ZATWIERDZAM

Ilona Hibner

Dyrektor Działu Systemów Informatycznych

/podpisano elektronicznie/

Warszawa, dnia 12 kwietnia 2021 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

(SWZ)

Przedmiotem zamówienia jest dostawa licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT

Nr postępowania 8/21/TPBN

TRYB UDZIELENIA ZAMÓWIENIA:

tryb podstawowy bez negocjacji

Zamawiający oczekuje, że Wykonawcy zapoznają się dokładnie z treścią niniejszej SWZ. Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów, oraz przedłożenia oferty nie odpowiadającej wymaganiom określonym przez Zamawiającego.

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO ORAZ WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI:

1. Zamawiający: NARODOWE CENTRUM BADAŃ I ROZWOJU W WARSZAWIE ul. Nowogrodzka 47a, 00-695 Warszawa.

   Numer tel.: 22 390 73 58

   Adres poczty elektronicznej: przetargi@ncbr.gov.pl.

   Adres strony internetowej prowadzonego postępowania: https://www.gov.pl/web/ncbr/postepowania-rozpoczete.

   Składanie ofert poprzez stronę: https://miniportal.uzp.gov.pl/

2. Wskazanie osób uprawnionych do komunikowania się z wykonawcami:

   Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:

   Imię Nazwisko: Paulina Lewandowska

   e-mail: przetargi@ncbr.gov.pl

II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: https://www.gov.pl/web/ncbr/postepowania-rozpoczete.

III. TRYB UDZIELENIA ZAMÓWIENIA

1. Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie **art. 275 pkt 1** ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm.) [zwanej dalej także „ ustawą PZP" lub „uPzp].
2. W zakresie nieuregulowanym niniejszą Specyfikacją Warunków Zamówienia, zwaną dalej „SWZ”, zastosowanie mają przepisy ustawy PZP.

IV. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

V. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest :
   1) **Dostawa licencji McAfee Complete EndPoint Protection – Business** (CEBCDE-AA-FG) – w ilości 900 (dziewięciuset) szt. ważnych od dnia 26 maja 2021 r. przez czas nieoznaczony;
   2) **Odnowienie subskrypcji McAfee Virtual Advanced Threat Defence Appliance** (AT1ECE-AB-AG) – w ilości 1 (jednej) szt. ważnej od dnia 26 maja 2021 r. przez okres 12 (dwunastu) miesięcy;
   3) **Odnowienie usługi wsparcia McAfee Threat Intelligence Exchange** (TIEYFM-AA-FG) – w ilości 800 (ośmiuset) szt. ważnych od dnia 26 maja 2021 r. przez okres 12 (dwunastu) miesięcy;

   lub oprogramowania równoważnego oraz zapewnienie usługi wsparcia technicznego producenta dla licencji i subskrypcji wskazanych powyżej w pkt 1) i 2) przez okres 12 (dwunastu) miesięcy liczonych od dnia udzielenia licencji/uruchomienia subskrypcji.
2. Szczegółowy opis przedmiotu zamówienia (SOPZ) znajduje się w Załączniku nr 1 do niniejszej Specyfikacji Warunków Zamówienia (SOPZ) i stanowi jej integralną część.
3. Zamawiający nie przewiduje prawa opcji.
4. Zamawiający nie dopuszcza składania ofert częściowych.
5. Zamawiający nie dopuszcza możliwości składania ofert wariantowych oraz w postaci katalogów elektronicznych.
6. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8.
7. Zamawiający nie wymaga, aby osoby wykonujące czynności w zakresie realizacji zamówienia zostały zatrudnione na podstawie umów o pracę.
8. Zamówienie jest niepodzielne ze względu na specyficzny charakter zamówienia, który ze względów technicznych nie mógłby zostać wykonany przez więcej niż jednego wykonawcę. Niedzielenie zamówienia na części nie wyklucza udziału w tym postępowaniu wykonawców z MŚP.
9. Nazwy i kody zamówienia według Wspólnego Słownika Zamówień (CPV):
   48731000-1 - Pakiety oprogramowania zabezpieczającego pliki;

   48000000-8 - Pakiety oprogramowania i systemy informatyczne;

   48700000-5 - Pakiety oprogramowania użytkowego;

   48730000-4 - Pakiety oprogramowania zabezpieczającego;

   48732000-8 - Pakiety oprogramowania do zabezpieczania danych;

   48760000-3 - Pakiety oprogramowania do ochrony antywirusowej.

VI. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest wykonać zamówienie w terminie do 7 dni kalendarzowych od dnia podpisania umowy, a w przypadku zaoferowania równoważnego oprogramowania nie później niż do dnia 26.05.2021 r.

VII. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają określone przez Zamawiającego w niniejszym rozdziale warunki udziału w postępowaniu dotyczące:

   1.1. zdolności technicznej lub zawodowej.

2. W zakresie warunku określonego w art. 112 ust. 2 pkt 4) ustawy PZP (zdolności technicznej lub zawodowej), Wykonawcy winni wykazać że:

   2.1 w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie, co najmniej dwie dostawy licencji na oprogramowanie ochrony infrastruktury IT o wartości każdej z nich co najmniej 50 000,00 zł (słownie: pięćdziesiąt tysięcy złotych) brutto.

Uwaga:

- Pod pojęciem dostawy Zamawiający rozumie jedną umowę zawartą z jednym podmiotem;
- Pod pojęciem dostawy wykonywanej należy rozumieć dostawy będącą w trakcie realizacji (dostawę aktualnie wykonywaną), przy czym jeśli Wykonawca powoła się na dostawę realizowaną, musi wykazać, że jej już zrealizowana część spełnia ww. wymagania;
- Wykonawca może wykazać się dostawą o szerszym zakresie niż wskazany w warunku i przedmiocie zamówienia, jednak dostawa ta musi spełniać wymagania minimalne określone w niniejszym SWZ. W wykazie dostaw należy wskazać zarówno wartość całej dostawy, jak również podać wartość dostawy dotyczącej określonej w niniejszym warunku;
- Zamawiający nie dopuszcza możliwości sumowania dostaw z różnych kontraktów w celu uzyskania ww. wartości minimalnej.

Na potwierdzenie spełnienia ww. warunku Wykonawcy przedłożą oświadczenie wymienione w pkt. 12 SWZ oraz - na wezwanie, oświadczenie i dokumenty, o których mowa w rozdziale XII pkt. 20 SWZ. W przypadku, gdy Wykonawcy będą polegać na zdolnościach technicznych lub zawodowych innego podmiotu, o którym mowa w art. 118 ust. 1 ustawy PZP, Wykonawca wraz z ofertą składa także oświadczenie tego podmiotu, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu lub kryteriów selekcji, w zakresie, w jakim wykonawca powołuje się na jego zasoby.

3. W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o wykonanie zamówienia wystarczy, że ww. warunek spełni jeden z nich lub Wykonawcy spełnią go łącznie.
4. Ocena spełnienia ww. warunku odbywać się będzie metodą spełnia/nie spełnia.
5. Z treści załączonych dokumentów i oświadczeń musi wynikać jednoznacznie, iż Wykonawca spełnia wyżej wymieniony warunek.
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. Niespełnienie warunku skutkować będzie odrzuceniem oferty Wykonawcy z postępowania.
8. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
9. W takim przypadku:
   9.1. 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.
   9.2. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 9.1. potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
      1) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
      2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
      3) 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 dostawy, których wskazane zdolności dotyczą.
10. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt. 4.

11. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają dostawy, do realizacji których te zdolności są wymagane.
12. W celu potwierdzenia spełniania warunków udziału w postępowaniu oraz wykazania braku podstaw wykluczenia, określonych w rozdziale XV, Wykonawcy ubiegający się o udzielenie zamówienia muszą wraz z ofertą złożyć następujące dokumenty:
    12.1. aktualne na dzień składania ofert oświadczenie o niepodleganiu wykluczeniu z postępowania w zakresie wskazanym odpowiednio w Załączniku nr 3 do SWZ. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu.
    12.2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym mowa w pkt 11.1. SWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to potwierdza brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców brak podstaw wykluczenia.

VIII PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy, określony został w Załączniku nr 4 do SWZ.

IX. INFORMACJE 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. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną przy użyciu miniPortalu https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal.
2. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do *formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.*
3. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej przekazywanej przy ich użyciu, opisane zostały w Regulaminie korzystania z miniPortalu dostępnym pod adresem https://miniportal.uzp.gov.pl/WarunkiUslugi.aspx oraz Regulaminie ePUAP.

4. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z miniPortalu, określone w Regulaminie miniPortalu oraz zobowiązuje się korzystając z miniPortalu przestrzegać postanowień tego regulaminu.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia i wycofania oferty oraz do komunikacji wynosi 150 MB.
6. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 ustawy pzp, podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na ePUAP.
7. W postępowaniu o udzielenie zamówienia korespondencja elektroniczna (inna niż oferta Wykonawcy i załączniki do oferty) odbywa się elektronicznie za pośrednictwem *dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji)*. Korespondencja przesłana za pomocą tego formularza nie może być szyfrowana. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP).
8. Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, email: przetargi@ncbr.gov.pl.
9. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem *Formularza do komunikacji,* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na adres email przetargi@ncbr.gov.pl. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 31 grudnia 2020 roku „*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*".
10. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
11. Zamawiający nie ponosi odpowiedzialności z tytułu nieotrzymania przez Wykonawcę informacji związanych z prowadzonym postępowaniem w przypadku wskazania przez Wykonawcę w ofercie np. adresu poczty elektronicznej.
12. Wykonawca może w drogą elektroniczną/za pomocą środków komunikacji elektronicznej zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający niezwłocznie udzieli wyjaśnień jednak nie później niż **2 dni** przed terminem składania ofert – pod warunkiem, że

wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego nie później niż na 4 dni przed upływem wyznaczonego terminu składania ofert i nie dotyczy udzielonych wyjaśnień.

13. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania ww. wniosków. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął po upływie terminu, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
14. Wnioski o wyjaśnienia SWZ należy przesyłać za pomocą poczty elektronicznej na adres: przetargi@ncbr.gov.pl. W temacie pisma należy podać: „***Dostawa licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN".***
15. Treść zapytań wraz z wyjaśnieniami Zamawiający przekaże Wykonawcy oraz zamieści na stronie internetowej prowadzonego postępowania bez ujawniania źródła zapytania.
16. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert zmodyfikować treść niniejszej SWZ.
17. Każda wprowadzona przez Zamawiającego zmiana SWZ stanie się częścią SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej Zamawiającego.
18. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku modyfikacji treści SWZ niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach.

X. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert przez 30 (trzydzieści) dni kalendarzowych tj. do dnia 19.05.2021 r.
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w SWZ, Zamawiający przed upływem terminu związania oferta zwróci 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 oferta, o którym mowa w pkt 1 wymaga złożenia przez Wykonawcę pisemnego[1] oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

[1] *t.j. wyrażonego przy użyciu wyrazów, cyfr lub innych znaków pisarskich, które można odczytać i powielić*

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. **Oferta musi być** sporządzona w języku polskim, w postaci elektronicznej w formacie danych: .pdf, .doc, .docx, .rtf,.xps, .odt i **opatrzona kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.**
2. Sposób zaszyfrowania oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
3. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego lub podpisu zaufanego lub podpisu osobistego.
4. Jeżeli na ofertę składa się kilka dokumentów, Wykonawca powinien stworzyć folder, do którego przeniesie wszystkie dokumenty oferty, podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Następnie z tego folderu Wykonawca skompresuje do jednego folderu .zip.
5. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj.: Dz. U. z 2020 r. poz. 1013), które Wykonawca zastrzeże, jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego, jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 pzp.

   Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Zaleca się, aby uzasadnienie, o którym mowa powyżej było sformułowane w sposób umożliwiający jego udostępnienie inny uczestnikom postępowania.

   Uwaga:

Zastrzegając informacje w ofercie Wykonawca winien mieć na względzie, że zastrzeżona informacja ma charakter tajemnicy przedsiębiorstwa, jeśli spełnia poniższe warunki, określone w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji tj.:

ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą, ***oraz***

jako całość lub w szczególnym zestawieniu i zbiorze elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji, ***albo*** *nie są łatwo dostępne dla takich osób,*

o ile uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

W nawiązaniu do orzecznictwa arbitrażowego i sądowego, należy przyjąć, iż sferą tajemnicy można objąć tylko takie informacje, które są znane jedynie poszczególnym osobom lub określonej grupie osób. Obszar ten nie może się rozciągać na informacje powszechnie znane lub te, o których treści każdy zainteresowany może się legalnie dowiedzieć.

6. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnym pliku oznaczonym, jako tajemnica przedsiębiorstwa. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
7. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 224 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich, jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
8. Wykonawca w szczególności nie może zastrzec w ofercie informacji:
   8.1 Przekazywanych po otwarciu ofert, o których mowa w art. 222 ust. 5 ustawy PZP,
   8.2 które są jawne na mocy odrębnych przepisów,
   8.3 cen jednostkowych stanowiących podstawę wyliczenia ceny oferty.
9. Wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania powyższych wymagań będą obciążały Wykonawcę.
10. Do oferty należy dołączyć wstępne oświadczenie o spełnieniu warunków udziału i niepodleganiu wykluczeniu w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub

podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

11. Do przygotowania oferty zaleca się wykorzystanie Formularza Oferty, którego wzór stanowi Załącznik nr 2 do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu Ofertowym.
12. Miniportal oraz ePuap nie weryfikuje poprawności podpisu z profilu zaufanego oraz podpisu osobistego, jak również nie weryfikuje poprawności dokumentów, poprawności rozumianej zgodnej w ustawą PZP i kompletności zgodnego z SWZ.
13. **Do oferty należy dołączyć:**
    - 13.1 **Pełnomocnictwo upoważniające do złożenia oferty** - o ile ofertę składa pełnomocnik (podpisane zgodnie z informacją zawartą w pkt 16).
    - 13.2 **Formularz ofertowy –** do wykorzystania wzór, stanowiący Załącznik nr 2 do SWZ (podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym).
    - 13.3 **Wstępne oświadczenie Wykonawcy o spełnieniu warunków udziału i niepodleganiu wykluczeniu z postępowania** wzór wstępnego oświadczenia o spełnieniu warunków udziału i niepodleganiu wykluczeniu stanowi Załącznik nr 3 do SWZ. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepoleganiu wykluczeniu składa każdy z Wykonawców (podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym).
    - 13.4 **Zobowiązanie podmiotu trzeciego –** jeżeli dotyczy (podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym).
    - 13.5 **Oświadczenie, o którym mowa w art. 117 ust. 4 –** w przypadku wykonawców wspólnie ubiegających się o zamówienie – do wykorzystania wzór, stanowiący Załącznik nr 10 (podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym).
14. Ofertę, oświadczenia zaleca się sporządzić na drukach stanowiących załączniki do SWZ.
15. Oferta, wstępne oświadczenie o spełnieniu warunków udziału i niepodleganiu wykluczeniu oraz oświadczenie, o którym mowa w art. 117 ust. 4 muszą być złożone w oryginale.
16. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (tj. w formie elektronicznej lub postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub 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, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym. Zamawiający dopuszcza również skan pełnomocnictwa sporządzonego uprzednio w formie opatrzony pisemnej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

17. **Wykonawcy ubiegający się wspólnie o udzielenie zamówienia** (np. spółki cywilne, konsorcja), zgodnie z art. 58 ust. 2 ustawy PZP, **zobowiązani są ustanowić pełnomocnika.** Z treści pełnomocnictwa winno jednoznacznie wynikać prawo pełnomocnika do reprezentowania Wykonawcy w postępowaniu o udzielenie zamówienia publicznego albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego w imieniu Wykonawcy. Dokument ten winien być podpisany przez osobę/osoby uprawnioną(-e) do jego udzielenia tj. zgodnie z formą reprezentacji każdego z Wykonawców (podpisany kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym). W przypadku wspólników spółki cywilnej dopuszczalne jest przedłożenie umowy spółki cywilnej, z której wynika zakres i sposób reprezentacji, a w przypadku konsorcjum przedłożenie umowy konsorcjum.
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 pkt 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. Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych, o których mowa w art. 273 ust. 1 ustawy PZP:

    20.1 **Wykaz dostaw** wykonanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem przedmiotu dostawy, dat wykonania, nazwy podmiotu na rzecz, którego była realizowana dostawa oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych

dokumentów - oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, że zostały wykonane należycie. Do ewentualnego wykorzystania przy sporządzaniu tego dokumentu służy Załącznik nr 8 do SWZ.

21. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
22. Wykonawca składa podmiotowe środki dowodowe aktualne na dzień ich złożenia.
23. W przypadku, kiedy Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcy, Zamawiający żąda wskazania przez wykonawcę w Formularzu oferty, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez wykonawcę firm podwykonawców o ile są znane.

XIII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia lub wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia 20.04.2021 r., do godz. 10:00.
3. Wykonawca może złożyć tylko jedną ofertę.
4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
5. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
6. Wykonawca po przesłaniu oferty za pomocą Formularza do złożenia lub wycofania oferty na „ekranie sukcesu" otrzyma numer oferty generowany przez ePUAP. Ten numer należy zapisać i zachować. Będzie on potrzebny w razie ewentualnego wycofania oferty.
7. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem Formularza do wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
8. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

XIV. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu 20.04.2021 r. o godzinie 12:00.

2. Otwarcie ofert jest niejawne.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informacją o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
   4.1. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   4.2. cenach lub kosztach zawartych w ofertach.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
7. W toku dokonywania badania i oceny złożonych ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących ich treści.
8. Oferty, które nie zostaną odrzucone, zostaną poddane procedurze oceny zgodnie z kryterium oceny ofert określonym w rozdziale XVIII niniejszej SWZ.
9. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie PZP oraz w SWZ, a ponadto uzyska największą liczbę punktów zgodnie z przyjętym kryterium oceny ofert.

XV. PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia wyklucza się z zastrzeżeniem art. 110 ust. 2 ustawy PZP, Wykonawcę w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych;
   1.1. w art. 108 ust.1 ustawy PZP;
   1.2. w art. 109 ust. 1 pkt. 4, 5, 7 ustawy PZP, tj.:
      a) 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;
      b) 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;

c) 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;

1.3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy PZP.

