***/Akademia Marynarki Wojennej im. Bohaterów Westerplatte, ul. Inż. J. Śmidowicza 69, 81-127 Gdynia/;***
- inspektorem ochrony danych osobowych w */nazwa zamawiającego/* jest Pan/~~Pani~~ ***/ mgr inż. Janusz Gawrych, kontakt: iod@amw.gdynia.pl, 261-262-644/ *;***
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego ***32/ZP/22*** prowadzonym w trybie **podstawowym (z art. 275 ust. 1 Pzp)**
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 ust. 6 oraz art. 19, art. 74 ust. 3 i 4, art. 75 i 76 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129), dalej „ustawa Pzp";
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 4 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO**.

1)rozporządzenie 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

* ***Wyjaśnienie:*** *informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych*

** ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

*** ***Wyjaśnienie:*** *prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

ROZDZIAŁ 39 Załączniki

Wykaz załączników do SWZ będących jej integralną częścią:

Załącznik nr 1	Formularz ofertowy dla części I i II
Załącznik nr 2	Opis przedmiotu zamówienia
Załącznik nr 3	Projekt umowy
Załącznik nr 4	Oświadczenie o grupie kapitałowej dla części I i II
Załącznik nr 5	Oświadczenie Wykonawcy o braku podstaw do wykluczenia dla części I i II
Załącznik nr 6	Oświadczenie z art. 117 ust 4 dla części I i II
Załącznik nr 7	Oświadczenie RODO dla części I i II
Załącznik nr 8	Oświadczenie o aktualności informacji dla części I i II
Załącznik nr 9	Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu dla części I
Załącznik nr 10	Oświadczenia podmiotu udostępniającego zasoby z art. 118 dla części I
Załącznik nr 11	Oświadczenia podmiotu udostępniającego zasoby z art. 125 ust. 5 dla części I
Załącznik nr 12	Oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia z art. 125 ust. 1 dla części I
Załącznik nr 13	Wykaz dostaw i usług dla części I
Załącznik nr 14	Wykaz osób dla części I
Załącznik nr 15-19	Oświadczenia o dysponowaniu osobami dla części I
Załącznik nr 20	Oświadczenia o dysponowaniu punktem serwisowym dla części I
Załącznik nr 21	Oświadczenia o dysponowaniu panelem serwisowym dla części I

Gdynia, …...06.2022 r.
Podpisy osób uprawnionych

WNIOSKUJĄCY
(odpowiedzialny za opis przedmiotu zamówienia, zawarcie i realizację umowy)**:**

_____
Marcin **SZULC**

UZGODNIONO Z:
(Sekcją Zamówień Publicznych w zakresie procedur Prawa zamówień publicznych)

_____
Anna **PARASIŃSKA**

UZGODNIONO Z:
(Kanclerz AMW)

_____
Marek **DRYGAS**

ZAŁĄCZNIK NR 1

FORMULARZ OFERTOWY WYKONAWCY

DANE DOTYCZĄCE WYKONAWCY

Nazwa Wykonawcy (firmy)

...../.....
Województwo

Adres Siedziby Wykonawcy (firmy)

…….....

Adres do korespondencji

……

Nr telefonu/**e-mail** …….../...../.....

NIP .....

REGON ….....

oświadczam, że jestem (*należy wybrać z listy*)

- mikroprzedsiębiorstwem,
- małym przedsiębiorstwem,
- średnim przedsiębiorstwem,
- jednoosobową działalność gospodarczą,
- osoba fizyczna nieprowadząca działalności gospodarczej,
- inny rodzaj.

Nawiązując do zamówienia ogłoszonego w trybie podstawowym bez negocjacji na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego *(32/ZP/22)*

zobowiązuję się wykonać przedmiot zamówienia za cenę:

CZĘŚĆ I *

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

cena netto.....PLN

(słownie: .....)

podatek VAT ..... PLN

cena brutto.....PLN

(słownie: .....)

Posiadamy polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę – **TAK / NIE** (niepotrzebne skreślić)

W tym:

- **Odnowienie subskrypcji na system ochrony antywirusowej i antyspamowej zasobów sieci komputerowej:**

…….netto/……brutto - zastosowano podatek VAT w wysokości .....%

- **Wsparcie techniczne systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego:**

…….netto/……brutto - zastosowano podatek VAT w wysokości .....%

Zapewniamy następujące warunki świadczenia usług serwisowych:

Czas reakcji serwisowej:	1 godzina
Miejsce świadczenia usług serwisowych	AMW

Zgłaszanie potrzeb serwisowych – wskazanie minimum 2 kontaktów	
Nazwiska osób "kontaktowych"	…….
Maile	…….
Telefony	…….
Faksy	…….
Inny sposób zgłaszania potrzeby serwisu – podać procedurę	……. …….

1) Wyrażamy zgodę na otrzymanie należności w ciągu 30 dni od daty otrzymania faktury przez Zamawiającego,
2) Zamówienie zrealizujemy sami/z udziałem podwykonawców/ w terminach:
   Część I: 29.06.2022 r. – subskrypcja na program antywirusowy
   30.06.2022 r. – przez 12 miesięcy – wsparcie techniczne
3) W przypadku zatrudnienia podwykonawców wskazujemy zakres zamówienia, którego wykonanie zamierzamy powierzyć następującym podwykonawcom:
   .....

W przypadku zatrudnienia podwykonawców odpowiadamy za ich pracę, jak za swoją własną i odpowiadamy za właściwe rozliczenie się z nimi za wykonaną pracę.

CZĘŚĆ II*

- CERTYFIKAT SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ

cena netto.....PLN

(słownie: .....)

podatek VAT ……..…….. PLN

cena brutto.....PLN

(słownie: .....)

1) Wyrażamy zgodę na otrzymanie należności w ciągu 30 dni od daty otrzymania faktury przez Zamawiającego,
2) Zamówienie zrealizujemy sami/z udziałem podwykonawców/ w terminach:
   20.08.2022 r. – certyfikat
3) W przypadku zatrudnienia podwykonawców wskazujemy zakres zamówienia, którego wykonanie zamierzamy powierzyć następującym podwykonawcom:
   .....

W przypadku zatrudnienia podwykonawców odpowiadamy za ich pracę, jak za swoją własną i odpowiadamy za właściwe rozliczenie się z nimi za wykonaną pracę.

Dla wszystkich części:

1) oświadczamy, że wybór oferty:
   - nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.
   - będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług. Powyższy obowiązek podatkowy będzie dotyczył …… (*Wpisać nazwę /rodzaj towaru lub usługi, które będą prowadziły do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług)* objętych przedmiotem zamówienia.
2) oświadczamy, że oferujemy przedmiot zamówienia zgodny z wymaganiami i warunkami określonymi przez Zamawiającego w SWZ i potwierdzamy przyjęcie warunków umownych i warunków płatności zawartych w SWZ i we wzorze umowy stanowiącym załącznik do SWZ,

Uwaga! Wykonawca zobowiązany jest do wypełnienia miejsc wykropkowanych.

Wypełnić właściwą część na którą składana jest oferta

ZAŁĄCZNIK NR 2

1. Opis przedmiotu zamówienia:
Przedmiotem zamówienia jest -

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego Przedłużenie subskrypcji i certyfikat w formie elektronicznej, wsparcie techniczne – usługa świadczona na miejscu lub zdalnie.

(32/ZP/22)

Część I:
Dostawa: Odnowienie rocznej subskrypcji na system ochrony antywirusowej

Roczna subskrypcja od 29.06.2022 r. na kompletny system ochrony antywirusowej i antyspamowej z centralnym zarządzaniem dla wszystkich urządzeń komputerowych w łącznej ilości 1200 sztuk obejmujący:

- Ochronę antywirusową i antyspamową dla sieci komputerowej składającej się z komputerów i serwerów z systemami operacyjnymi: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, Mac OS, Windows 2003 R2 Server, Windows 2008 R2 Server, Windows 2012 R2 Server, Windows 2016 Server, Windows 2019 Server;
- Ochronę urządzeń mobilnych (tablety i smartfony);
- Ochronę antywirusową i antyspamową dla kontrolerów domeny Windows Server 2016, klastra Hyper-V systemu Windows Server 2008 R2, klastra Hyper-V systemu Windows Server 2016, Windows 2019 Server, serwera plików, drukarek, systemu Microsoft Exchange 2016 (dwa serwery w DAG), serwera kopii zapasowych Microsoft DPM 2016, serwera FTP, WSUS, serwerów aplikacji;
- System centralnego zarządzania ochroną antywirusową i antyspamową sieci komputerowej;

Zamawiający informuje, że aktualnie używa systemu antywirusowego ESET Endpoint Security.