XVI. SPOSÓB OBLICZENIA CENY

1. Wykonawca poda cenę oferty w Formularzu ofertowym sporządzonym według wzoru stanowiącego Załącznik nr 2 do SWZ, tj. cenę netto, cenę brutto (z uwzględnieniem kwoty podatku od towarów i usług (VAT) z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
3. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty.
4. Wykonawca poda w Formularzu ofertowym także ceny jednostkowe poszczególnych elementów zamówienia zgodnie z zamieszczoną w nim tabelą.
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

XVII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Za najkorzystniejszą zostanie uznana oferta z największą ilością punktów.
2. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty dwie lub więcej ofert przedstawiających taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający zastosuje procedurę opisaną w art. 248 ustawy PZP.

3. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
4. 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.
5. W przypadku braku zgody, o której mowa w ust. 4, oferta podlega odrzuceniu, a Zamawiający zwróci się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba ze zachodzą przesłanki do unieważnienia postępowania.
6. Zamawiający dokona oceny ofert, które nie będą podlegały odrzuceniu.
7. Przy ocenie ofert zostaną uwzględnione następujące kryteria:

Lp.	Nazwa kryterium	Waga
1	Cena	100%

Zamawiający oceni oferty przyznając punkty w ramach kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt. Zamawiający dokona wyliczenia punktów dla danej oferty do dwóch miejsc po przecinku i wybierze ofertę z najwyższą liczbą punktów ogółem, spośród ofert nie podlegających odrzuceniu.

7.1. <u>Punkty za kryterium: cena oferty brutto „C" – waga 100%</u>

Maksymalną liczbę punktów w tym kryterium (100 pkt) otrzyma oferta Wykonawcy, który zaproponuje najniższą cenę oferty brutto podaną przez Wykonawcę w Formularzu oferty (Załącznik nr 2 do SWZ), natomiast pozostali Wykonawcy otrzymają odpowiednio mniejszą liczbę punktów obliczoną zgodnie z poniższym wzorem:

$$\textbf{CO}\ (\text{liczba przyznanych punktów}) = \frac{\text{cena brutto oferty najtańszej}}{\text{cena brutto oferty badanej}} \times 100$$

Punkty w kryterium „**Cena oferty brutto**" zostaną zaokrąglone do dwóch miejsc po przecinku.

8. Wykonawca za kryterium „**Cena oferty brutto**" może uzyskać maksymalnie 100 pkt.
9. Zamawiający odrzuci ofertę w sytuacjach, o których mowa w art. 226 ust. 1 ustawy Pzp.

XVIII. POPRAWIENIE OMYŁEK W OFERCIE

1. Zamawiający poprawi w ofercie, w szczególności:
   1.1. oczywiste omyłki pisarskie;

1.2. oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek;

1.3. inne omyłki - polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty.

O poprawieniu omyłek w ofercie Zamawiający niezwłocznie zawiadomi Wykonawcę, którego oferta została poprawiona.

2. W przypadku, o którym mowa w ust. 1 pkt 3 powyżej, Zamawiający wyznaczy Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.

XIX. 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 PZP 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 umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana, jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o 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 nr 4 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 postępowanie.

XX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia 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, podjęta w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie wnosi sią 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 PZP, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargą wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" ustawy PZP.

XXI. ZAŁĄCZNIKI DO SWZ

Integralną częścią niniejszej SWZ stanowią następujące załączniki:

Załącznik nr 1- Szczegółowy opis przedmiotu zamówienia;

Załącznik nr 2- Formularz ofertowy;

Załącznik nr 3- Wstępne oświadczenie o spełnieniu warunków udziału w postępowaniu i niepodleganiu wykluczeniu;

Załącznik nr 4- Projektowane postanowienia umowy;

Załącznik nr 5- Regulamin korzystania z miniPortalu.

Załącznik nr 6- Arkusz weryfikacji podmiotu przetwarzającego dane osobowe;

Załącznik nr 7- Klauzula informacyjna dotycząca przetwarzania danych osobowych;

Załącznik nr 8- Wykaz dostaw;

Załącznik nr 9 – Oświadczenie, o którym mowa w art. 117 ust. 4.

Załącznik nr 1 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) **Dostawa licencji McAfee Complete EndPoint Protection – Business** (CEBCDE-AA-FG) – w ilości 900 (dziewięciuset) szt. ważnych od dnia 26 maja 2021 r. przez czas nieoznaczony;
2) **Odnowienie subskrypcji McAfee Virtual Advanced Threat Defence Appliance** (AT1ECE-AB-AG) – w ilości 1 (jednej) szt. ważnej od dnia 26 maja 2021 r. przez okres 12 (dwunastu) miesięcy;
3) **Odnowienie usługi wsparcia McAfee Threat Intelligence Exchange** (TIEYFM-AA-FG) – w ilości 800 (ośmiuset) szt. ważnych od dnia 26 maja 2021 r. przez okres 12 (dwunastu) miesięcy;

lub oprogramowania równoważnego oraz zapewnienie usługi wsparcia technicznego producenta oprogramowania dla licencji i subskrypcji wskazanych powyżej w pkt 1) i 2) przez okres 12 (dwunastu) miesięcy liczonych od dnia udzielenia licencji/uruchomienia subskrypcji.

II. Szczegółowy opis przedmiotu zamówienia

1. Zamawiający posłużył się nazwą własną producenta dla ułatwienia opisu przedmiotu zamówienia, w oparciu o przesłanki art. 99 ust. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm.).
2. Zaoferowane artykuły równoważne muszą być o parametrach wymaganych przez Zamawiającego lub lepszych, oraz spełniać następujące kryteria:

Lp.	Konfiguracja minimalna
1.	System musi wspierać, co najmniej następującą platformę wirtualizacyjną (jeżeli zostanie dostarczony w postaci maszyn wirtualnych): VMware.
2.	Oprogramowanie powinno wspierać następujące klienckie systemy operacyjne: a. Windows 7 (wersja x32 i x64) b. Windows 8 i 8.1 (wersja x32 i x64) c. Windows 10 (wersja x32 i x64) d. Mac OS X 10.9.x, 10.10.x oraz 10.11.x Oprogramowanie powinno wspierać następujące serwerowe systemy operacyjne: a. Windows Server 2008/2008 R2 b. Windows Server 2012/2012 R2 c. Windows Server 2016/2016 R2 W przypadku systemów Mac OS – Zamawiający dopuszcza pewne różnice we wspieranych funkcjonalnościach w stosunku do systemów Windows.
3.	Zaproponowane rozwiązanie musi zapewniać ochronę w zakresie: a) Kompleksowej ochrony stacji końcowych i serwerów przed złośliwym

	kodem/oprogramowaniem, uruchamianiem aplikacji, ochroną przed podatnościami usług, wyciekiem danych, podłączaniem nieznanych urządzeń. b) Zapewnieniem poufności danych poprzez możliwość szyfrowania systemów plików (filesystems), całych dysków, jak i pojedynczych plików znajdujących się na dyskach twardych (m.in.: HDD, SSD - lista niewyczerpująca) oraz nośnikach zewnętrznych (m.in. pendrive, inne dyski podłączane poprzez port USB, karty pamięci - lista niewyczerpująca). c) Ochrony na poziomie sieciowym, analiza ruchu webowego i wiadomości pocztowych w kontekście ochrony przed wyciekiem danych, złośliwego kodu, spamu i reputacji.
4.	Rozwiązanie musi pozwalać na swobodne przekazanie zdarzeń do zewnętrznych repozytoriów logów przy pomocy formatu syslog CEF/LEEF.
5.	Oprogramowanie musi umożliwiać uruchomienie serwera do obsługi stacji roboczych znajdujących się poza siecią lokalną Zamawiającego. Serwer taki musi być przystosowany do pracy w DMZ.
6.	Zaproponowany System Ochrony w przypadku, gdy składa się z komponentów różnych producentów, musi stanowić jedną całość, gdzie poszczególne komponenty nie utrudniają sobie wzajemnie pracy, nie wypaczają działania mechanizmów innych modułów a użycie komponentów różnych producentów nie obniża poziomu bezpieczeństwa infrastruktury Zamawiającego.
7.	Wszystkie moduły Systemu Ochrony muszą komunikować się między sobą w bezpieczny sposób (transmisja pomiędzy maszynami musi być szyfrowana).