Usługa: Wsparcie techniczne

Wsparcie techniczne środowiska serwerowego oraz systemu ochrony antywirusowej i antyspamowej składającego się z:

- serwerów i macierzy dyskowych,
- domeny Active Directory,
- środowiska aktualizacji Windows Software Update Services
- środowiska wymiany plików Windows Server
- środowiska zarządzania usługami pulpitu zdalnego Remote Desktop Services
- środowiska wirtualnego Microsoft Hyper-V,
- środowiska do zarządzania wirtualizacją Microsoft SCVMM
- środowiska systemu poczty Microsoft Exchange
- środowiska kopii zapasowych Microsoft System Center DPM .

W skład fizycznego środowiska serwerowego wchodzą:

- 2 kontrolery domeny z systemami Windows 2016 Serwer,
- 2 serwery Microsoft Exchange 2016 pracujące w klastrze DAG,
- 2 serwery kopii zapasowych jeden z systemem Microsoft DPM 2016 z systemem Windows Server 2016, drugi z systemem Microsoft DPM 2019 z systemem Windows Server 2016
- klaster dwuwęzłowy Hyper-V maszyn wirtualnych z systemami Windows 2008 R2 wraz z macierzami dyskowymi

- klaster trzywęzłowy Hyper-V maszyn wirtualnych z systemami Windows 2019 wraz z macierzami dyskowymi
- 2 serwery z konsolą do zarządzania maszynami wirtualnymi Microsoft SCVMM 2012 R2 oparty na systemie Windows Server 2012 R2, drugi z systemem Microsoft SCVMM 2019.
- serwer do zarządzania usługami pulpitu zdalnego z systemem Windows Server 2019,
- serwer do uwierzytelniania stacji roboczych z protokołem Radius

Na platformie wirtualnej pracują następujące maszyny wirtualne:

- serwery aplikacji Windows oraz Linux,
- serwer do zarządzania drukowaniem z systemem Windows Server 2016
- serwer plików z systemem Windows Server 2016
- serwer do zarządzania aktualizacjami WSUS z systemem Windows Server 2019,
- serwer ochrony antywirusowej i antyspamowej z konsolą do zarządzania ESET Protect 9.0 oparty na systemie Windows Server 2016,
- serwer FTP z systemem Windows 2008 R2 Server
- serwer zarządzania macierzami Dell z systemem Windows Server 2012 R2.

Część II: Dostawa

Certyfikatu SSL Wildcard z roczną subskrypcją o parametrach nie gorszych niż:

- zgodność ze standardem X.509 v.3 (RFC5280),
- zabezpieczony funkcją skrótu SHA2,
- obsługa siły szyfrowania połączeń do 256 bitów,
- wsparcie dla SGC (Server Gated Cryptography),
- obsługa kluczy o długości 4096 bitów i więcej,
- minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571,
- wydany przez CERTUM PCC posiadający aktualny certyfikat zgodności ze standardami Web-Trust,
- możliwa weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP.

Parametry/wymagania techniczne i jakościowe odnoszące się do przedmiotu zamówienia

Oprogramowanie antywirusowe

Ochrona stacji roboczych - Windows

1. Pełne wsparcie dla systemów operacyjnych Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Rozwiązanie musi wspierać architekturę ARM64
5. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
6. Pomoc w programie (help) i dokumentacja do programu ma być dostępna co najmniej w języku polskim oraz angielskim.
7. Skuteczność programu ma być potwierdzona nagrodami VB100 i AV-comparatives.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Administrator ma mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
15. Rozwiązanie musi mieć możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. Rozwiązanie musi mieć możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
21. Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
23. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP musi odbywać się „w locie" (w czasie rzeczywistym), zanim zostanie ona dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
24. Rozwiązaniu musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Rozwiązanie musi mieć możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Rozwiązanie musi mieć możliwość skanowania ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch ma być automatycznie blokowany, a użytkownikowi wyświetlane ma być stosowne powiadomienie.

27. Rozwiązanie musi posiadać możliwość blokowania przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
28. Musi istnieć możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
31. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
32. Musi istnieć możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
34. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
37. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
38. Program ma posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
39. Musi być możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (bez ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
40. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Musi być też możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. Program ma mieć możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
44. Powinna być też możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformowania o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
47. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacji krytycznych, aktualizacji ważnych, aktualizacji zalecanych oraz aktualizacji o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
48. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.

49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
51. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
52. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
54. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
55. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
57. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem użytkownika.
58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
62. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
63. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
64. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
65. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
66. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
67. Ma być automatyczna, inkrementacyjna aktualizacja silnika detekcji.

68. Ma istnieć możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
69. Ma być możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
72. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
73. Program ma być wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
65. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
66. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
67. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
68. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
69. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
70. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
71. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
72. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
73. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
74. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
75. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
76. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
77. Administrator ma mieć możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
78. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
79. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
80. Musi być możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji ma być w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
81. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
82. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
83. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

84. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
85. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
86. Administrator ma mieć możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
87. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść".
88. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
89. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
90. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
91. Program ma mieć wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
92. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
93. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
94. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona stacji roboczych Apple Mac OS X

1. Ma mieć pełne wsparcie dla systemów Mac OS X 10.9 lub nowszych.
2. Wersja programu ma być dostępna co najmniej w języku polskim oraz angielskim.
3. Pomoc w programie (help) ma być co najmniej w języku polskim oraz angielskim.
4. Program musi zapewnić pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi wykrywać i usuwać niebezpieczne aplikacje typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
7. Ma skanować w czasie rzeczywistym otwierane, tworzone i wykonywane pliki.
8. Ma mieć możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Rozwiązanie ma mieć możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchamiania z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
10. Musi istnieć możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Rozwiązanie ma mieć możliwość skanowania plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Instalacja programu nie może wymuszać ponownego uruchomienia (restartu) komputera.
14. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15. Powinny być wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
16. Program musi mieć możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.
17. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie może wymagać ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie

mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
18. Musi istnieć możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
19. Musi być możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
20. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".
21. Program ma posiadać funkcję blokowania nośników wymiennych: płyt CD/DVD, pamięci masowej, sieci, drukarki USB, urządzeń do tworzenia obrazów, portów szeregowych, urządzeń przenośnych.
22. Musi istnieć automatyczna, inkrementacyjna aktualizacja silnika detekcji.
23. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.
24. Program ma obsługiwać pobieranie aktualizacji za pośrednictwem serwera proxy.
25. Program ma umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
26. Program ma być wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
27. Dziennik zdarzeń ma rejestrować informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanego skanowania komputera.
28. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
29. Program musi posiadać mechanizm ochrony dostępu do stron internetowych który monitoruje komunikację w ramach protokołu HTTP.
30. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.
31. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" modyfikację konfiguracji programu.
32. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
33. Ma być możliwość zdalnego zarządzania programem z poziomu administracji zdalnej.
34. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP ma odbywać się "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
35. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
36. Rozwiązanie musi umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
37. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
38. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
39. Zapora osobista rozwiązania musi pracować w jednym z 2 trybów:
    - Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
    - Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
40. Rozwiązanie musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
41. Również możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
42. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.

43. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
44. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
45. Ma tworzyć profil pracy zapory osobistej w zależności od wykrytej sieci.
46. Administrator musi mieć możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
47. Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, sieć wifi, podsieć IPv4/IPv6, zakres adresów IPv4/IPv6, adres IPv4/IPv6.
48. Kontrola dostępu do stron internetowych
    - Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
    - Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
    - Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
    - Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
    - Aplikacja musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
    - Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
    - Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
    - Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

Ochrona urządzeń mobilnych opartych o system Android

1. Wspierany system: od Android 5.0.
2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższą.
3. Rozwiązanie musi wspierać procesory ARM z obsługą ARMv7 lub x86 Intel Atom.
4. Ochrona plików w czasie rzeczywistym.
5. Ochrona przed atakami typu „phishing”.
6. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
10. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

12. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Ochrona przed kradzieżą:

16. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
17. W przypadku kradzieży urządzenia, administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,
b. przywrócenie urządzenie do ustawień fabrycznych,
c. zablokowanie urządzenia,
d. uruchomienie sygnału dźwiękowego,
e. lokalizację GPS.

Polityka ustawień:

18. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
    a. połączenie Wi-Fi,
    b. GPS,
    c. usługi lokalizacyjne,
    d. pamięć,
    e. roaming danych,
    f. roaming połączeń,
    g. nieznane źródła,
    h. tryb debugowania,
    i. komunikację NFC,
    j. szyfrowanie pamięci masowej,
    k. urządzenie zrootowane.

Kontrola aplikacji:

19. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
20. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
21. Blokowanie aplikacji musi być możliwe w oparciu o:
    a. nazwę aplikacji,
    b. nazwę pakietu,
    c. kategorię sklepu Google Play,
    d. uprawnienia aplikacji,
    e. pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:

22. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
    a. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
    b. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
    c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
    d. czas, po którym automatycznie nastąpi blokada ekranu,
    e. ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje sygnatur:

23. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
24. Aplikacja ma mieć możliwość określenia harmonogramu, zgodnie z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
25. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

26. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
27. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
28. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
29. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.
30. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:
    a. za pomocą kodu QR,
    b. za pomocą unikatowego łącza,
    c. za pomocą wiadomości e-mail,

31. W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).

Ochrona stacji roboczych Linux

1. Rozwiązanie ma wspierać systemy operacyjne Ubuntu,18.4/20.4 LTS 64-bit, Red Hat Enterprise Linux 7, 8 64 bit, SUSE Linux Enterprise Desktop.
2. A także wsparcie dla dystrybucji 64-bitowych.
3. Pomoc w programie (help) ma być dostępna co najmniej w języku polskim i angielskim.
4. Program ma zapewnić pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Program ma wykrywać i usuwać niebezpieczne aplikacje typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Ma mieć wbudowaną technologię do ochrony przed rootkitami.
7. Program ma skanować w czasie rzeczywistym otwierane, tworzone i wykonywane pliki.
8. Ma być możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Program ma skanować pliki spakowane i skompresowane.
10. Ma być możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11. Instalacja programu nie może wymagać ponownego uruchomienia (restartu) komputera.
12. Program ma mieć wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
13. Musi istnieć możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
14. Musi być możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymagana ma być ingerencja użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie,.
15. Musi istnieć możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
16. W programie ma być automatyczna, inkrementacyjna aktualizacja silnika detekcji.
17. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, , a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
18. Program ma obsługiwać pobieranie aktualizacji za pośrednictwem serwera proxy.
19. Program ma być wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20. Program ma umożliwiać importowanie oraz eksportowanie ustawień oraz zdalnie za pomocą dedykowanego narzędzia.
21. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona serwera Windows :

1. Rozwiązanie musi posiadać wsparcie dla systemów: Microsoft Windows 2008 R2 i nowszych
2. Instalator musi umożliwiać wybór wersji językowej programu przed rozpoczęciem procesu instalacji.
3. Rozwiązanie musi zapewnić pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami i exploitami.

6. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje
7. Rozwiązanie musi posiadać mozliwość skanowania w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie ma mieć możliwość uruchomiania z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
10. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
11. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
12. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
13. Rozwiązanie musi mieć możliwość skanowania dysków sieciowych i dysków przenośnych.
14. Rozwiązanie musi mieć możliwość skanowania plików spakowanych i skompresowanych.
15. Musi istnieć możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
21. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
22. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
23. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
24. Aplikacja musi posiadać funkcjonalność odpytywania na bieżąco serwerów producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
25. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD, pamięci masowych FireWire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
26. Funkcja blokowania nośników wymiennych bądź grup urzadzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o: typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia lub model urządzenia.
27. Aplikacja musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
28. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.

29. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
30. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
32. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
34. Dodanie automatycznych wyłączeń nie powinno wymagać restartu serwera.
35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
37. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
38. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
39. Musi być możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
40. Program ma mieć wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
41. Musi istnieć możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie może być wymagana ingerencja użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie
42. Musi być możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Musi być możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. W przypadku wykrycia zagrożenia, musi być możliwość wysłania ostrzeżenia do użytkownika i/lub administratora poprzez e-mail.
46. Musi istnieć możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik obsługujący serwer przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
47. Ma być możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora - przy próbie deinstalacji program ma pytać o hasło.
48. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji ma być takie samo.
49. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – ma poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
50. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
51. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.

52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach sieciowych, harmonogramie systemu operacyjnego, pliku hosts, sterownikach.
55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
57. Aktualizacja baz wirusów i innych zagrożeń powinna być automatyczna i inkrementacyjna.
58. Musi istnieć możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
59. Musi być możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
60. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
61. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
62. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
63. System antywirusowy ma być wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
64. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
65. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
66. Dziennik zdarzeń ma rejestrować informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
67. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
68. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
69. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
70. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
71. Program ma mieć wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
72. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
73. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
74. Aplikacja ma mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
75. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
76. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
77. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
78. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

Ochrona serwera - Linux

Architektura rozwiązania

1. Rozwiązanie musi posiadać skaner antywirusowy i antyspyware.
2. Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Oprogramowanie musi posiadać wbudowany mechanizm typu „watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikro-serwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Rozwiązanie musi posiadać wsparcie dla SecureBoot-a
8. Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i ma obejmować skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
12. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie „Permissive" jak i „Enforcing".
13. Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7, Centos 8.
14. Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ma pozwalać na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
16. Musi istnieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
17. Administrator ma mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
18. Oprogramowanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
19. Rozwiązanie musi wspierać system plików zamontowany z flagą „noexec".
20. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających „w tle", z możliwością ustawienia dla nich niskiego priorytetu.
21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

Interfejs graficzny

1. Produkt musi pozwalać na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników w lokalnej konsoli administracyjnej.
8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.
9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

Skanowanie sieciowych systemów plików

1. Oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Oprogramowanie antywirusowe nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Oprogramowanie antywirusowe do celów skanowania plików na rozwiązaniach NAS / SAN musi w pełni wspierać rozwiązanie Dell EMC Isilon.

Instalacja

1. Oprogramowanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.
2. Oprogramowanie antywirusowe musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.
3. Aktualizacja silnika detekcji musi być automatyczna i inkrementacyjna.
4. Oprogramowanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL) 7 64-bit, CentOS 7 64-bit, Ubuntu Server 16.04 LTS 64-bit, Ubuntu Server 18.04 LTS 64-bit, Debian 9 64-bit, SUSE Linux Enterprise Server (SLES) 12 64-bit, SUSE Linux Enterprise Server (SLES) 15 64-bit, Oracle Linux oraz Amazon Linux

Licencjonowanie

1. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
2. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

Ochrona przed spamem

1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Musi istnieć możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Musi być możliwe ręczne dodanie nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Rozwiązanie musi posiadać możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
9. Program ma posiadać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
10. Program ma posiadać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

1. Zapora osobista ma pracować w jednym z 4 trybów:

- tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące;
- tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie;
- tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora;
- tryb uczenia się – oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji, a administrator określa czas działania trybu;

2. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.
3. Musi istnieć możliwość tworzenia list sieci zaufanych.
4. Musi istnieć możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
5. Musi być możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
6. Musi istnieć możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
7. Pożądana jest możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
8. Ma być możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
9. Program ma wykrywać modyfikacje w aplikacjach korzystających z sieci i powiadamiać o tych zdarzeniach.
10. Ma umożliwiać tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma mieć możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
12. Profile mają mieć możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.

13. Autoryzacja stref ma się odbywać m.in. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowanie sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
15. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
16. Program musi posiadać kreator, który umożliwia rozwiązanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:

- z aplikacją lokalną, którą administrator wskazuje z listy;
- z połączeniem z urządzeniem zdalnym na podstawie jego adresu IP.

Kontrola dostępu do stron internetowych

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
3. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i podkategorii.
4. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
5. Moduł musi posiadać także możliwość grupowania kategorii oraz adresów stron internetowych.
6. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych – zezwól, zezwól i ostrzeż, blokuj.
9. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach strony internetowej.

Bezpieczna przeglądarka

10. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
11. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
12. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
13. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
14. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
15. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

Administracja zdalna

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
55. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
61. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Musi istnieć możliwość wysłania raportu za pośrednictwem wiadomości email, zapisania do pliku w formacie PDF, CSV oraz PS.
70. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
71. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
72. Powiadomienia mailowe mają być wysyłane w formacie HTML.
73. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.

74. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
75. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
76. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
77. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
78. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
79. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
80. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
81. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
82. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
83. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
84. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
85. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
86. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
87. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
88. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
89. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
90. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputerów oraz szablonów grup dynamicznych.
91. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
92. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
93. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
94. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Serwer 2008 R2 i nowszych
2. Musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010(SP1,SP2)/2013/2016/2019.
3. Musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.

4. Aplikacja musi umożliwiać administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane.
5. Aplikacja musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
6. Program ma zapewnić skanowanie bezpośrednio w storach Exchange przy pomocy VSAPI.
7. Program musi mieć możliwość zdefiniowania ilości wątków skanujących w celu optymalizacji pracy serwera. Zakres wątków skanowania: od 1 do 21.
8. Program ma zapewnić skanowanie przed zapisaniem wiadomości w storze przy pomocy transport agenta.
9. W przypadku wykrycia wirusa/blokowania wiadomości system musi umożliwić usunięcie wiadomości/załącznika i podmianę załącznika na czysty plik zawierający jedynie informację o infekcji.
10. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości, w tym co najmniej po: zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
11. Program musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail.
12. Aplikacja musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange.
13. Program musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
14. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
15. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL z których będzie korzystać aplikacja.
16. Program ma posiadać mechanizmy greylistingu (szare listy).
17. Aplikacja musi posiadać możliwość tworzenia wyjątków dla mechanizmu greylistingu.
18. Program ma posiadać możliwość stworzenia kwarantanny poczty per użytkownik.
19. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki www.
20. Pliki zapisywane w katalogu kwarantanny powinny być szyfrowane.
21. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie, w tym co najmniej mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie.
22. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki www.
23. Aplikacja musi umożliwiać przesyłanie raportów dotyczących plików poddanych kwarantannie na wskazany adres e-mail.
24. Program musi umożliwiać pominięcie reguł kwarantanny podczas zwolnienia wiadomości e-mail w środowisku klastrowym.
25. Musi istnieć możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera "na żądanie" lub według harmonogramu.
26. Ma wykrywać niebezpieczne aplikacje typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor itp.
27. Rozwiązanie ma mieć wbudowaną technologię do ochrony przed rootkitami.
28. Ma mieć wbudowaną technologię ochrony przed atakami typu backscatter.
29. Aplikacja musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI.
30. Program ma mieć wbudowany skaner UEFI.
31. Aplikacja musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS).
32. Aplikacja musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku.
33. Aplikacja musi wyświetlać powiadomienia po wykryciu ataku.
34. Aplikacja musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB.
35. Aplikacja musi odmawiać połączenia starym (nieobsługiwanym) dialektom protokołu SMB oraz zabezpieczeniom tego protokołu bez rozszerzeń zabezpieczeń.

36. Aplikacja musi umożliwiać komunikację z usługą menadżera konta zabezpieczeń, urzędu zabezpieczeń lokalnych, rejestru zdalnego, service control manager, usługą serwera i innymi usługami.
37. Ma być wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe.
38. Aplikacja musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS.
39. Aplikacja musi umożliwiać określenie białej listy domen, dla których analiza protokołów SSL/TLS nie będzie wykonywana.
40. Program ma wykonywać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
41. Program ma wykonywać skanowanie plików spakowanych i skompresowanych.
42. Ma mieć wbudowaną technologię monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci botnet.
43. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 i nowszych).
44. Aplikacja musi w momencie instalacji na serwerze wykrywać usługi jakie są zainstalowane i tworzyć dla nich odpowiednie wyjątki.
45. Zainstalowana aplikacja musi wykorzystywać technologię chmury w celu przyśpieszenia reakcji na nowe zagrożenia oraz optymalizacji samego procesu skanowania.
46. Program musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta.
47. Program musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy SPAM.
48. Program musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy, np. plików zawierających informacje poufne.
49. Aplikacja musi umożliwiać zapisywanie informacji diagnostycznych w dziennikach dla aparatu antyspamowego.
50. Aplikacja musi być wyposażona w mechanizm chroniący serwer przed exploitami i atakami typu 0-day.
51. Aplikacja musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
52. Zainstalowany system ochrony musi być wyposażony w system HIPS.
53. Aplikacja musi w natywny sposób wspierać środowiska klastrowe.
54. System musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.
55. Aplikacja musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
56. Program ma skanować i czyścić w czasie rzeczywistym pocztę przychodzącą i wychodzącą obsługiwaną przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Windows Live Mail zainstalowanego lokalnie na serwerze pocztowym.
57. Program ma mieć wbudowaną ochronę przed atakami typu phishing w wiadomościach e-mail.
58. Aplikacja musi umożliwiać skanowanie w środowiskach hybrydowych opartych na MS Office 365.
59. Aplikacja musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu.
60. Aplikacja musi tworzyć log ochrony protokołu SMTP.
61. Musi istnieć możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchamiania z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności) .
62. Aplikacja musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego programu.
63. Program musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
64. Musi istnieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów.
65. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik.

66. Aplikacja musi być wyposażona w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).
67. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie.
68. Aplikacja musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – bez ingerencji użytkownika.
69. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu aplikacji i nie można do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie.
70. Program musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
71. W przypadku wykrycia wirusa, program ma mieć możliwość wysłania ostrzeżenie do administratora poprzez e-mail.
72. Aplikacja musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
73. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
74. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie programu antywirusowego oraz jego odinstalowanie.
75. Aplikacja musi w sposób automatyczny i przyrostowy dokonywać aktualizacji silnika detekcji.
76. Aktualizacja musi być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy ma mieć wbudowany serwer HTTP).
77. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP
78. Aplikacja musi wspierać aktualizacje za pośrednictwem serwera Proxy.
79. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchamiania z własnymi ustawieniami.
80. Aplikacja musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP.
81. Aplikacja musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczących uruchomionych procesów, aktywności procesora, o działania dysku.
82. Aplikacja musi rejestrować komunikację produktu z serwerami licencji producenta.
83. Aplikacja musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy.
84. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8), Ascii (7-bit), Japanese (ISO-2022-JP), lokalne.
85. Rozwiązanie musi posiadać wsparcie dla RMM (Remote Monitoring and Management).
86. Aplikacja musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
87. Aplikacja musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
88. Aplikacja musi być wyposażona w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług.
89. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
90. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.
91. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark).
92. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

<u>Zakres czynności do wykonania w ramach wsparcia technicznego:</u>

1. Identyfikacja potencjalnych problemów w działaniu serwerów na bazie logów i dzienników zdarzeń oraz podjęcie czynności naprawczych.

2. Optymalizacja konfiguracji systemów na bazie monitoringu wydajności serwerów.
3. Instalacja i testowanie poprawek zbiorczych wydawanych przez Microsoft dla serwerów i systemów objętych wsparciem technicznym.
4. Zmiany w konfiguracjach zadań tworzenia kopii zapasowych serwerów mające na celu usuwanie nieprawidłowości po konsultacji z administratorami.
5. Optymalizacja działania kontrolerów domeny poprzez weryfikację: ustawień zasad grup w GPO i dystrybucji zasad grup do użytkowników, replikacji danych usług katalogowych, poprawności rozwiązywania nazw DNS.
6. Odnawianie certyfikatów oraz weryfikacja poprawności działania serwera certyfikatów.
7. Dokumentowanie rozwiązywanych problemów w raportach.

Serwer WSUS:

1. Weryfikacja procedur aktualizacji oprogramowania Microsoft na serwerze i stacjach roboczych.
2. Weryfikacja poprawności pobierania aktualizacji oprogramowania serwera WSUS z witryny Microsoft.
3. Rozwiązywanie problemów dotyczących stacji, na których występują błędy aktualizacji w uzgodnieniu z administratorami.
4. Instalacja nowych wersji i poprawek WSUS.

Serwer plików

1. Identyfikacja potencjalnych problemów w działaniu serwerów poprzez weryfikację: dzienników zdarzeń, stanu logów i sprawdzenie poprawności funkcjonowania usług serwera plików oraz podjęcie czynności naprawczych.
2. Nadzór nad sprawną i bezawaryjną pracą serwera.
3. Pomoc w rozwiązywaniu problemów z dostępnością usług sieciowych.