1.1. Moduł szyfrowania dysków

Lp.	Konfiguracja minimalna
1.	System szyfrowania musi zapewniać centralne zarządzanie poprzez Centralną Konsolę Zarządzania (dalej CKZ) co najmniej w zakresie szyfrowania danych, w oparciu o centralną bazę danych, gdzie przetrzymywane są informacje o użytkownikach, kluczach i politykach szyfrowania niezbędne do uzyskania dostępu do danych zaszyfrowanych na stacji w sytuacji awaryjnej.
2.	Rozwiązanie musi zapewnić szyfrowanie danych na poziomie dysku w sposób transparentny dla systemu operacyjnego i użytkowników, z możliwością uruchomienia funkcjonalności uwierzytelniania użytkownika bezpośrednio po uruchomieniu komputera (przed wystartowaniem właściwego systemu operacyjnego - tzw. pre-boot authentication, zwany dalej PBA).
3.	Oprogramowanie szyfrujące na stacjach końcowych musi komunikować się z CKZ w bezpieczny sposób (transmisja szyfrowana).
4.	Rozwiązanie musi obsługiwać, co najmniej algorytm AES 256, jako algorytm szyfrowania danych.
5.	Uwierzytelnianie użytkownika w PBA ma być możliwe z wykorzystaniem hasła i nazwy użytkownika.
6.	System musi pobierać użytkowników z domeny opartej o Active Directory (AD) oraz dać możliwość ręcznej definicji użytkowników niezależnie od AD. System musi umożliwiać wskazanie, który użytkownik i grupa mają prawo używać komputer i uzyskać dostęp do zaszyfrowanych danych: a) użytkownicy i grupy użytkowników przypisywani do komputerów muszą być synchronizowani z domeny Microsoft Active Directory, b) usunięcie użytkownika w serwerze usług katalogowych AD powinno skutkować automatycznym usunięciem lub zablokowaniem użytkownika w serwerze zarządzającym systemem szyfrowania.
7.	Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych komputerach, do których jest przypisany ten

	użytkownik.
8.	Zmiana hasła z poziomu systemu Windows musi być automatycznie replikowana do systemu szyfrującego tak, by nie było potrzeby dwukrotnej zmiany hasła.
9.	Rozwiązanie musi umożliwiać pracę w trybie single sign-on (SSO) – po zalogowaniu się w trybie PBA użytkownik nie musi już logować się po raz kolejny do systemu Windows, jego dane są automatycznie przekazywane przez moduł PBA do procesu logowania Windows.
10.	System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowania danych i umożliwić odzyskanie zaszyfrowanych danych z ich wykorzystaniem w sytuacji awaryjnej.
11.	Każdy komputer musi posiadać swój unikalny klucz wykorzystywany do szyfrowania danych na dysku oraz powinien być obecny w bazie CKZ.
12.	Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.
13.	System musi zapewniać możliwość centralnej konfiguracji parametrów szyfrowania, w tym centralne ustalanie polityk dla użytkowników i komputerów.
14.	Stacje i użytkownicy muszą synchronizować zmiany w politykach szyfrowania oraz parametrach systemu bez konieczności interwencji administratora.
15.	System przed rozpoczęciem szyfrowania musi sprawdzić, czy na komputerze nie znajduje się oprogramowanie niekompatybilne.
16.	System musi umożliwiać generowanie raportów dotyczących, co najmniej: stanu zaszyfrowania systemu (stacja nie zaszyfrowana, stacja zaszyfrowana, stacja w trakcie szyfrowania), wersji działającego oprogramowania szyfrowania, przypisanych do stacji użytkowników.
17.	System na stacjach końcowych musi umożliwiać zmianę hasła użytkownika w przypadku jego zapomnienia. Proces zmiany hasła musi spełniać, co najmniej jeden z poniższych warunków: a. musi istnieć tryb zmiany hasła nie wymagający podłączenia stacji do sieci firmowej, b. musi istnieć możliwość samodzielnego zresetowania hasła przez użytkownika w trybie PBA w oparciu o podanie odpowiedzi na wcześniej zdefiniowane pytania, podanie tokenu lub z wykorzystaniem podobnych technik.
18.	System musi oferować możliwość wykorzystania wbudowanego w system operacyjny mechanizmu szyfrowania oprócz oferowania własnego mechanizmu szyfrującego. System musi obsługiwać, co najmniej poniższe mechanizmy szyfrowania: a) Bitlocker w przypadku systemów Microsoft Windows, b) FileVault w przypadku systemów Mac OS.
19.	System musi zapewniać automatyczne szyfrowanie tzw. pliku wymiany Windows (pagefile).
20.	Moduł szyfrowania dysków pozwala na określenie, czy szyfrowaniu mają podlegać wszystkie partycje dysku, czy tylko partycja bootowalna (z której startuje właściwy system operacyjny) lub tylko partycje danych (non-bootable). Musi też istnieć możliwość określenia dowolnej konfiguracji partycji do zaszyfrowania.

1.2. Moduł szyfrowania plików

Lp.	Konfiguracja minimalna
1.	Rozwiązanie musi zapewnić: a. szyfrowanie plików i katalogów w ramach systemu operacyjnego i udziałów sieciowych udostępnianych przez serwery sieciowe. b. szyfrowanie danych kopiowanych na dyski twarde oraz nośniki zewnętrzne USB oraz CD/DVD.
2.	System szyfrowania plików i katalogów musi zapewniać centralne zarządzanie, w oparciu o CKZ, co najmniej w obszarze szyfrowania plików.
3.	Oprogramowanie szyfrujące na stacjach końcowych musi komunikować się z CKZ w

	bezpieczny sposób (transmisja szyfrowana).
4.	Rozwiązanie musi obsługiwać, co najmniej algorytm AES 256, jako algorytm szyfrowania danych.
5.	Rozwiązanie musi zapewniać mechanizm odzyskania danych, gdy użytkownik zapomni hasła lub utraci klucz.
6.	Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów oraz nośników zewnętrznych także w trybie off-line (kiedy stacja nie jest podłączona do sieci Zamawiającego i jeśli nie ma połączenia z centralnym serwerem zarządzającym)
7.	Decyzja o zaszyfrowaniu pliku/katalogu może zostać podjęta w oparciu o: a. centralnie zdefiniowaną politykę wskazująca foldery/pliki obligatoryjnie szyfrowane, b. lokalnie przez użytkownika.
8.	W przypadku centralnie definiowanej polityki musi być możliwe, co najmniej: a. wskazanie plików/folderów, które powinny być obligatoryjnie szyfrowane, b. wskazanie udziałów sieciowych, których pliki powinny być zaszyfrowane. Komunikacja między stacją użytkownika a udziałem sieciowym z zaszyfrowanymi plikami nie może powodować, że pliki lub ich części są przesyłane niezaszyfrowane.
9.	Uwierzytelnianie użytkownika na potrzeby systemu szyfrowania plików musi wykorzystywać uwierzytelnianie Microsoft Windows i umożliwiać przezroczystą pracę dla użytkowników bez potrzeby dodatkowego uwierzytelniania się.
10.	W przypadku, gdy Zamawiający zrezygnuje z mechanizmów uwierzytelniania wbudowanych w Microsoft Windows – powinna istnieć możliwość wykorzystania wbudowanego systemu uwierzytelniania w moduł szyfrowania plików.
11.	Rozwiązanie musi obsługiwać dowolne zewnętrzne nośniki wymienne USB i umożliwiać szyfrowanie na nich plików i katalogów. Powinny istnieć następujące możliwości szyfrowania nośników wymiennych: a. szyfrowanie proste, poprzez wymuszenia szyfrowania kopiowanych plików wprost na nośnik zewnętrzny (każdy wkopiowany plik będzie poddany szyfrowaniu), b. szyfrowanie konkretnego katalogu określonego ścieżką.

1.3. Oprogramowanie służące do ochrony stacji końcowych przed zagrożeniami (zwane dalej OOPZ):

Lp.	Konfiguracja minimalna
1.	Pakiet oprogramowania do ochrony stacji komputerowych przed zagrożeniami winno składać się z: a) modułu antywirusowego (dalej AV), b) modułu hostowego firewall'a (dalej FW), c) modułu Host IPS (dalej HIPS), d) modułu ochrony przeglądarek webowych przed złośliwymi stronami web (dalej WP), e) modułu kontroli portów (dalej KP), f) modułu kontroli aplikacji (dalej KA), g) modułu ochrony poczty elektronicznej (dalej OPE), h) modułu sandbox. Rozwiązanie winno posiadać Centralną Konsolę Zarządzającą obsługującą konfigurację, przegląd zdarzeń, itp. co najmniej obejmującą swym zakresem obszar pojedynczych modułów wchodzących w skład OOPZ.
2.	Instalacja OOPZ (co najmniej agenta zarządzającego na stacji końcowej) powinna być możliwa poprzez instalację ręczną oraz instalację automatyczną z użyciem konsoli zarządzającej lub zewnętrznego oprogramowania wymagającego plików MSI.
3.	Oprogramowanie OOPZ powinno umożliwić pracę w środowiskach całkowicie izolowanych, gdzie nie ma dostępu do Internetu. Powinna istnieć możliwość ręcznej aktualizacji wszystkich komponentów wymagający cyklicznej aktualizacji z użyciem

	CKZ.
4.	W ramach modułów OOPZ muszą być obecne mechanizmy samoobrony przed próbami zatrzymania lub wyłączenia ochrony poprzez te moduły. Powinny być mechanizmy zapobiegające modyfikacjom zarówno struktury plików, procesów, jak i rejestrów niezbędnych do pracy OOPZ. Wszystkie próby zatrzymania lub modyfikacji konfiguracji powinny być logowane.
5.	System OOPZ musi mieć możliwość ochrony przed zmianą konfiguracji przez użytkownika pracującego na stacji końcowej oraz przed odinstalowaniem oprogramowania OOPZ. Wprowadzenie zmian czy deinstalacja powinny być możliwe po wprowadzeniu zdefiniowanego przez Administratora hasła, lub z użyciem innego, bezpiecznego mechanizmu wymuszającego posiadanie specjalnych przywilejów w systemie.
6.	Rozwiązanie musi zapewniać ochronę przed modyfikacją systemu operacyjnego oraz innych zasobów, w tym: a. musi umożliwiać definiowanie reguł pozwalających na blokowanie dostępu do katalogów lub plików, b. musi zapewniać na stacjach roboczych ochronę systemu operacyjnego przed nieuprawnionymi modyfikacjami, korzystając z wbudowanych mechanizmów pozwalających co najmniej na kontrolę: zmian ustawień sieciowych, dodawania programów do obszaru autorun, zmian i tworzenia plików systemowych oraz procesów podszywających się pod procesy systemowe, dodawania nowych usług, zmian kluczowych rejestrów, c. system powinien posiadać wbudowane reguły realizujące ochronę kluczowych obszarów stacji roboczej, d. w ramach ochrony przed modyfikacją systemu operacyjnego, powinno być możliwe zdefiniowanie procesów, które nie będą podlegały pod tę ochronę.
7.	Musi istnieć możliwość automatycznego instalowania na komputerach roboczych nowych wersji modułów wchodzących w skład OOPZ, poprawek typu service pack oraz hot-fix'ów.
8.	Rozwiązanie musi umożliwiać sprawdzanie adresów, z którymi łączy się stacja robocza w bazie reputacyjnej producenta rozwiązania. W przypadku stwierdzenia próby komunikacji z niebezpiecznym adresem – oprogramowanie winno umożliwiać, co najmniej blokowanie połączenia.
Moduł Antywirusowy (dalej AV)	
9.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej, co najmniej procesy związane z AV.
10.	System AV musi zapewnić ochronę antywirusową na podstawie następujących mechanizmów: a. plikach definicji antywirusowych (zwanych dalej plikami DEF), b. heurystyki, c. reputacji obiektów z użyciem systemu reputacji producenta.
11.	Pliki z definicjami (sygnatury) – pliki DEF, muszą być regularnie dostarczane przez producenta rozwiązania, oprogramowanie musi pozwalać na, co najmniej dzienne aktualizacje (w okresie trwania wsparcia technicznego). Rozwiązanie musi zapewniać dostęp w czasie rzeczywistym do aktualnych sygnatur zlokalizowanych na serwerach producenta. Oferowane rozwiązanie musi umożliwiać aktualizację plików DEF na stacjach klienckich z wykorzystaniem poniższych mechanizmów: a. serwera aktualizacji wskazanego przez producenta, umiejscowionego w Internecie, b. serwera aktualizacji zdefiniowanego przez Zamawiającego, c. serwera aktualizacji umieszczonego w sieci intranetowej Zamawiającego.

	W przypadku serwera aktualizacji zdefiniowanego przez Zamawiającego lub zlokalizowanego w intranecie Zamawiającego, serwer ten musi umożliwiać zdefiniowanie harmonogramu aktualizacji.
12.	Skanowanie antywirusowe musi odbywać się w dwóch następujących trybach: a. Skanowanie podczas dostępu – skanowanie wybranych plików, gdy jest realizowany dostęp do pliku, b. Skanowanie na żądanie – skanowanie plików według wcześniej zdefiniowanego harmonogramu przez administratora. W przypadku skanowania na żądanie rozwiązanie musi umożliwiać: a. zdefiniowanie skanu, który wykona się według zadanego harmonogramu jednorazowo lub cyklicznie, b. zdefiniowanie skanu, który będzie wstrzymywany w momencie wykrycia podwyższonej aktywności użytkownika na danej stacji roboczej, c. wznawianie skanowania, które zostało wstrzymane w momencie wykrycia pracy użytkownika lub przerwany w wyniku restartu komputera, d. definiowanie obszaru skanowania: wśród dostępnych obszarów powinny być co najmniej: pamięć komputera, wszystkie dyski, wybrane dyski, rejestr systemowy, wszystkie uruchomione procesy, wybrane foldery. W przypadku skanowania podczas uzyskiwania dostępu i skanowania na żądanie rozwiązanie musi umożliwiać: a. definiowanie list plików lub katalogów wykluczonych ze skanowania - zdefiniowane pliki lub lokalizacje będą pomijane przez moduły skanujące, b. włączanie/wyłączanie mechanizmu reputacyjnego plików, c. definiowanie akcji, które będą podjęte przy wykryciu zagrożenia - wśród dostępnych akcji powinny być co najmniej: próba wyczyszczenia pliku, skanowania pliku lub uniemożliwienie dostępu do pliku.
13.	System AV musi zapewnić ochronę przed programami typu Spyware oraz Potencjalnie Niechcianymi Programami.
14.	System AV musi posiadać funkcjonalność lokalnej kwarantanny dla plików zainfekowanych. Uwolnienie plików z kwarantanny powinno być możliwe z użyciem lokalnego interfejsu graficznego, jeśli polityka na to zezwala lub z poziomu Centralnej Konsoli Zarządzającej.
15.	System AV musi mieć możliwość skanowania sektorów rozruchowych dysków.
16.	System AV musi mieć możliwość skanowania dysków sieciowych.
Moduł firewall (dalej FW)	
17.	Moduł FW ma za zadanie kontrolować ruch przychodzący i wychodzący ze stacji roboczej i wymuszać politykę dopuszczonego ruchu wymuszaną przez Administratora.
18.	W ramach modułu FW musi być możliwe tworzenie reguł, które mogą być oparte o: a. kierunek ruchu – wejściowy lub wyjściowy, b. interfejs sieciowy lub sieć logiczna, c. użyty protokół sieciowy, d. typ połączenia sieciowego - powinny być dostępne, co najmniej typy: połączenie przewodowe, połączenie bezprzewodowe, e. źródłowych i docelowych adresów IP, f. protokołu obecnego w warstwie czwartej - w przypadku wybrania protokołu TCP oraz UDP możliwość zdefiniowania portu źródłowego i docelowego, g. aplikacji generującej ruch – definicja aplikacji powinna być realizowana poprzez, co najmniej jedną z metod: wskazanie nazwy lub/i ścieżki pliku, skrótu kryptograficznego (hash, minimum jeden z: MD5, SHA-1 lub SHA-2) lub/oraz podpisu cyfrowego pliku.
19.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej

	Konsoli Zarządzającej obsługującej, co najmniej procesy związane z FW.
20.	Wszystkie reguły muszą być zarządzane z poziomu Centralnej Konsoli Zarządzania i rozpatrywane w kolejności wystąpienia.
21.	Wszystkie reguły muszą mieć możliwość logowania wystąpienia danego ruchu i jego przeglądania z poziomu Centralnej Konsoli Zarządzającej.
22.	Musi istnieć możliwość tworzenia reguł przypisanych do konkretnej sieci, wcześniej zdefiniowanej. W przypadku, gdy stacja robocza włącza się do konkretnej sieci, oprócz reguł globalnych, winny obowiązywać reguły przypisane do tej sieci.
23.	Moduł FW musi mieć możliwość izolacji ruchu sieciowego pomiędzy różnymi interfejsami sieciowymi.
24.	W module FW musi istnieć możliwość definiowania, co najmniej sieci zaufanych oraz aplikacji zaufanych by w łatwy sposób zezwalać na ruch sieciowy w obrębie sieci zaufanych lub ruch sieciowy inicjowany przez zaufane aplikacje.
25.	Moduł FW powinien dawać możliwość ograniczania ruchu do/ze stacji roboczej zanim usługi modułu FW będą aktywne.
Moduł ochrony przeglądarek webowych przed złośliwymi stronami web (dalej WP)	
26.	Moduł WP musi współpracować, co najmniej z następującymi przeglądarkami: Microsoft Internet Explorer, Mozilla Firefox i Google Chrome działającymi na stacjach roboczych.
27.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z ochroną ruchu webowego.
28.	Producent modułu WP musi dokładać wszelkich starań, by zapewniać wsparcie dla nowych wersji przeglądarek niedługo po ich ukazaniu się.
29.	Zaproponowane rozwiązanie winno posiadać mechanizm uniemożliwiający wyłączenie ochrony ruchu webowego przez użytkownika na stacji roboczej.
30.	Reputacja stron musi być określana dynamicznie na podstawie reputacyjnej bazy danych udostępnianej przez producenta oprogramowania. Baza reputacyjna winna być regularnie aktualizowana by zapewnić maksymalne bezpieczeństwo ruchu webowego.
31.	W przypadku zidentyfikowania próby dostępu do strony o złej reputacji, mechanizmy aplikacji winny umożliwiać blokowanie dostępu do strony, jednocześnie wyświetlając użytkownikowi stosowny komunikat.
32.	Moduł WP musi posiadać możliwość sprawdzania reputacji obiektów ściągniętych ze strony oraz skanowania ich poprzez przekazanie ich do innych modułów, w tym AV.
33.	Moduł WP musi wykrywać ładowanie stron typu „phishing", które podszywają się pod inne strony cieszące się dobrym zaufaniem.
34.	Moduł WP musi umożliwiać określenie zakresów blokowanych stron web na podstawie kategorii stron (np. pornografia, hazard, gry, portale społecznościowe, itp.). Musi istnieć możliwość skorzystania, z co najmniej 50 różnych popularnych kategorii utrzymywanych i aktualizowanych przez producenta modułu.
35.	Moduł WP musi umożliwiać blokowanie i przepuszczanie dostępu do wskazanych stron web, określonych przez administratora w politykach globalnych, niezależnie od ich poziomu reputacji/ryzyka (tzw. whitelist i blacklist), poprzez podanie adresu DNS lub IP.
36.	Zasady ostrzegania i blokowania dostępu do stron muszą działać także w sytuacji, kiedy stacja robocza pracuje poza siecią firmową Zamawiającego.
Moduł Host IPS (dalej HIPS)	
37.	Oferowane oprogramowanie musi oferować funkcjonalność Host IPS i zapobiegać włamaniom, korzystając z reguł zabezpieczających stację roboczą i uniemożliwiających wykorzystanie podatności aplikacji i systemu operacyjnego.
38.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej, co najmniej procesy związane z obsługą IPS.
39.	Zaimplementowane mechanizmy IPS muszą operować na sygnaturach znanych ataków i wykorzystywanych przez nie podatności oraz na analizie behawioralnej zachowania procesów działających na chronionych stacjach roboczych.