System antywirusowy i antyspamowy dla serwerów i stacji roboczych:

1. Aktualizacja oprogramowania do aktualnych wersji.
2. Weryfikacja procedur ochrony przed wirusami.
3. Nadzór nad sprawną i bezawaryjną pracą serwera antywirusowego;
4. Weryfikacja poprawności pobierania aktualizacji sygnatur i oprogramowania antywirusowego.
5. Optymalizacja dystrybucji sygnatur wirusów pobranych na serwery i stacje klienckie.
6. Weryfikacja stacji, na których występują błędy aktualizacji, usuwanie nieprawidłowości w tym zakresie w uzgodnieniu z administratorami.

Serwer poczty elektronicznej Exchange 2016:

1. Identyfikacja potencjalnych problemów w działaniu serwerów poprzez weryfikację: dzienników zdarzeń, stanu logów i sprawdzenie poprawności funkcjonowania usług serwera poczty oraz podjęcie czynności naprawczych .
2. Pomoc w rozwiązywanie problemów z dostępnością systemu pocztowego za pomocą przeglądarek z sieci wewnętrznej i zewnętrznej.
3. Optymalizacja struktury logicznej (nazewnictwo skrzynek użytkowników, list dystrybucyjnych) i fizycznej (np. ilość skrzynek w grupach magazynowania) systemu poczty
4. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera poczty dystrybuowanych przez producenta systemu firmę Microsoft.
5. Pomoc w rozwiązywaniu problemów związanych z przesyłaniem poczty.

System antywirusowy i antyspamowy dla serwera poczty elektronicznej Exchange:

1. Konfiguracja reguł filtrowania poczty pod względem wirusów, robaków i spamu oraz reguł filtrowania treści wiadomości i załączników.
2. Konfiguracja treści powiadomień w zależności od przesyłanych komunikatów.
3. Instalacja i testowanie poprawek do oprogramowania antywirusowego dla serwera poczty dystrybuowanych przez producenta systemu.

System kopii zapasowych Microsoft SCDPM

1. Weryfikacja poprawności wykonywania zadań kopii zapasowych systemu Exchange.
2. Optymalizacja zadań kopii zapasowych w uzgodnieniu z administratorami.
3. Odtwarzanie na żądanie skrzynek użytkowników z okresu objętego ochroną.
4. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera kopii zapasowych dystrybuowanych przez producenta systemu firmę Microsoft.
5. Rozwiązywanie problemów związanych z działaniem serwera.
6. Przenoszenie zadań kopii zapasowej między serwerami SCDPM12 i SCDPM19

System zarządzania maszynami wirtualnymi Microsoft SCVMM

1. Identyfikacja potencjalnych problemów w działaniu serwera poprzez weryfikację: dzienników zdarzeń, stanu logów i sprawdzenie poprawności funkcjonowania usług oraz podjęcie czynności naprawczych.
2. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera SCVMM dystrybuowanych przez producenta systemu firmę Microsoft.
3. Rozwiązywanie problemów związanych z zarządzaniem maszynami wirtualnymi.

Środowisko wirtualne Hyper-V:

1. Utrzymanie ciągłości pracy maszyn wirtualnych (reakcja na awarie), w tym usuwanie problemów sprzętowych i oprogramowania.
2. Optymalizacja konfiguracji węzłów klastra do pracy z macierzami.
3. Przygotowanie procedur archiwizacji i odtwarzania maszyn wirtualnych.
4. Optymalizacja działania maszyn wirtualnych.
5. Przygotowanie szablonów maszyn wirtualnych dla wybranych systemów operacyjnych.

W ramach wsparcia technicznego zamawiający wymaga od Wykonawcy następujących usług:

- Stałej wizyty serwisowej, trwającej minimum 8 godzin, realizowanej raz w miesiącu w ustalonym dniu każdego miesiąca. Celem wizyty ma być kontrola działania wszystkich systemów objętych umową i rozwiązywanie bieżących problemów. Dokładny zakres czynności do wykonania jest opisany powyżej. Łączna ilość czasu poświęconego na planowane wizyty serwisowe ma wynosić 12 dni roboczych rocznie.
- Wsparcia-serwisu w zakresie usuwania awarii i problemów związanych z działaniem ww. środowiska serwerowego.
  Czas reakcji Wykonawcy na zgłoszony problem – maksymalnie 1 godzina od zgłoszenia w każdym dniu roku, o każdej porze.
  „Reakcja" – przybycie serwisanta do siedziby Zamawiającego i przystąpienie do usuwania awarii. Na świadczenie wsparcia-serwisu przeznaczonych ma być minimum 18 dni roboczych rocznie.
- Wykonawca dołączy informację o sposobie zgłaszania problemów i adresie punktu serwisowego, umożliwiającego dotarcie do siedziby Zamawiającego w ciągu 1 godziny od zgłoszenia awarii.
- Świadczenie wsparcia przez 12 miesięcy od 30.06.2022 r.

ZAŁĄCZNIK NR 3
projekt

Część I

UMOWA nr ……..……projekt

zawarta w dniu …… r. w Gdyni pomiędzy:

Akademią Marynarki Wojennej im. Bohaterów Westerplatte, ul. Śmidowicza 69, 81-127 Gdynia, **NIP: 586-010-46-93,**
reprezentowaną przez: *:*
Kanclerza – Marka Drygasa, upoważnionego do działania na mocy pełnomocnictwa **Rektora-Komendanta AMW- kontradmirała prof. dr hab. Tomasza Szubrychta,**
zwaną dalej **Zamawiającym,**

a

firmą:
……
wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej w dniu ……., pod numerem **NIP: ……., REGON …….** reprezentowaną przez **……** ,
zwaną dalej **Wykonawcą**,

zwanymi dalej łącznie Stronami, a każdy indywidualnie Stroną,

o następującej treści:

§1

1. W wyniku wyboru oferty Wykonawcy, w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji na podstawie art. 275 pkt 1 ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych (t.j. Dz.U. z 2021 r. poz. 1129 z późn. zm.)**,** o nr ……., **część 1** w dniu ……., Wykonawca zrealizuje na rzecz Zamawiającego następujące świadczenia:

1. odnowienie SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
2. usługę WSPARCIA TECHNICZNEGO SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO,

zgodnie i na szczegółowych zasadach określonych w ofercie złożonej w postępowaniu przetargowym.

§2

Wykonawca oświadcza, że:

1. Jest uprawniony oraz posiada niezbędne kwalifikacje do pełnej realizacji przedmiotu Umowy.
2. Realizowany przedmiot Umowy może być wykorzystywany bez naruszania praw własności osób trzecich, w tym praw patentowych i praw autorskich.
3. Realizowany przedmiot Umowy spełnia normy przewidziane prawem polskim.

§3

1. Umowa zostaje zawarta ze skutkiem na dzień 30.06.2022 r. i obowiązywać będzie przez 12 miesięcy licząc od tego dnia.
2. Realizacja przedmiotu Umowy w przedmiocie odnowienia subskrypcji odbędzie się dnia 29.06.2022 r.
3. Usługa wsparcia techniczne realizowana będzie przez 12 miesięcy licząc od dnia 30.06.2022 r.
4. Odbiór przedmiotu Umowy tytułem dostarczenia subskrypcji nastąpi na podstawie protokołu przekazania/odbioru podpisanego przez obie Strony.
5. Wykonawca ma obowiązek osobistego wykonania całości zamówienia.

6. W przypadku przekroczenia terminu określonego w ust. 1 i 2 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% ceny określonej w § 4 ust. 1 za każdy dzień opóźnienia, nie więcej jednak niż 20% ceny.
7. Za odstąpienie od Umowy z przyczyn niezależnych od Zamawiającego Wykonawca zapłaci karę umowną w wysokości 20% wartości niewykonanego zakresu Umowy.
8. Za każdą zwłokę w usunięciu wad przedmiotu zamówienia, ujawnionych w okresie gwarancji – Wykonawca zapłaci karę umowną w wysokości 0,5% wartości przedmiotu Umowy za każdy dzień zwłoki liczony od dnia wyznaczonego na ich usunięcie, nie więcej jednak niż 20% ceny.
9. Zamawiający zastrzega sobie prawo potrącenia równowartości naliczonych kar umownych z wynagrodzenia Wykonawcy wynikającego z wystawionej przez Wykonawcę faktury.
10. Jeżeli szkoda spowodowana niewykonaniem lub nienależytym wykonaniem Umowy przekroczy wartość zastrzeżonych kar umownych, bądź wynika z innych tytułów niż zastrzeżone, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego do pełnej wysokości szkody.
11. Łączna wysokość kar umownych, których może dochodzić każda ze stron wynosi 40% ceny określonej w § 4 ust. 1 niniejszej Umowy.