40.	Oprogramowanie host IPS musi wykrywać i zapobiegać atakom przepełnienia bufora (Buffer Overflow) we wszystkich aplikacjach działających na chronionej stacji roboczej.
41.	Do każdej sygnatury musi być dołączony opis, który opisuje działanie sygnatury i w miarę możliwości odwołuje się do bazy CVE.
42.	Zaoferowane rozwiązanie musi oferować możliwość pisania własnych sygnatur IPS i wysłania ich na chronione systemy.
43.	Oprogramowanie musi uniemożliwiać zmianę konfiguracji IPS przez użytkownika na stacji roboczej.
Moduł kontroli portów (dalej KP)	
44.	Moduł KP musi zapewnić ochronę przed podłączaniem niepożądanych urządzeń do stacji klienckich i powinien być w pełni zarządzany przez co najmniej własną Centralną Konsolę Zarządzającą.
45.	Moduł musi mieć możliwość: logowania zdarzeń, powiadamiania użytkowników o zdarzeniach, blokowania/dopuszczania urządzeń zgodnie z konfiguracją.
46.	Moduł KP musi wykrywać i blokować urządzenia podłączane przez porty zewnętrzne komputera, takie jak pendrive, PDA, kamera cyfrowa, odtwarzacze MP3, drukarki, karty pamięci, aparaty telefoniczne, tablety i inne typy urządzeń oraz umożliwiać zmianę sposobu dostępu do urządzeń posiadających system plików. Moduł KP musi oferować co najmniej poniższe tryby dostępu do urządzeń posiadających system plików: - pełny dostęp, - tylko do odczytu, - blokowanie urządzenia.
47.	Rozwiązanie musi umożliwiać przechowywanie informacji o: nazwie urządzenia, czasie przyłączenia, typie urządzania, kodzie producenta i urządzenia, nr seryjnym i typie systemu plików (zależnie od typu urządzenia i jego zestawu parametrów).
48.	Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania zewnętrznych nośników danych USB na podstawie ich numeru seryjnego, ID producenta i ID produktu.
49.	Polityka działania modułu musi umożliwiać przypisanie różnych polityk zależnie od przynależności użytkownika do grup użytkowników synchronizowanych z Active Directory.
Moduł kontroli aplikacji (dalej KA)	
50.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy kontroli aplikacji (KA).
51.	System KA musi umożliwiać budowanie whitelist (białych list), czyli list aplikacji dozwolonych na danej stacji roboczej. Aplikacje z tej listy będą mogły być uruchamiane na wskazanych stacjach roboczych.
52.	System KA musi umożliwiać budowanie blacklist (czarnych list), czyli list aplikacji niedozwolonych na danej stacji roboczej. Uruchomienie aplikacji z tej listy musi być blokowane na wskazanych stacjach roboczych.
53.	Rozwiązanie KA ma działać, jako agent na chronionych komputerach w sposób ciągły i reagować natychmiast – nie jest dopuszczalne wykonywanie kontroli aplikacji okresowo, co pewien czas.
54.	Oprogramowanie KA musi być chronione przed nieupoważnionym zatrzymaniem lub odinstalowaniem.
55.	Rozwiązanie musi zapewnić taki sam poziom ochrony niezależnie od tego czy stacja robocza pracuje w sieci firmowej czy poza nią – bez dostępu do CKZ.
56.	Rozwiązanie musi monitorować (generować logi z wystąpienia) i aktywnie blokować próby uruchomienia nieupoważnionego oprogramowania w postaci wykonywalnej (exe, com), skryptów (co najmniej BAT, JavaScript, VBScript), bibliotek, driverów podejmowane przez użytkowników, nieupoważnionych administratorów czy inne oprogramowanie uruchomione na stacji klienckiej.

57.	Rozwiązanie musi zapewniać bazę reputacyjną aplikacji prowadzoną przez producenta oprogramowania. Baza reputacyjna musi umożliwiać określenie poziomu bezpieczeństwa aplikacji. Blokowanie uruchomienia aplikacji musi odbywać się na podstawie zawartości czarnej listy oraz/lub informacji pozyskanych z bazy reputacyjnej. Baza reputacyjna musi być regularnie aktualizowana przeze producenta oprogramowania. Baza reputacyjna musi być dostępna zarówno z sieci wewnętrznej Zamawiającego jak i z Internetu.
58.	Rozwiązanie musi umożliwiać włączenie trybu, w którym przygotowana zostanie automatycznie lista aplikacji uruchomionych na stacji roboczej. Jednocześnie wszystkie umieszczone na tej liście aplikacje otrzymają status „dopuszczonych" do użytkowania na tej stacji. Centralna Konsola Zarządzająca musi umożliwiać przeglądanie list wykrytych i dopuszczonych do działania aplikacji i procesów. CKZ musi również umożliwiać administratorowi zmianę statusu aplikacji umieszczonych na w/w liście na aplikacje blokowane.
59.	Rozwiązanie musi zapewnić obsługę trybu obserwacji/monitorowania, w którym agent realizuje politykę ochrony, ale nie jest wymuszane blokowanie aplikacji. Informacje o blokowaniu, które byłoby podjęte przez agenta KA w normalnym trybie pracy mają być wysyłane do Centralnej Konsoli Zarządzającej celem ułatwienia przygotowania przez administratora docelowej polityki blokowania aplikacji.
60.	Rozwiązanie KA musi umożliwiać wyświetlenie użytkownikowi komunikatu na stacji z informacją o zablokowaniu uruchomienia aplikacji/procesu.
61.	W razie wystąpienia nieautoryzowanej próby uruchomienia aplikacji, procesu, drivera, biblioteki czy skryptu, agent KA ma zapisać informacje o zdarzeniu i przekazać je do Centralnej Konsoli Zarządzającej. W ramach tej informacji powinny się znaleźć, co najmniej następujące dane: a. czas zdarzenia, b. nazwa komputera, na jakim wystąpiło zdarzenie, c. nazwa zalogowanego użytkownika, d. opis zdarzenia z podaniem nazwy aplikacji, procesu, drivera, biblioteki, skryptu, która została zablokowana, e. informację o ewentualnym procesie/aplikacji inicjującej zablokowane uruchomienie.
Moduł ochrony poczty elektronicznej (dalej OPE)	
62.	Moduł OPE ma realizować ochronę serwerów poczty elektronicznej pracujących pod kontrolą MS Exchange 2013 i nowszych, wykorzystywanych przez Zamawiającego.
63.	Moduł OPE musi: 1. Zapewniać ochronę przed wszystkimi rodzajami szkodliwego oprogramowania typu: wirus, koń trojański, ransomware, spyware, adware, rootkit, auto-dialer i innymi potencjalnie niebezpiecznymi lub niechcianymi programami. 2. Skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. 3. Umożliwiać skanowanie bezpośrednio w bazach Exchange na serwerze pocztowym. 4. Umożliwiać usunięcie wiadomości lub załącznika w przypadku wykrycia wirusa lub blokowania wiadomości i wyleczenia / podmiany załącznika na czysty plik zawierający jedynie informację o infekcji. 5. Umożliwiać stosowanie i tworzenie różnych reguł blokowania wiadomości w zależności od zdefiniowanych filtrów/ kryteriów (minimum: nadawca, odbiorca, temat, treść, nazwa i rozszerzenie pliku załącznika, wielkość wiadomości). 6. Posiadać mechanizm antyspamowy wyposażony w co najmniej filtr, sprawdzanie list reputacji, a także kontrolę reputacji poczty. 7. Realizować skanowanie w czasie rzeczywistym otwieranych, zapisywanych plików. 8. Zapewnić skanowanie plików archiwów (spakowanych).