§4

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy kwotę brutto w łącznej wysokości **……..zł**
   (słownie: …….. zł …… groszy).
2. Zapłata nastąpi zgodnie z ofertą, po wykonaniu przedmiotu umowy w następujących transzach:

a. tytułem dostarczenia subskrybcji – kwota ……. zł, płatna po podpisaniu przez Zamawiającego protokołu zdawczo/odbiorczego;
b. tytułem usługi wsparcia technicznego – kwota ……. zł, płatna w 12-tu równych miesięcznych ratach na podstawie wystawionych faktur VAT.

3. Ww. płatności realizowane będą przelewem w terminie 30 dni od doręczenia prawidłowo wystawionej faktury VAT, z konta Zamawiającego:

SANTANDER BANK POLSKA SA
95 1500 1881 1210 2003 3251 0000

na konto **Wykonawcy** w:
……
przy czym za dzień zapłaty Strony Umowy przyjmują datę obciążenia rachunku **Zamawiającego**.

§5

Wykonawca deklaruje następujące warunki serwisu:

Czas reakcji serwisowej:	1 godz.
Miejsce świadczenia usług serwisowych	AMW

Zgłaszanie potrzeb serwisowych – wskazanie minimum 2 kontaktów	
Nazwiska osób "kontaktowych"	
e-maile	
Telefony	
Faksy	
Inny sposób zgłaszania potrzeby serwisu – wg załączonej procedury	

§6

Uprawnienia z tytułu rękojmi nie są wyłączone.

§7

Wszystkie zmiany Umowy wymagają zgody obu Stron w formie pisemnej pod rygorem nieważności, z uwzględnieniem art. 455 Prawa zamówień publicznych.

§8

Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osoby trzecie bez uprzedniej pisemnej zgody **Zamawiającego**.

§9

W sprawach nieuregulowanych niniejszą Umową będą miały zastosowanie odpowiednie przepisy ustawy Prawo zamówień publicznych oraz kodeksu cywilnego.

§10

a) Zakres świadczenia **Wykonawcy** wynikający z Umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
b) Umowa jest nieważna w części wykraczającej poza określenie przedmiotu zamówienia zawartego w specyfikacji istotnych warunków zamówienia.
c) Zakazuje się zmian postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub w specyfikacji istotnych warunków zamówienia oraz określił warunki takiej zmiany.
d) Zamawiający może odstąpić od umowy:

1. w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu;
2. jeżeli zachodzi co najmniej jedna z następujących okoliczności:
   1) dokonano zmiany umowy z naruszeniem art. 454 i art. 455,
   2) Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108,
   3) Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.

e) Z zastrzeżeniem przepisów odrębnych, Umowa podlega unieważnieniu w przypadkach określonych w art. 457 Prawa zamówień publicznych.
f) Strony zgodnie oświadczają, iż tryb przewidziany w ustawie z dnia 11.09.2019 Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) i aktach wykonawczych do tej ustawy został zachowany.
g) Zamawiający, zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t. j. Dz. U. z 2021 r. poz. 424), oświadcza iż posiada status dużego przedsiębiorcy.
h) Strony zgodnie oświadczają, że zmiany: stawki podatku od towarów i usług oraz podatku akcyzowego, wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub ubezpieczenie zdrowotne, zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. poz. 2215 oraz z 2019 r. poz. 1074 i 1572) - nie będą miały wpływu na koszty wykonania zamówienia przez Wykonawcę.

§11

- W czasie wykonywania niniejszej Umowy oraz w okresie gwarancji (rękojmi), **Wykonawca** jest zobowiązany do pisemnego powiadamiania Zamawiającego :

1. o zmianie siedziby Wykonawcy,
2. o upadłości Wykonawcy,
3. o wszczęciu postępowania układowego,
4. o ogłoszeniu likwidacji,
5. o zawieszeniu działalności,
6. o zmianie w zakresie rejestracji działalności Wykonawcy.

- O wystąpieniu powyższych okoliczności, Wykonawca zobowiązany jest powiadomić Zamawiającego najpóźniej w terminie 3 dni od ich zaistnienia pod rygorem naliczenia kary umownej w wysokości 1 % ceny określonej w § 4 ust. 1 za każdy przypadek naruszenia.

§12

1. Spory wynikłe na tle realizacji niniejszej Umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
2. W przypadku rozbieżności pomiędzy zapisami Umowy, a treścią załączników do niej, pierwszeństwo zachowują postanowienia Umowy.

§13

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy oraz dwa dla Zamawiającego.

---------- ----------

Wykonawca **Zamawiający**

Część II

UMOWA nr ……..……projekt

zawarta w dniu …… r. w Gdyni pomiędzy:

Akademią Marynarki Wojennej im. Bohaterów Westerplatte, ul. Śmidowicza 69, 81-127 Gdynia, **NIP: 586-010-46-93,**
reprezentowaną przez: *:*
Rektora-Komendanta AMW- kontradmirała prof. dr hab. Tomasza Szubrychta,
zwaną dalej **Zamawiającym,**

a

firmą:
……
wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej w dniu ……., pod numerem **NIP: …….., REGON ……** reprezentowaną przez **…… ,**
zwaną dalej **Wykonawcą**,

zwanymi dalej łącznie Stronami, a każdy indywidualnie Stroną,

o następującej treści:

§1

1. W wyniku wyboru oferty Wykonawcy, w postępowaniu o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego na podstawie art. 129 ust. 1 pkt 1 oraz art. 132 i nast. ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych,** o nr ……, w dniu …….., Wykonawca zrealizuje na rzecz Zamawiającego następujące świadczenia:
   a) dostawę CERTYFIKATU SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ
   b) dostawę SERWERA USŁUG PULPITU ZDALNEGO,
   zgodnie z ofertą złożoną w postępowaniu przetargowym.

§2

Wykonawca oświadcza, że:
1. Jest uprawniony oraz posiada niezbędne kwalifikacje do pełnej realizacji przedmiotu Umowy.
2. Realizowany przedmiot Umowy może być wykorzystywany bez naruszania praw własności osób trzecich, w tym praw patentowych i praw autorskich.
3. Realizowany przedmiot Umowy spełnia normy przewidziane prawem polskim.

§3

1. Certyfikat, serwer wraz z oprogramowaniem dostarczone zostaną do dnia 30.08.2021 r.
2. Odbiór przedmiotu Umowy tytułem dostarczenia certyfikatu oraz serwera z oprogramowaniem nastąpi na podstawie protokołu przekazania/odbioru podpisanego przez obie Strony.
3. Wykonawca ma obowiązek osobistego wykonania całości zamówienia.
4. W przypadku przekroczenia terminu określonego w ust. 1 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% ceny określonej w § 4 ust. 1 za każdy dzień opóźnienia, nie więcej jednak niż 20% ceny.
5. Za odstąpienie od Umowy z przyczyn niezależnych od Zamawiającego Wykonawca zapłaci karę umowną w wysokości 5% wartości niewykonanego zakresu Umowy.
6. Za każde opóźnienie w usunięciu wad przedmiotu zamówienia, ujawnionych w okresie gwarancji – Wykonawca zapłaci karę umowną w wysokości 0,5% wartości przedmiotu Umowy za każdy dzień opóźnienia liczonego od dnia wyznaczonego na ich usunięcie, nie więcej jednak niż 10% ceny.
7. Zamawiający zastrzega sobie prawo potrącenia równowartości naliczonych kar umownych z wynagrodzenia Wykonawcy wynikającego z wystawionej przez Wykonawcę faktury.
8. Jeżeli szkoda spowodowana niewykonaniem lub nienależytym wykonaniem Umowy przekroczy wartość zastrzeżonych kar umownych, bądź wynika z innych tytułów niż zastrzeżone, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego do pełnej wysokości szkody.
9. Łączna wysokość kar umownych, których może dochodzić każda ze stron wynosi 40% ceny określonej w § 4 ust. 1 niniejszej Umowy.

§4

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy kwotę brutto **……..zł**
   (słownie: …….. zł …… groszy).
2. Zapłata nastąpi zgodnie z ofertą, po wykonaniu przedmiotu umowy. Kwota płatna po podpisaniu przez Zamawiającego protokołu zdawczo/odbiorczego;

3. Ww. płatności realizowane będą przelewem w terminie 30 dni od doręczenia prawidłowo wystawionej faktury VAT, z konta Zamawiającego:

   SANTANDER BANK POLSKA SA
   95 1500 1881 1210 2003 3251 0000

   na konto **Wykonawcy** w:
   ……
   przy czym za dzień zapłaty Strony Umowy przyjmują datę obciążenia rachunku **Zamawiającego**.

§5

Uprawnienia z tytułu rękojmi nie są wyłączone.

§6

Wszystkie zmiany Umowy wymagają zgody obu Stron w formie pisemnej pod rygorem nieważności, z uwzględnieniem art. 455 Prawa zamówień publicznych.

§7

Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osoby trzecie bez uprzedniej pisemnej zgody **Zamawiającego**.

§8

1. Zakres świadczenia **Wykonawcy** wynikający z Umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
2. Umowa jest nieważna w części wykraczającej poza określenie przedmiotu zamówienia zawartego w specyfikacji istotnych warunków zamówienia.
3. Zakazuje się zmian postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub w specyfikacji istotnych warunków zamówienia oraz określił warunki takiej zmiany.
4. Zamawiający może odstąpić od umowy:
   1) w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu;
   2) jeżeli zachodzi co najmniej jedna z następujących okoliczności:
      a) dokonano zmiany umowy z naruszeniem art. 454 i art. 455,
      b) Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108,
      c) Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.
5. Z zastrzeżeniem przepisów odrębnych, Umowa podlega unieważnieniu w przypadkach określonych w art. 457 Prawa zamówień publicznych.
6. Strony zgodnie oświadczają, iż tryb przewidziany w ustawie z dnia 11.09.2019 Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) i aktach wykonawczych do tej ustawy został zachowany.
7. Zamawiający, zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t. j. Dz. U. z 2021 r. poz. 424), oświadcza iż posiada status dużego przedsiębiorcy.

§9

1. W czasie wykonywania niniejszej Umowy oraz w okresie gwarancji (rękojmi), **Wykonawca** jest zobowiązany do pisemnego powiadamiania Zamawiającego :
   - o zmianie siedziby Wykonawcy,
   - o upadłości Wykonawcy,
   - o wszczęciu postępowania układowego,
   - o ogłoszeniu likwidacji,
   - o zawieszeniu działalności,
   - o zmianie w zakresie rejestracji działalności Wykonawcy.
2. O wystąpieniu powyższych okoliczności, Wykonawca zobowiązany jest powiadomić Zamawiającego najpóźniej w terminie 3 dni od ich zaistnienia pod rygorem naliczenia kary umownej w wysokości 1 % ceny określonej w § 4 ust. 1. W przypadku zaistnienia okoliczności, o których mowa w ust. 1.

§10

1. Spory wynikłe na tle realizacji niniejszej Umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
2. W przypadku rozbieżności pomiędzy zapisami Umowy, a treścią załączników do niej, pierwszeństwo zachowują postanowienia Umowy.
3. W sprawach nie uregulowanych niniejszą Umową będą miały zastosowanie odpowiednie przepisy ustawy Prawo zamówień publicznych oraz kodeksu cywilnego.

§11

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy oraz dwa dla Zamawiającego.

---------- ----------

Wykonawca **Zamawiający**

ZAŁĄCZNIK NR 4

Wykonawca:

……
……
reprezentowany przez:
……
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE
O PRZYNALEŻNOŚCI / BRAKU PRZYNALEŻNOŚCI
DO GRUPY KAPITAŁOEJ*

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego** *(32/ZP/22)*, prowadzonego w trybie przetargu podstawowego z art. 275 ust.1, na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2021 r. poz. 1129 ze zm.), oświadczam/y, że:

- należę ** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2021 r. poz. 275 z późn.zm.), co następujący Wykonawca, który złożył odrębną ofertę, w postępowaniu:

……

……

lub

- nie należę ** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2021 r. poz. 275 z późn.zm.), co inny Wykonawca, który złożył odrębną ofertę, w postępowaniu.

Data, miejscowość oraz podpis(-y):

---

* niniejsze oświadczenie składa każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia

** niepotrzebne skreślić

ZAŁĄCZNIK NR 5

Wykonawca:

……
……
reprezentowany przez:
……
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE
DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Składając ofertę w postępowaniu nr spr.: **32/ZP/22** na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy PZP.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 1, 4, 5 i od 7 do 10 ustawy PZP.
3. Oświadczam, że nie jestem umieszczony na listach i nie podlegam wykluczeniu z niniejszego postępowania o udzielenie zamówienia, na podstawie obowiązujących przepisów określonych w art. 7 ust. 1 Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 r. poz. 835)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy PZP *(podać mającą zastosowanie podstawę wykluczenia spośród wskazanych powyżej).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy PZP podjąłem następujące środki naprawcze:

……..…….
.....……..…
…….....……
……..…….....……

ZAŁĄCZNIK NR 6

OŚWIADCZENIE WYKONAWCÓW
WSPÓLNIE UBIEGAJĄCYCH SIĘ O ZAMÓWIENIE

(o którym mowa w art. 117 ust. 4 ustawy)

Oświadczenia wykonawców wspólnie ubiegających się o udzielenie zamówienia

PODMIOTY W IMIENIU KTÓRYCH SKŁADANE JEST OŚWIADCZENIE: ……..…...……

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEIDG) ……

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEIDG) reprezentowane przez: ……..

……..
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jedn.: Dz. U. z 2021 r., poz. 1129 z późn. zm.) - dalej: ustawa Pzp Na potrzeby postępowania o udzielenie zamówienia publicznego którego przedmiotem jest **Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego** *(32/ZP/22),* prowadzonego w **trybie przetargu podstawowego** działając jako pełnomocnik podmiotów, w imieniu których składane jest oświadczenie oświadczam, że:

Wykonawca: ……..…...…...……

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

……

Wykonawca: ……..…...……

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

……
……

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą.

ZAŁĄCZNIK NR 7

Wykonawca:

……

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych wynikających z RODO

Wykonawca ubiegając się o udzielenie zamówienia publicznego jest zobowiązany do wypełnienia wszystkich obowiązków formalno-prawnych związanych z udziałem w postępowaniu. Do obowiązków tych należą m.in. obowiązki wynikające z RODO[4)], w szczególności obowiązek informacyjny przewidziany w **art. 13 RODO** względem osób fizycznych, których dane osobowe dotyczą i od których dane te wykonawca bezpośrednio pozyskał. Jednakże obowiązek informacyjny wynikający z art. 13 RODO nie będzie miał zastosowania, gdy i w zakresie, w jakim osoba fizyczna, której dane dotyczą, dysponuje już tymi informacjami (vide: art. 13 ust. 4).

Wykonawca musi wypełnić obowiązek informacyjny wynikający z **art. 14 RODO** względem osób fizycznych, których dane przekazuje zamawiającemu i których dane pośrednio pozyskał, chyba że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO.

W celu zapewnienia, że wykonawca wypełnił ww. obowiązki informacyjne oraz ochrony prawnie uzasadnionych interesów osoby trzeciej, której dane zostały przekazane w związku z udziałem wykonawcy w postępowaniu, wykonawca składa w postępowaniu o udzielenie zamówienia publicznego oświadczenie o wypełnieniu przez niego obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO.

Oświadczenie wykonawca składa razem z ofertą.

Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.*

* W przypadku, gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

[4)] rozporządzenie 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

ZAŁĄCZNIK NR 8

Wykonawca: …….....……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG) reprezentowany przez:

……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu podstawowego z art. 275 ust.1 **znak: 32/ZP/22**:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego

w zakresie art. 108 ust. 1 pkt 3-6 ustawy Pzp, dodatkowo art. 109 ust. 1 pkt 5 i 7-8 oświadczamy, że: wszystkie informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania **są** aktualne na dzień złożenia oświadczenia

ZAŁĄCZNIK NR 09
dotyczy części I

Wykonawca:

……..
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE
O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Składając ofertę w postępowaniu na:
Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22

oświadczamy, że spełniamy warunki udziału
w postępowaniu określone przez Zamawiającego w SWZ:

oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w Rozdziale 20 SWZ

1. posiadam doświadczenie opisane przez Zamawiającego w Rozdziale 20 SWZ, w tym:

1) warunek ten spełniam samodzielnie – Tak w pełnym zakresie*/Tak, częściowo w zakresie ……./ Nie*,

2) w celu spełnienia tego warunku polegam na zasadach określonych w art. 118 ustawy PZP, na następującym podmiocie*:

……..……

(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

w następującym zakresie:

……..

* niepotrzebne skreślić

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji

ZAŁĄCZNIK NR 10
dotyczy części I

Wykonawca:

……
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE

(dotyczy, gdy Wykonawca w celu potwierdzenia spełnienia warunków udziału w postępowaniu polega na zdolnościach innych podmiotów)

Oświadczam, iż podmiotem, na którego zasoby powołujemy się na zasadach określonych w art. 118 ustawy PZP, w celu wykazania spełnienia warunków udziału w postępowaniu, jest*:

……..……
(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

** niepotrzebne skreślić*

PISEMNE ZOBOWIĄZANIE PODMIOTU DO ODDANIA DO DYSPOZYCJI WYKONAWCY NIEZBĘDNYCH ZASOBÓW NA OKRES KORZYSTANIA Z NICH PRZY WYKONYWANIU ZAMÓWIENIA ZGODNIE Z ART. 118 USTAWY PZP

Nazwa ……

Adres ……

Ja (My) niżej podpisany (ni)

…….

działając w imieniu i na rzecz :
……
……

oświadczam(y), że w postępowaniu **32/ZP/22** na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego

zobowiązuję (zobowiązujemy) się udostępnić swoje zasoby Wykonawcy:

……
…….

(pełna nazwa Wykonawcy i adres/siedziba Wykonawcy)

W celu oceny, czy ww. Wykonawca będzie dysponował moimi zasobami w stopniu niezbędnym dla należytego wykonania zamówienia oraz oceny, czy stosunek nas łączący gwarantuje rzeczywisty dostęp do moich zasobów podaję:

1) zakres moich zasobów dostępnych Wykonawcy:
……
……
……

2) sposób wykorzystania moich zasobów przez Wykonawcę przy wykonywaniu zamówienia:
……
……
……

3) charakteru stosunku, jaki będzie mnie łączył z Wykonawcą:
……
……
……

4) zakres i okres mojego udziału przy wykonywaniu zamówienia:
……

UWAGA:
Pisemne zobowiązanie podmiotu udostępniającego musi być podpisane podpisem kwalifikowanym przez ten podmiot i złożone wraz z ofertą.

ZAŁĄCZNIK NR 11
dotyczy części I

Podmiot:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenia podmiotu udostępniającego zasoby

UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

składane na podstawie art. 125 ust. 5 ustawy Pzp

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)**, oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:

1. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 108 ust 1 ustawy Pzp.
2. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 109 ust. 1 ustawy Pzp.
3. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego *(Dz. U. poz. 835)*[5].

[5] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, *zwanej* dalej „ustawą", z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w ……..……..……..

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu) w następującym zakresie: ……

……..……..…….....

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

1) .....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

2) .....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

……

kwalifikowany podpis elektroniczny
lub podpis zaufany lub podpis osobisty

ZAŁĄCZNIK NR 12
dotyczy części I

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenia

wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia

UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

składane na podstawie art. 125 ust. 1 ustawy Pzp

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)**, oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
   Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 ustawy Pzp.
2. [UWAGA: zastosować, gdy zachodzą przesłanki wykluczenia z art. 108 ust. 1 pkt 1, 2 i 5 lub art.109 ust.1 pkt 2-5 i 7-10 ustawy Pzp, a wykonawca korzysta z procedury samooczyszczenia, o której mowa w art. 110 ust. 2 ustawy Pzp] Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2-5 i 7-10 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze i zapobiegawcze:
   ……
   ……
3. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U. poz. 835)[6].

[6] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą”,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

[UWAGA: *stosuje tylko wykonawca/ wykonawca wspólnie ubiegający się o zamówienie*]

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w ……..……..……..

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu).

[UWAGA: *stosuje tylko wykonawca/ wykonawca wspólnie ubiegający się o zamówienie, który polega na zdolnościach lub sytuacji podmiotów udostepniających zasoby, a jednocześnie samodzielnie w pewnym zakresie wykazuje spełnianie warunków*]

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w ……..……..……..

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu) w następującym zakresie: ……..……..……..

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTÓW UDOSTEPNIAJĄCYCH ZASOBY:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w……..……..…….. *(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu),* polegam na zdolnościach lub sytuacji następującego/ych podmiotu/ów udostępniających zasoby: *(wskazać nazwę/y podmiotu/ów)*……

……..……..……..……

w następującym zakresie:…… ……..

(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu).

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

1) .....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

2) .....

(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

……

kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty

ZAŁĄCZNIK NR 13
dla części I

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Wykaz wykonanych usług i dostaw

– odnowienie subskrypcji na system ochrony antywirusowej i antyspamowej zasobów sieci komputerowej;
– wsparcie techniczne systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego;

Lp.	Odbiorca (dokładna nazwa i adres)	Data wykonania (czas trwania umowy od - do)	Przedmiot wykonywanej dostawy/usługi	Wartość

UWAGA !!!
W załączeniu dokumenty potwierdzające należyte wykonanie dostaw wyszczególnionych w wykazie.

ZAŁĄCZNIK NR 14
dla części I

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WYKAZ OSÓB SKIEROWANYCH DO REALIZACJI ZAMÓWIENIA ZGODNY Z WARUNKIEM SWZ

– odnowienie subskrypcji na system ochrony antywirusowej i antyspamowej zasobów sieci komputerowej;
– wsparcie techniczne systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego;

Lp.	Imię i Nazwisko	Posiadane kwalifikacje	Wykształcenie	Wykonywane czynności	Doświadczenie	Podstawa do dysponowania

ZAŁĄCZNIK NR 15
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na usługę i dostarczenie:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….…….....

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …….

…….

…….……

z siedzibą

w ……..……..

Oświadczam, że:

Pani/Pan …… posiada certyfikat potwierdzający umiejętność instalowania i konfigurowania oferowanego oprogramowania. Certyfikat musi być wystawiony przez producenta lub autoryzowanego dystrybutora oferowanego oprogramowania lub autoryzowany przez niego ośrodek szkoleniowy.

ZAŁĄCZNIK NR 16
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na usługę i dostarczenie:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….…….....

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …….

…….

……..…….

z siedzibą

w ……..……..

Oświadczam, że:

Pani/Pan …… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Windows Serwer 2008 lub nowszego.

ZAŁĄCZNIK NR 17
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na usługę i dostarczenie:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….…….....

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …….

…….

……..…….

z siedzibą

w ……..……..

Oświadczam, że:

Pani/Pan …… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Microsoft Exchange 2010 lub nowszego.

ZAŁĄCZNIK NR 18
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

……..…….....

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …….

…….

……..……

z siedzibą

w ……..……..

Oświadczam, że:

Pani/Pan …… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność wdrażania i administrowania środowiskiem wirtualnym opartym o Microsoft Hyper-V

ZAŁĄCZNIK NR 19
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….…….....

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …….

…….

…….……

z siedzibą

w ……..……..

Oświadczam, że:

Pani/Pan …… posiada certyfikat potwierdzający umiejętność świadczenia usług serwisowych zgodnie z ITIL (np. ITIL Foundation)

ZAŁĄCZNIK NR 20
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….....
(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): ……..……..…….……
……..……
……..……..……
z siedzibą w
……..……

Oświadczam, że:

Dysponujemy punktem serwisowym umożliwiającym dotarcie do siedziby Zamawiającego w ciągu 1 godziny od zgłoszenia serwisowego.

ZAŁĄCZNIK NR 21
dla części I

Wykonawca:

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

……., dn. ……

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 32/ZP/21 na:

Dostawa licencji na system ochrony antywirusowej wraz z wsparciem technicznym systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego (32/ZP/22)

Część I:

- ODNOWIENIE SUBSKRYPCJI NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTY-SPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
- WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMO-WEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

Ja, niżej podpisany

…….…….....
(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): ……

…….……

……...……

z siedzibą w

……..……...……

Oświadczam, że:

Dysponujemy portalem/systemem serwisowym w którym Zamawiający będzie mógł dokonywać zgłoszeń serwisowych i widzieć szczegóły ich realizacji.