	9. Skanować w czasie rzeczywistym pocztę przychodzącą i wychodzącą. 10. Zapewniać skanowanie i oczyszczanie poczty przychodzącej MAPI oraz IMAP w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji klienckiej. W przypadku wykrycia wirusa moduł musi wysłać powiadomienie do administratora systemu pocztowego z użyciem e-mail. 11. Umożliwiać prowadzenie dziennika zdarzeń rejestrującego informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania, musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych modułu. 12. Zapewnić codzienną aktualizację wzorców wirusów. 13. Zapewnić zarządzanie modułem OPE z poziomu Centralnej Konsoli Zarządzania obsługującej przynajmniej konfigurację i kontrolę logów w module OPE.
	Moduł Sandbox
64.	Zaproponowane rozwiązanie musi dawać możliwość konteneryzacji przy wykonywaniu nieznanych plików. Pliki nieznane (z punktu widzenia sygnatur i mechanizmu reputacji) powinny być uruchamiane w izolowanym środowisku (sandbox), które minimalizuje ryzyko wykonania szkodliwej aktywności kodu. Wszystkie dane otrzymywane za pośrednictwem poczty email lub poprzez strony Web, które zostaną przez system uznane za „niepewne" powinny być sprawdzane w izolowanym środowisku. Analiza nie może wymagać przesyłania testowanych plików poza chronioną infrastrukturę. Zamawiający dopuszcza wyjątek dla skanowania zagrożeń dotyczących systemu operacyjnego MacOS X. Zamawiający oczekuje funkcjonalności pozwalającej na dowolność włączenia i wyłączenia analizowania zagrożeń dla systemu MacOS X. Rozwiązanie winno zapewniać ochronę sieci i innych podsystemów teleinformatycznych przed zaawansowanymi atakami typu APT (Advanced Persistent Threat) mającymi na celu uniknięcie wykrycia przez obecne w infrastrukturze zamawiającego systemy zabezpieczające takie jak bramy e-mail i webowe, systemy IPS/IDS czy oprogramowanie antywirusowe. Rozwiązanie winno również ograniczać skutki szkodliwego oprogramowania typu zero-day. Izolowane środowiska (sandbox), w których powinny być sprawdzane podejrzane pliki winny składać się z co najmniej 5 maszyn wirtualnych, które można spreparować w taki sposób, by imitowały stacje robocze użytkowane w infrastrukturze Zamawiającego (te same wersje systemów operacyjnych, charakterystyczne aplikacje, konfiguracja, itp.).

1.4. Ochrona serwerów fizycznych oraz wirtualnych:

Lp.	Konfiguracja minimalna
1.	System musi zapewniać bezpieczeństwo na poziomie serwerów fizycznych oraz wirtualnych. Moduł ochrony serwerowej musi zapewnić co najmniej poniższe funkcjonalności bezpieczeństwa: firewall, IPS, monitorowanie integralności danych, inspekcja logów, blokowanie ruchu zabronionych aplikacji, anti-malware. Poszczególne funkcjonalności bezpieczeństwa muszą posiadać zakres ochrony co najmniej na poziomie ich odpowiedników na stacjach roboczych, opisanych w części dotyczącej OOPZ. System musi pozwalać na definiowanie polityk bezpieczeństwa przypisanych do

	konkretnych typów maszyn. Tak utworzone polityki powinny być przypisywane automatycznie (przez system) do nowo tworzonych maszyn, aktywując na nich przewidziane polityką mechanizmy ochrony. W związku z powyższym, system musi umożliwiać tworzenie logicznych grup serwerów. Moduł potrafi ochronić system przed szeregiem znanych podatności, pomimo tego, że system nie posiada zaimplementowanych odpowiednich łatek niwelujących zagrożenie. Moduł działa na zasadzie ochrony przed możliwością wykonania kodu wykorzystującego podatność na podatnej wersji oprogramowania. Moduł ochrony serwerowej winien również na bieżąco analizować zainstalowane aplikacje i w przypadku pojawienia się nowej, automatycznie uruchamiać dodatkowe polityki bezpieczeństwa. Moduł ochrony serwerowej musi zapewniać wsparcie dla następujących systemów operacyjnych: Windows Server 2008/2008R2, Windows Server 2012/2012R2, Windows Server 2016/2016R2, Ubuntu LTS. Moduł ochrony serwerowej musi zapewniać wsparcie dla środowiska wirtualizacji, co najmniej VMware. System musi pozwalać na swobodny wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych.

1.5. Funkcjonalności ogólne:

Lp.	Funkcjonalności ogólne:
1.	**Kryterium: Centralna Konsola Zarządzająca** Rozwiązanie musi dostarczać Centralną Konsolę Zarządzania (dalej zwaną CKZ), która pozwala na zarządzanie z jednego miejsca co najmniej poniższymi modułami: - szyfrowania dysków, - szyfrowania plików, - zarządzania mechanizmami ochrony stacji końcowych przed zagrożeniami (OOPZ). CKZ zapewni funkcjonalność zarządzania politykami w celu konfiguracji oraz implementacji ustawień modułów na poziomie samych modułów oraz poziomie stacji roboczych. Konsola zarządzająca CKZ zapewni pojedynczy punkt monitoringu dla oprogramowania *anti-malware*, oraz modułów badających zawartość danych pod kątem bezpieczeństwa. CKZ umożliwia administratorom systemów monitorowanie i raportowanie aktywności takich jak: infekcje, naruszenia bezpieczeństwa oraz punkty wejścia w przypadku wirusów oraz malware. Funkcjonalności CKZ pozwolą administratorom systemów ściągnąć i zastosować uaktualnienia komponentów poprzez sieć, dzięki czemu zapewniona zostanie aktualność oraz konsystencja systemu. CKZ umożliwi manualne oraz predefiniowane aktualizacje. CKZ umożliwi także konfigurowanie oraz administrowanie produktami w grupach lub osobno. CKZ służy do wymiany informacji o zagrożeniach w obrębie organizacji, w której zainstalowane są komponenty wchodzące w skład obsługiwanych modułów.

	Centralna Konsola Zarządzania powinna się składać z oprogramowania serwerowego oraz agentów instalowanych na stacjach końcowych, których zadaniem jest konfigurowanie zarządzanych produktów oraz zbieranie zdarzeń i przekazywanie ich do CKZ. Zarządzanie wszystkimi modułami i pełnym zakresem funkcji dostarczonego systemu ochrony musi następować z jednej i tej samej aplikacji (konsoli) działającej co najmniej na serwerze Microsoft Windows (wymagane wsparcie dla co najmniej wersji Windows 2008 R2 i Windows 2012 i Windows 2012 R2 oraz Windows 2016/2016 R2) lub Linux i korzystającej z bazy danych Microsoft SQL (wymagane wsparcie co najmniej dla wersji SQL 2014) lub bazy danych MySQL co najmniej w wersji 5.5. CKZ musi być skalowalna i umożliwiać zarządzanie co najmniej 1 tysiącem komputerów i zainstalowanych na nich produktów - wymaganie dotyczy możliwości technicznych, wydajnościowych aplikacji a nie możliwości jakie dają zaoferowane licencje. Centralna konsola zarządzająca (CKZ) musi umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów. Centralna konsola zarządzająca (CKZ) musi umożliwiać tworzenie szczegółowych konfiguracji pracy poszczególnych produktów i dystrybucję polityk oraz wymuszanie ich zastosowania. CKZ musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu. CKZ musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory. CKZ musi być przygotowana do pracy w strefie DMZ (dostępnej z sieci publicznych) tak, aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną, bez zestawiania połączeń VPN lub SSL VPN i aby jednocześnie podstawowy serwer zarządzający zawierający CKZ nie był narażony na potencjalne ataki z zewnątrz. System zarządzania CKZ ma zapewnić centralne repozytorium (oparte na relacyjnej bazie danych) dla logów i zdarzeń logowanych przez wszystkie moduły systemu ochrony: a. Zbieranie zdarzeń logowanych we wszystkich modułach dostarczanego systemu ochrony na wszystkich chronionych węzłach (komputerach i serwerach) i składowanie ich w centralnym repozytorium będącym integralną częścią systemu. b. Zbieranie zdarzeń musi obejmować wszystkie zdarzenia logowane przez moduły dostarczonego oprogramowania. c. Mechanizm zbierania zdarzeń musi umożliwiać ograniczenie zbieranych zdarzeń na podstawie wybieranego przez administratora kryterium, d. Podsystem zbierający zdarzenia musi zapewniać centralne zarządzanie z pojedynczej konsoli dla wszystkich komponentów oprogramowania.

	Konsola zarządzająca CKZ ma umożliwiać centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach (np. PDF, XML, HTML): a. Raporty powinny być generowane na żądanie, ale powinna istnieć możliwość określenia zakresu raportu i częstotliwości jego automatycznego generowania b. Raporty powinny bazować na predefiniowanych przez producenta szablonach dla poszczególnych zarządzanych produktów, a także powinna być możliwość tworzenia własnych raportów przez administratorów. CKZ musi posiadać dostępny bez dodatkowych opłat licencyjnych interfejs API umożliwiający Zamawiającemu automatyzację podstawowych czynności administracyjnych - w tym co najmniej: dodawanie i usuwanie kont administratorów systemu, usuwanie logów, uruchamianie i zatrzymywanie zadań do wykonania przez serwer zarządzający (np. ściągaj aktualizację produktów), przypisywanie określonych polityk produktów do grup komputerów, dodawanie komputerów do listy zarządzanych maszyn wraz z automatycznym uruchomieniem dla nich zadań instalacji oprogramowania ochronnego, usuwanie komputerów z listy zarządzanych maszyn.

W przypadku zaoferowania oprogramowania równoważnego Wykonawca zapewni wdrożenie, migrację danych z systemu posiadanego przez Zamawiającego, wsparcie techniczne na czas trwania umowy oraz szkolenie 5 administratorów w wymiarze 40 (czterdziestu) godzin.

Załącznik Nr 2 do SWZ

FORMULARZ OFERTY

dla Narodowego Centrum Badań i Rozwoju

Ja/my* niżej podpisani:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

działając w imieniu i na rzecz:

.....

.....

(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)

Adres:

……

Kraj ……..

REGON ……

NIP: ……..

TEL. …….

Adres skrzynki ePUAP ……

adres e-mail:……

(na który Zamawiający ma przesyłać korespondencję)

Wykonawca jest mikro, małym, średnim przedsiębiorcą - **TAK/NIE***

Ubiegając się o udzielenie zamówienia publicznego na ***dostawę licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN.***

SKŁADAMY OFERTĘ na realizację przedmiotu zamówienia w zakresie określonym w Specyfikacji Warunków Zamówienia, na następujących warunkach:

1.1. **Cena oferty netto** za realizację całego zamówienia wynosi: ……..……. zł, (słownie:……),

1.2. **Cena oferty brutto** za realizację całego zamówienia wynosi: ……..……. zł, (słownie:……).

w tym podatek od towarów i usług (VAT), wg stawki: ……. %,

zgodnie z cenami jednostkowymi ujętymi w poniższej tabeli:

l.p.	**Nazwa oprogramowania**	**Nazwa oprogramowania w przypadku oferowania oprogramowania równoważnego**	**Liczba licencji**	**Cena jednostkowa netto**	**Cena netto (Cena jednostkowa netto*liczba licencji)**	**Cena brutto**
1	McAfee Complete EndPoint Protection – Business		900			
2	McAfee Threat Intelligence Exchange		800			
3	McAfee Virtual Advanced Threat Defence Appliance		1			
				Suma		

2. **OŚWIADCZAMY,** że zamówienie wykonamy w terminie podanym przez Zamawiającego.
3. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i akceptujemy oraz spełniamy wszystkie warunki w niej zawarte.
4. **OŚWIADCZAMY**, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.
5. **OŚWIADCZAMY**, że jesteśmy związani niniejszą ofertą od dnia upływu terminu składania ofert do dnia 19.05.2021 roku.
6. **OŚWIADCZAMY**, że zapoznaliśmy się z Projektowanymi Postanowieniami Umowy, określonymi w Załączniku nr 4 do Specyfikacji Warunków Zamówienia i ZOBOWIĄZUJEMY SIĘ, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.
7. **AKCEPTUJEMY** Projektowane Postanowienia Umowne, w tym warunki płatności oraz termin realizacji przedmiotu zamówienia podany przez Zamawiającego.

8. **OŚWIADCZAM**, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[2] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**
9. **SKŁADAMY** ofertę na _____stronach.
10. Wraz z ofertą **SKŁADAMY** następujące oświadczenia i dokumenty:

1. ……
2. ……
3. ……

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

Informacja dla Wykonawcy:

Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.

** niepotrzebne skreślić*

*** 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 Wykonawca nie składa oświadczenia (usunięcie treści oświadczenia następuje np. przez jego wykreślenie).*

[2] 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 3 do SWZ

Nazwa Wykonawcy, w imieniu którego składane jest oświadczenie:

.....

.....

.....

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

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WSTĘPNE OŚWIADCZENIE WYKONAWCY[3]

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako: Pzp)

DOTYCZĄCE PODSTAW WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. *Dostawa licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN,* prowadzonego przez Narodowe Centrum Badań i Rozwoju (NCBR), z siedzibą w Warszawie (00-695), przy ul. Nowogrodzkiej 47a (NIP: 701-007-37-77, REGON: 141032404), oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 art. 109 ust. 1 pkt 4, 5, 7 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, 5 lub 6 ustawy Pzp)*. Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:

[3] *Pouczenie o odpowiedzialności karnej Art. 297 § 1 Kodeksu karnego* (Dz. U. Nr 88 poz. 553 z późn. zm.)*:*
„Kto w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi – kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, elektronicznego instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”

……

……

……

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

DOTYCZĄCE SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Oświadczam, że spełniam(-my) warunki udziału w postępowaniu na *dostawę licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN,* dotyczące posiadania zdolności technicznej oraz zawodowej określonej w art. 112 ust. 2 pkt 4 ustawy *z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.)*, zwanej dalej „uPzp".

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

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.

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

Załącznik nr 4 do SWZ

PROJEKTOWANE POSTANOWIENIA UMOWY

/osobny plik/

Załącznik nr 6 do SWZ

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Lp.	Pytanie	Odpowiedź	Uwagi
1	Czy podmiot przetwarzający dane osobowe planuje wyznaczyć/wyznaczył Inspektora Ochrony Danych Osobowych (IOD)?	* - tak zaplanowano wyznaczenie - tak wyznaczono - nie zaplanowano wyznaczenia (uzasadnienie: np. nie jest wymagane przepisami prawa) - zaplanowano wyznaczenie (kiedy: podać przewidywaną datę)	
2	Jeżeli nie został wyznaczony IOD to proszę o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu….., stanowisko/funkcja…., numer tel.	
3	Czy podmiot przetwarzający dane osobowe wprowadził środki techniczne i organizacyjne, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych?	* TAK/NIE/INNE	
4	Czy podmiot przetwarzający dane osobowe korzysta z dalszych przetwarzających dane osobowe w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	* TAK/NIE	
5	Czy dane osobowe będą przekazywane poza Europejski Obszar Gospodarczy?	* TAK/NIE	

*Właściwe podkreślić/uzupełnić

Oświadczenie:

W imieniu podmiotu przetwarzającego dane osobowe /nazwa podmiotu/, oświadczam, że powyżej przekazane informacje są zgodne z prawdą. W przypadku zmiany któregokolwiek z ww. elementów, zobowiązuje się niezwłocznie (nie później niż w terminie 7 dni od wystąpienia zdarzenia) powiadomić o tym Narodowe Centrum Badań i Rozwoju.

…….. ……

data *Imię i nazwisko*

podpisano elektronicznie

Ocena Inspektora Ochrony Danych w Narodowym Centrum Badań i Rozwoju

Wypełnia IOD NCBR:

Rekomenduję/nie rekomenduję zawarcie umowy powierzenia przetwarzania danych osobowych.

Uzasadnienie:

……

……

……

…….. ……

data podpis

Załącznik Nr 7 do SWZ

Klauzula informacyjna dotycząca przetwarzania danych osobowych

1. Zgodnie z art. 13 ust. 1 i 2 oraz 14 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 Narodowe Centrum Badań i Rozwoju, ul. Nowogrodzka 47a, 00-695 Warszawa (dalej NCBR)*;*
   - w sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres ……, bądź pocztą elektroniczną na adres e-mail: iod@ncbr.gov.pl**;**

- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia zamówienia publicznego na *dostawę licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN,* udzielonego w trybie podstawowym bez negocjacji art. 275 pkt 1 ustawy Pzp;
- Pani/Pana dane osobowe zostały pozyskane od podmiotu, który odpowiedział na ogłoszenie o postępowaniu o udzielenie zamówienia publicznego wskazanym powyżej;
- NCBR będzie przetwarzał Pani/Pana dane w zakresie danych kontaktowych, informacji o zatrudnieniu, stopni naukowych oraz inne w zakresie podanym przez podmiot składający ofertę w odpowiedzi na ogłoszenie o udzieleniu zamówienia publicznego;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Pzp;
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 i 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, a następnie w celu archiwalnym przez okres zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;
- 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 lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia 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.
  - − 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 oraz art. 19 ust. 3 ustawy Pzp ;
  - − 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.

2. Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

Załącznik nr 8 do SWZ

Pełna nazwa Wykonawcy/Wykonawców

……

……

……

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

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WYKAZ DOSTAW

Dotyczy: zamówienia publicznego, którego przedmiotem jest ***dostawa licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT. Nr postępowania 8/21/TPBN***

W zakresie niezbędnym do wykazania spełnienia warunku wiedzy i doświadczenia, o którym mowa w rozdziale VII pkt 2.1 SWZ, w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie.

	Wymaganie Zamawiającego: **Wykonawca w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie, co najmniej dwie dostawy licencji na oprogramowanie ochrony infrastruktury IT o wartości każdej z nich, co najmniej 50 000,00 zł (słownie: pięćdziesiąt tysięcy złotych) brutto.**	
1.	**Nazwa i zakres dostawy**	…….. ……..
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej dostawy)*	od ……/……/……..... do ……/……/……..... *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał	……..……..……

	wykonanie dostawy)	……..…….……. *(nazwa i adres*)
	Wartość brutto	…….
	Dokument potwierdzający należyte wykonanie wyżej wymienionej dostawy	Nr załącznika do oferty ……..……
2.	**Nazwa i zakres dostawy**	…….. ……..
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej dostawy)*	od …..…/…..…./…..... do …..…/…..…./…..... *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał wykonanie dostawy)	……..…….…… ……..…….……. *(nazwa i adres*)
	Wartość brutto	…….
	Dokument potwierdzający należyte wykonanie wyżej wymienionej dostawy	Nr załącznika do oferty ……..……

Do powyższego wykazu załączam dowody potwierdzające, że wskazane w nim usługi, o których mowa w rozdziale VII pkt 2.1 SWZ, zostały wykonane należycie. [4]

……..……., dnia ……. r.

……..

Imię i nazwisko

podpisano elektronicznie

[4] W przypadku większej liczby usług należy powielić tabelę

Załącznik nr 9 do SWZ

Oświadczenie, o którym mowa w art. 117 ust. 4 ustawy z dnia 11 września 2019 r.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia

Działając na podstawie art. 117 ust. 4 ustawy Pzp oświadczam, iż Wykonawcy wspólnie ubiegający się o udzielenie zamówienia zrealizują przedmiotowe zamówienie w zakresie określonym w tabeli:

l.p.	Nazwa Wykonawcy	Zakres zamówienia realizowany przez Wykonawcę
1.		
2.		

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie