Załącznik Nr …

Projektowane postanowienia umowy

(dalej: „**Umowa**")

zawarta w Warszawie, pomiędzy:

Narodowym Centrum Badań i Rozwoju z siedzibą w Warszawie (00-695 Warszawa), adres: ul. Nowogrodzka 47a, posiadającym REGON: 141032404 oraz NIP: 701-007-37-77, działającym na podstawie ustawy z dnia 30 kwietnia 2010 r. o Narodowym Centrum Badań i Rozwoju (t.j. Dz. U z 2020 r. poz. 1861, ze zm.), zwanym dalej „**Zamawiającym**" lub „**NCBR**", reprezentowanym przez:

Panią/Pana …… – Dyrektora Działu ……. Narodowego Centrum Badań i Rozwoju, działającą/ego na podstawie upoważnienia z dnia ……...

(kopia upoważnienia do reprezentowania Zamawiającego stanowi Załącznik nr 1 do Umowy),

a

<imię i nazwisko>,……, zamieszkały/a w …… (kod pocztowy ……), przy ul. …….., PESEL …… prowadzący/a działalność gospodarczą pod firmą …… adres do doręczeń: …… (kod pocztowy ……), przy ul. ……, miejscowość ……. wpisany do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP ……, REGON ……, zwany/a dalej **„Wykonawcą"**, reprezentowany/a przez:……..

lub

<nazwa> spółka z ograniczoną odpowiedzialnością, z siedzibą w …… (miejscowość) adres: kod pocztowy ……, ulica ……, miejscowość ……. wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy ……, pod nr KRS ……, o kapitale zakładowym w wysokości …… zł, NIP ……, REGON ……, zwana dalej **„Wykonawcą"**, reprezentowana przez[1] :……

(wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Wykonawcy, kopia dokumentu, który upoważnia przedstawiciela Wykonawcy do zawarcia Umowy *stanowią Załącznik nr 2 do Umowy*)

zwanymi dalej łącznie „**Stronami**", a każda z osobna „**Stroną**."

Osoba upoważniona do reprezentacji Zamawiającego oświadcza, że udzielone jej upoważnienie nie wygasło, ani nie zostało odwołane, a jego treść nie uległa zmianie.

Umowa została zawarta w wyniku postępowania o udzielenie zamówienia publicznego prowadzonego na podstawie art. 275 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021

[1] Reprezentacja powinna być zgodna z informacjami w Krajowym Rejestrze Sądowym, który zawiera dane obowiązujące na dzień zawarcia umowy.

r., poz. 1129 ze zm.), zwanej dalej „pzp”.

§ 1.

Przedmiot Umowy

1. Przedmiotem umowy jest:
   1) odnowienie usługi wsparcia technicznego producenta dla McAfee Complete EndPoint Protection – Business – w ilości 900 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy;
   2) dostawa licencji McAfee Complete EndPoint Protection – Business – w ilości 150 szt. ważnych od dnia 26 maja 2022 r. przez czas nieoznaczony wraz z usługą wsparcia technicznego producenta na okres 36 miesięcy;
   3) odnowienie subskrypcji McAfee MVISION TIE – w ilości 800 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
   4) dostawa subskrypcji McAfee MVISION TIE – w ilości 100 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
   5) odnowienie subskrypcji McAfee Virtual Advanced Threat Defence Appliance – w ilości 1 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy,

   lub dostawa oprogramowania równoważnego (dalej jako: „**Oprogramowanie**” lub „**Przedmiot Umowy**”)
2. Szczegółowy opis Szczegółowy opis Przedmiotu Umowy, terminy i pozostałe wymagania Zamawiającego w zakresie wykonania Przedmiotu Umowy zawiera Szczegółowy Opis Przedmiotu Zamówienia, stanowiący Załącznik nr 3 do Umowy (dalej: „**SOPZ**”) oraz oferta Wykonawcy z dnia ……., stanowiąca Załącznik nr 4 do Umowy (dalej: „**Oferta**”).
3. W przypadku dostarczenia oprogramowania równoważnego, opis wymagań dla oprogramowania równoważnego zawarty został w pkt II SOPZ. Zaoferowane Oprogramowanie równoważne musi zakresowo odpowiadać co najmniej zakresowi Oprogramowania referencyjnego określonego w § 1 ust. 1 Umowy (rząd wielkości).
4. Wykonawca, ma prawo wypowiedzieć licencje na Oprogramowanie, z zachowaniem 10 letniego okresu wypowiedzenia, ze skutkiem na koniec roku kalendarzowego.

§ 2.

Zadania i zakres odpowiedzialności Wykonawcy

1. Na mocy Umowy Wykonawca zobowiązuje się do należytego wykonania Przedmiotu Umowy, w szczególności do:
   1) wykonania Przedmiotu Umowy w terminie oraz zgodnie z wymaganiami określonymi w Umowie, SOPZ i Ofercie;
   2) ponoszenia odpowiedzialności za wszelkie szkody, które Wykonawca lub działający na jego zlecenie Podwykonawca lub inny podmiot działający na zlecenie Wykonawcy spowoduje podczas lub w związku z wykonywaniem prac będących Przedmiotem Umowy;

3) zapewnienia możliwości korzystania z Oprogramowania i odnośnego wsparcia przez podmioty gospodarczo powiązane z Zamawiającym[2], w tym w szczególności NCBR+ sp. z o.o..

2. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem techniczno – organizacyjnym, personelem posiadającym odpowiednie kwalifikacje oraz wiedzą i doświadczeniem pozwalającym na należyte wykonanie Przedmiotu Umowy.
3. Wykonawca zobowiązuje się wykonać Umowę w sposób rzetelny i terminowy, z zachowaniem najwyższej staranności uwzględniającej zawodowy charakter prowadzonej przez niego działalności.
4. Wykonawca oświadcza, że nie są mu znane żadne przeszkody natury technicznej, prawnej ani finansowej, które mogą uniemożliwić wykonanie Przedmiotu Umowy.

§ 3.

Warunki realizacji Umowy

1. Oprogramowanie zostanie dostarczone na koszt i ryzyko Wykonawcy w terminie do 7 (siedmiu) dni kalendarzowych od zawarcia Umowy. Dostarczenie Oprogramowania polega na udostępnieniu przez Wykonawcę Zamawiającemu kluczy do Oprogramowania obejmującego licencje wskazane w Umowie za pośrednictwem poczty elektronicznej, wysyłając wiadomość email na adres: […] oraz na dostarczeniu w sposób umówiony przez Strony dokumentów potwierdzających udzielenie przez producenta Oprogramowania Zamawiającemu odpowiednich licencji[3].

   lub

   Oprogramowanie równoważne zostanie dostarczone na koszt i ryzyko Wykonawcy w terminie do 7 (siedmiu) dni kalendarzowych od zawarcia Umowy, natomiast usługi określone w pkt II SOPZ, tj. wdrożenie, migracja danych z systemu posiadanego przez Zamawiającego oraz szkolenie 5 administratorów w wymiarze 40 (czterdziestu) godzin zostaną zrealizowane nie później niż do dnia 26 maja 2022 r. Dostarczenie Oprogramowania równoważnego polega na udostępnieniu przez Wykonawcę Zamawiającemu kluczy do Oprogramowania równoważnego obejmującego licencje wskazane w Umowie za pośrednictwem poczty elektronicznej, wysyłając wiadomość email na adres: […] oraz na dostarczeniu w sposób umówiony przez Strony dokumentów potwierdzających udzielenie przez producenta Oprogramowania równoważnego Zamawiającemu odpowiednich licencji[4].
2. Oprogramowanie zostanie przekazane Zamawiającemu w sposób określony w ust. 1 przez przedstawicieli Wykonawcy, uprawnionych do udostępnienia/przekazania oraz dokonania wszelkich związanych z tym czynności.
3. Wykonawca nie może powierzyć wykonania Umowy innym podmiotom bez uprzedniego uzyskania w tym przedmiocie pisemnej zgody Zamawiającego. W przypadku uzyskania pisemnej zgody Zamawiającego i powierzenia przez Wykonawcę innym podmiotom wykonania Umowy, Wykonawca odpowiada za działania i zaniechania tych podmiotów, jak za własne działania lub zaniechania.
4. Wykonawca zapewnia, że dostarczone Oprogramowanie jest najwyższej jakości, wolne od

[2] Przez podmioty gospodarczo powiązane rozumie się spółki tworzone przez Zamawiającego na podstawie art. Art. 30a. ust. 1 pkt 2 Ustawy o Narodowym Centrum Badań i Rozwoju (Dz. U. 2020 poz. 1861 ze zm.)
[3] W przypadku zaoferowania oprogramowania referencyjnego
[4] W przypadku zaoferowania rozwiązania równoważnego

jakichkolwiek wad prawnych oraz zgodne z wymogami określonymi w SOPZ.

5. Z czynności odbioru Oprogramowania, w terminie do 5 (pięciu) dni od dnia dostawy Oprogramowania o którym mowa w ust. 1 powyżej, zostanie sporządzony i podpisany przez Zamawiającego protokół odbioru, którego wzór znajduje się w Załączniku nr 5 do Umowy (dalej jako: „**Protokół odbioru**"). Sporządzony i podpisany Protokół odbioru zostanie przesłany Wykonawcy w formie elektronicznej, na adres mailowy wskazany w § 8 ust. 2 pkt 1 Umowy[5].

   lub

   Z czynności odbioru Oprogramowania równoważnego, w terminie do 5 (pięciu) dni od dnia dostawy Oprogramowania równoważnego o którym mowa w ust. 1 powyżej, po dokonaniu przez Wykonawcę czynności wskazanych w SOPZ, zostanie sporządzony i podpisany przez Zamawiającego Protokół odbioru. Sporządzony i podpisany Protokół odbioru zostanie przesłany Wykonawcy w formie elektronicznej, na adres mailowy wskazany w § 8 ust. 2 pkt 1 Umowy. Realizacja Przedmiotu Zamówienia w zakresie usług określonych w pkt II SOPZ, polega na wykonaniu wszystkich czynności tam określonych i zgłoszeniu tego na adres mailowy zamawiającego wskazany w § 8 ust. 2 pkt 2 Umowy, po zakończeniu realizacji ostatniej z tych czynności. Z czynności odbioru zrealizowanych usług określonych w pkt II SOPZ zostanie sporządzony i podpisany przez Zamawiającego Protokół odbioru. Sporządzony i podpisany Protokół odbioru zostanie przesłany Wykonawcy w formie elektronicznej, na adres mailowy wskazany w § 8 ust. 2 pkt 1 Umowy [6].

6. W przypadku stwierdzenia w Protokole odbioru braków i/lub wad dostarczonego Oprogramowania lub stwierdzenia jego dostarczenia przez Wykonawcę w sposób niezgodny z Umową, Wykonawca zobowiązuje się najdalej w ciągu **3 (trzech) dni** kalendarzowych do wymiany i dostarczenia Oprogramowania zgodnego z Umową. Termin, o którym mowa w zdaniu poprzednim, liczony będzie od dnia przekazania Protokołu odbioru z zastrzeżeniami na adres mailowy wskazany w § 8 ust. 2 pkt 1 Umowy[7].

   lub

   W przypadku stwierdzenia w Protokole odbioru:

   1) braków i/lub wad dostarczonego Oprogramowania równoważnego lub stwierdzenia jego dostarczenia przez Wykonawcę w sposób niezgodny z Umową,
   2) niewykonania lub nieprawidłowego wykonania usług określonych w pkt II SOPZ,

   Wykonawca zobowiązuje się najdalej w ciągu **3 (trzech) dni** kalendarzowych do wymiany i dostarczenia Oprogramowania równoważnego zgodnego z Umową lub należytego wykonania usług określonych w pkt II SOPZ. Termin, o którym mowa w zdaniu poprzednim, liczony będzie od dnia przekazania Protokołu odbioru z zastrzeżeniami na adres mailowy wskazany w § 8 ust. 2 pkt 1 Umowy[8].

7. Strony ustalają, że w przypadku, o którym mowa w ust. 6, zapłata wynagrodzenia zostanie wstrzymana

[5] W przypadku zaoferowania oprogramowania referencyjnego
[6] W przypadku zaoferowania oprogramowania równoważnego
[7] W przypadku zaoferowania oprogramowania referencyjnego
[8] W przypadku zaoferowania oprogramowania równoważnego

do chwili dostarczenia kompletnego Oprogramowania zgodnego z Umową i będzie płatna na podstawie Protokołu odbioru stwierdzającego należyte wykonanie Umowy, bez zastrzeżeń podpisanego przez obydwie strony.

8. Złożenie przez Zamawiającego zastrzeżeń, o których mowa w ust. 6, nie wpływa na przedłużenie ostatecznego terminu dostarczenia Oprogramowania określonego w Umowie.
9. W przypadku stwierdzenia niezgodności Oprogramowania z Umową w toku realizacji zamówienia (np. produkt o innych parametrach niż wymagany), wad dostarczonego Oprogramowania, Zamawiający prześle reklamację na podany przez Wykonawcę w § 8 ust. 2 pkt 1 Umowy adres e-mail nie później niż w terminie 3 (trzech) dni kalendarzowych od dnia, w którym Zamawiający powziął informację o istniejących niezgodnościach. Wykonawca zobowiązuje się rozpatrzyć reklamację najpóźniej w terminie 14 (czternastu) dni roboczych od dnia jej otrzymania i w przypadku jej zasadności dokonać wymiany niezgodnego z Umową Oprogramowania na Oprogramowanie o odpowiednich parametrach, na własny koszt i ryzyko.
10. W przypadku nie usunięcia wad przez Wykonawcę zgodnie z postanowieniami ust. 9 niniejszego paragrafu, Zamawiający ma prawo odstąpić od Umowy w terminie 30 (trzydziestu) dni kalendarzowych od upływu terminu o którym mowa w ust. 9 oraz naliczyć kary umowne o jakich mowa w § 6 ust. 4 Umowy.

§ 4.

Wynagrodzenie i płatności

1. Strony zgodnie ustalają, że z tytułu należytego wykonania Przedmiotu Umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w łącznej kwocie: ……. (słownie: …… /00) złotych netto, powiększone o należny podatek VAT, tj. ……. (słownie: ……) złotych brutto.
2. Strony postanawiają, że kwota wskazana w ust. 1, jest całkowitą kwotą wynagrodzenia należną Wykonawcy z tytułu należytego wykonania Przedmiotu Umowy oraz, że wynagrodzenie pokrywa wszelkie koszty, jakie Wykonawca poniesie w związku z realizacją Przedmiotu Umowy.
3. Zapłata wynagrodzenia, o którym mowa w ust. 1, nastąpi po stwierdzeniu przez Zamawiającego należytego wykonania Przedmiotu Umowy bez zastrzeżeń, w Protokole odbioru, o którym mowa w § 3 ust. 5 Umowy, na podstawie prawidłowo wystawionej i doręczonej Zamawiającemu faktury, w terminie do 30 (trzydziestu) dni kalendarzowych od dnia jej doręczenia Zamawiającemu albo odebrania przez Zamawiającego przesłanej przez Wykonawcę ustrukturyzowanej faktury elektronicznej za pośrednictwem adresu e-mail: ……. lub Platformy Elektronicznego Fakturowania, z zastrzeżeniem art. 4 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2020 poz. 1666 z późn, ze zm.), zawierającej prawidłowy numer rachunku bankowego, znajdujący się w wykazie podatników VAT udostępnianym w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych. Zapłata wynagrodzenia nastąpi na rachunek bankowy wskazany w fakturze

elektronicznej.

4. Brak rachunku bankowego Wykonawcy, znajdującego się w wykazie podatników VAT udostępnianym w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych, uprawnia Zamawiającego do poinformowania o tym fakcie Wykonawcę droga elektroniczną i wstrzymania płatności z faktury do czasu spełnienia wymogów opisanych powyżej, a termin płatności tej faktury ulega wydłużeniu o czas tego opóźnienia. W takim przypadku Wykonawcy nie przysługują odsetki za nieterminową płatność ani uprawnienie do wstrzymania lub braku realizacji obowiązków wynikających z Umowy.
5. W przypadku gdy termin zapłaty za fakturę, w związku z wydłużeniem terminu płatności, o którym mowa w ust. 4 powyżej, przekroczyłby 30 (trzydzieści) dni kalendarzowych, do którego zachowania Zamawiający jest zobowiązany na podstawie art. 8 ust. 2 ustawy o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych z dnia 8 marca 2013 r. (tj. Dz. U.2021 poz. 424 ze zm.), liczonych od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury, Zamawiający zrealizuje płatność na rachunek wskazany przez Wykonawcę i na podstawie art. 117 ab § 1 w związku z § 3 pkt 2 ustawy ordynacja podatkowa z dnia 29 sierpnia 1997 r. (tj. Dz. U. z 2021 poz. 1540) złoży zawiadomienie o zapłacie należności na ten rachunek do naczelnika urzędu skarbowego właściwego dla Wykonawcy w terminie 7 (siedmiu) dni kalendarzowych od dnia zlecenia przelewu oraz poinformuje Wykonawcę drogą elektroniczną o płatności.
6. Wykonawca na fakturze, w której kwota należności ogółem stanowi kwotę, o której mowa w art. 19 pkt 2 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców (t.j. Dz.U. z 2021 r. poz. 162 ze zm.), obejmującą dokonaną na rzecz Zamawiającego dostawę towarów/świadczenie usług, o których mowa w załączniku nr 15 do ustawy o podatku od towarów i usług (t.j. Dz.U. z 2021 r. poz. 685 ze zm.) umieści wyrazy „mechanizm podzielonej płatności" zgodnie z art. 106e ust. 1 pkt 18a ustawy o podatku od towarów i usług.
7. Nieprawidłowo wystawiona faktura nie będzie stanowiła podstawy do zapłaty wynagrodzenia i zostanie zwrócona Wykonawcy. W takim przypadku, termin zapłaty należnego Wykonawcy wynagrodzenia biegnie od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury.
8. Za dzień zapłaty uważa się dzień wydania dyspozycji przelewu z rachunku bankowego Zamawiającego.

§ 5.

Odstąpienie od Umowy

1. Zamawiający może odstąpić od Umowy ze skutkiem na dzień złożenia oświadczenia o odstąpieniu w przypadku gdy zachodzi co najmniej jedna z poniższych okoliczności:
   1) Wykonawca nie wykonuje Umowy lub rażąco narusza postanowienia Umowy – w terminie 30 (trzydziestu) dni kalendarzowych od dnia powzięcia wiadomości o powyższych okolicznościach;
   2) Wykonawca nie dotrzymał terminów, o których mowa w § 3 ust. 1 i 6 Umowy - w terminie 30 (trzydziestu) dni kalendarzowych od bezskutecznego upływu danego terminu;

3) Wykonawca dokonał zmian organizacyjno- prawnych w swoim statusie zagrażających realizacji Umowy lub nie poinformował Zamawiającego o zamiarze dokonania zmian prawno-organizacyjnych, które mogą mieć wpływ na realizację Umowy - w terminie 30 (trzydziestu) dni kalendarzowych od dnia powzięcia wiadomości o powyższych okolicznościach;
4) Wykonawca zaprzestał realizacji Umowy i nie podjął jej w terminie wyznaczonym przez Zamawiającego pomimo wezwania go do tego przez Zamawiającego - w terminie 30 (trzydziestu) dni kalendarzowych od dnia bezskutecznego upływu terminu wyznaczonego w wezwaniu;
5) w celu zawarcia Umowy Wykonawca przedstawił fałszywe oświadczenia lub dokumenty – w terminie 30 (trzydziestu) dni kalendarzowych od dnia powzięcia wiadomości o powyższych okolicznościach;
6) podane przez Wykonawcę w Ofercie informacje nie odpowiadają stanowi faktycznemu – w terminie 30 (trzydziestu) dni kalendarzowych od dnia powzięcia wiadomości o powyższych okolicznościach;
7) wystąpią inne nieprawidłowości w realizacji Umowy, które czynią dalszą realizację Umowy niemożliwą lub niecelową - w terminie 30 (trzydziestu) dni kalendarzowych od dnia powzięcia wiadomości o powyższych okolicznościach;
8) wystąpienia istotnej okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. Odstąpienie od Umowy w tym wypadku może nastąpić w terminie 30 (trzydziestu) dni kalendarzowych od powzięcia wiadomości o tych okolicznościach, zgodnie z art. 456 ust. 1 pkt. 1) pzp;
9) jeżeli zachodzi co najmniej jedna z następujących okoliczności:
   a) dokonano zmiany umowy z naruszeniem art. 454 i art. 455 pzp;
   b) Wykonawca w chwili zawarcia Umowy podlegał wykluczeniu na podstawie art. 108 pzp;
   c) Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.

2. W przypadku odstąpienia od Umowy przez Zamawiającego, Wykonawca może żądać od Zamawiającego wyłącznie wynagrodzenia z tytułu należytego wykonania części Umowy do momentu złożenia przez Zamawiającego oświadczenia o odstąpieniu od Umowy. Pomimo odstąpienia od Umowy, Zamawiający zachowuje prawa do rezultatu świadczenia zrealizowanego przez Wykonawcę na podstawie Umowy do momentu złożenia przez Zamawiającego oświadczenia o odstąpieniu od Umowy. W przypadku ewentualnych wątpliwości, po ustaniu obowiązywania Umowy w związku z odstąpieniem, Strony zgodnie podejmą działania, celem ustalenia zakresu świadczenia zrealizowanego przez Wykonawcę na podstawie Umowy do momentu złożenia przez Zamawiającego

oświadczenia o odstąpieniu od Umowy oraz wysokości wynagrodzenia przysługującego Wykonawcy w powyższym zakresie.

3. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności.
4. Odstąpienie od Umowy nie powoduje odpowiedzialności odszkodowawczej Zamawiającego w związku ze skróceniem okresu obowiązywania Umowy.

§ 6.

Kary umowne

1. W razie niewykonania Przedmiotu Umowy lub jego części, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 10 % wynagrodzenia brutto, określonego w § 4 ust. 1 Umowy.
2. Za każdy rozpoczęty dzień zwłoki w terminie dostawy Oprogramowania, ewentualnego wdrożenia Oprogramowania Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 1 % wynagrodzenia brutto, wskazanego w § 4 ust. 1 Umowy.
3. Z tytułu niezachowania pozostałych terminów wynikających z Umowy, w tym z SOPZ, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 0,5 % wynagrodzenia brutto, określonego w § 4 ust. 1 Umowy, za każdy rozpoczęty dzień zwłoki.
4. W razie odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 10 % wynagrodzenia brutto, określonego w § 4 ust. 1 Umowy.
5. Za każdy inny przypadek nienależytego wykonania Przedmiotu Umowy, niż określony w ust. 2 i 3, Zamawiający ma prawo do naliczenia Wykonawcy kary umownej w wysokości 2 % wynagrodzenia brutto, określonego w § 4 ust. 1 Umowy.
6. Za nienależyte wykonanie Przedmiotu Umowy należy uznać w szczególności:
   1) dostarczenie Oprogramowania w niewłaściwej ilości;
   2) wykonanie Przedmiotu Umowy z naruszeniem postanowień Umowy, w tym SOPZ i Oferty.
7. Wykonawca wyraża zgodę na potrącanie naliczonych kar umownych przez Zamawiającego, z kwoty przysługującego mu wynagrodzenia brutto, o którym mowa w § 4 ust. 1 Umowy, choćby którakolwiek z wierzytelności przedstawionych do potrącenia przez Zamawiającego była niewymagalna lub niezaskarżalna. W przypadku braku pokrycia nałożonych kar umownych w kwotach pozostałych do zapłaty, Wykonawca zobowiązuje się do uregulowania kary w terminie 14 (czternastu) dni kalendarzowych od dnia doręczenia Wykonawcy noty obciążeniowej w formie pisemnej.
8. Zapłata kar umownych nie zwalnia Wykonawcy od obowiązku wykonania Umowy.
9. Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych, aż do wysokości poniesionej szkody, na zasadach ogólnych.
10. Łączna wartość kar umownych nałożonych na wykonawcę nie może przekroczyć 20 % wynagrodzenia, o którym mowa w § 4. ust. 1.

§ 7.

Informacje poufne

1. Wykonawca zobowiązuje się zachować w poufności wszelkie informacje techniczne, technologiczne, ekonomiczne, finansowe, handlowe, prawne, organizacyjne, informacje dotyczące stosowanych systemów informatycznych w tym systemów bezpieczeństwa i inne dotyczące drugiej Strony posiadające ekonomiczną/gospodarczą wartość, które nie są powszechnie znane, uzyskane w związku z realizacją Umowy, wyrażone za pomocą mowy, pisma, obrazu, rysunku, znaku, dźwięku albo zawarte w urządzeniu, przyrządzie lub innym przedmiocie, a także wyrażone w jakikolwiek inny sposób (dalej jako: **„Informacje”**).
2. Wykonawca zobowiązuje się nie kopiować, nie powielać, ani w jakikolwiek inny sposób rozpowszechniać Informacji lub ich części, za wyjątkiem przypadków, gdy jest to konieczne do realizacji celów ściśle związanych ze współpracą Stron wynikającą z postanowień Umowy oraz przypadków określonych w ust. 3-5. Wykonawca zobowiązuje się również do zastosowania właściwych środków w celu ochrony Informacji i ich zabezpieczenia przed ujawnieniem nieupoważnionym osobom trzecim, przed ich utratą, kradzieżą i innym nieuprawnionym dostępem.
3. Wymogi zawarte w niniejszym paragrafie nie będą miały zastosowania odnośnie Informacji:
   a) opublikowanych lub podanych do publicznej wiadomości, bez naruszenia obowiązków wynikających z Umowy,
   b) otrzymanych przez Wykonawcę, zgodnie z przepisami prawa powszechnie obowiązującego, bez obowiązku zachowania poufności,
   c) znanych Wykonawcy, bez obowiązku zachowania poufności, w momencie ich przekazania przez Zamawiającego,
   d) co do których Wykonawca uzyskał uprzednią zgodę Zamawiającego na ich ujawnienie, wyrażoną w formie pisemnej pod rygorem nieważności.
4. W przypadku skierowania przez uprawniony organ żądania ujawnienia Informacji, Wykonawca, dokona natychmiastowego powiadomienia Zamawiającego o wystąpieniu takiego żądania i jego okolicznościach towarzyszących.
5. Powyższe nie dotyczy ujawniania Informacji pracownikom Wykonawcy, jego pełnomocnikom oraz osobom bezpośrednio związanym z realizacją Umowy, którym ujawnienie Informacji będzie niezbędne do prawidłowego wykonania Przedmiotu Umowy oraz przypadków, gdy ujawnienie Informacji będzie wymagane przez przepisy prawa.
6. Wykonawca zobowiązuje się do poinformowania osób, przy pomocy których wykonuje Umowę i które będą miały dostęp do Informacji, o wynikających z Umowy obowiązkach w zakresie zachowania poufności, a także do skutecznego zobowiązania i egzekwowania od tych osób obowiązków w zakresie zachowania poufności.
7. Wykonawca ponosi odpowiedzialność za przestrzeganie postanowień niniejszego paragrafu przez wszystkie osoby, którymi posługuje się przy wykonywaniu Umowy jak za własne działania lub zaniechania.
8. Informacje otrzymane od Zamawiającego Wykonawca zobowiązuje się wykorzystywać wyłącznie w celu realizacji Umowy.

9. W przypadku naruszenia przez Wykonawcę obowiązków dotyczących Informacji, w tym danych osobowych, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości ……. PLN (słownie: ……) za każdy przypadek naruszenia. Wykonawca zobowiązuje się do uregulowania kary w terminie 14 (słownie: czternastu) dni kalendarzowych od dnia doręczenia Wykonawcy wezwania do zapłaty/noty obciążeniowej. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych Kodeksu cywilnego.
10. Zobowiązanie określone w niniejszym paragrafie pozostaje w mocy przez cały okres obowiązywania Umowy, jak również przez okres ..... (słownie: ……) lat po zakończeniu Umowy, niezależnie od przyczyny (wykonanie, wygaśnięcie, rozwiązanie, odstąpienie, wypowiedzenie Umowy) chyba, że przepisy powszechnie obowiązującego prawa przewidują dłuższy okres ochrony.

§ 8.

Osoby do kontaktów i ochrona danych osobowych

1. Strony postanawiają, że do kontaktów pomiędzy Stronami oraz do podejmowania bieżących uzgodnień związanych z realizacją Umowy wyznaczeni są:
   1) ze strony Wykonawcy:
      a) ....., tel.:....., e-mail: .....;
      b) ....., tel.:....., e-mail: .....
   2) ze strony Zamawiającego:
      a) ....., tel.:....., e-mail: .....;
      b) ....., tel.:....., e-mail: .....
2. Osobą uprawnioną do podpisania Protokołu odbioru jest:
   1) ze strony Wykonawcy:
      a) ....., tel.:....., e-mail: .....;
      b) ....., tel.:....., e-mail: .....
   2) ze strony Zamawiającego:
      a) ....., tel.:....., e-mail: .....;
      b) ....., tel.:....., e-mail: .....
3. Zmiana danych, o których mowa w ust. 1 i 2, wymaga poinformowania drugiej Strony w formie elektronicznej na adres wskazany w § 8. ust. 1 Umowy . Zmiana taka nie stanowi zmian postanowień Umowy w rozumieniu § 11 ust. 1.
4. Uznaje się, iż dotarcie informacji do osób wskazanych w ust. 1, jest poinformowaniem Stron Umowy.
5. Strony oświadczają, że przetwarzanie w zakresie udostępnionych im przez drugą Stronę Umowy danych osobowych dokonywane będzie przez każdą ze Stron, jako administratora danych osobowych w celu realizacji Przedmiotu Umowy.
6. Dane osobowe przedstawicieli Stron, w tym wymienionych w § 8 ust. 1 i 2 Umowy udostępniane będą drugiej Stronie, która stanie się ich administratorem danych i przetwarzane będą przez nią w celu realizacji Umowy.

7. Zamawiający podaje, iż wszelkie informacje dotyczące przetwarzania danych osobowych przez Zamawiającego jako Administratora Danych Osobowych znajdują się w Klauzuli informacyjnej o której mowa w art. 13 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm., dalej RODO), która stanowi Załącznik nr 6 do Umowy.
8. W przypadku, gdy Zamawiający będzie przetwarzał w ramach niniejszej Umowy dane pracowników lub współpracowników Wykonawcy oraz podwykonawców, Zamawiający realizuje obowiązek informacyjny, o którym mowa w art. 14 RODO, poprzez Klauzulę stanowiącą Załącznik nr 7 i zobowiązuje drugą stronę Umowy do udostępnienia tejże informacji wskazanym osobom.
9. Zmiana załączników wskazanych w ust. 7 i 8 powyżej nie wymaga zmiany Umowy, Strony mogą aktualizować dane zawarte w powyżej wskazanych Klauzulach informacyjnych w formie dokumentowej.

§ 9.

Okres obowiązywania Umowy

Umowa zostaje zawarta na czas oznaczony, to jest od dnia jej zawarcia do dnia 25 maja 2025 r.

§ 10.

Klauzula salwatoryjna

1. W przypadku stwierdzenia, że którekolwiek z postanowień Umowy jest z mocy prawa nieważne lub bezskuteczne, okoliczność ta nie będzie miała wpływu na ważność, skuteczność lub możliwość wyegzekwowania pozostałych postanowień, chyba że z okoliczności wynikać będzie w sposób oczywisty, że bez postanowień nieważnych lub bezskutecznych, Umowa nie zostałaby zawarta.
2. W sytuacji, o której mowa w ust. 1, Strony zobowiązują się zawrzeć aneks do Umowy, w którym sformułują postanowienia zastępcze, których cel gospodarczy i ekonomiczny będzie równoważny lub maksymalnie zbliżony do celu postanowień nieważnych lub bezskutecznych.
3. W przypadku nieosiągnięcia porozumienia do treści postanowień zastępczych zastosowanie będą miały przepisy kodeksu cywilnego.

§ 11.

Zmiany Umowy

1. Z zastrzeżeniem wyjątków wskazanych w Umowie, zmiana treści Umowy wymaga zachowania formy pisemnej pod rygorem nieważności i musi być zgodna z art. 455 ustawy pzp.
2. Umowa może zostać zmieniona w sytuacji gdy:
   1) zaistnieją okoliczności związane z wystąpieniem wirusa SARS-CoV-2, które wpływają lub mogą wpłynąć na należyte wykonanie Umowy;
   2) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy;

3) wynikną rozbieżności lub niejasności w Umowie, których nie można usunąć w inny sposób, a zmiana Umowy będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej postanowień przez Strony;
4) zaistnieje konieczność wprowadzenia zmiany terminu realizacji Przedmiotu Umowy;
5) zaistnieje działanie siły wyższej rozumianej jako nadzwyczajne okoliczności niezależne od Stron, których nie można było przewidzieć, jak m.in.: wojna, stany wyjątkowe, strajki generalne, blokady, embargo, działania sił przyrody o charakterze klęsk żywiołowych jak huragany, powodzie, trzęsienia ziemi, pożary, epidemie, pandemie itp., uniemożliwiającej realizację w części lub w całości Przedmiotu Umowy;
6) wystąpią uzasadnione zmiany w zakresie sposobu realizacji, w tym zmiana miejsca lub terminu realizacji Przedmiotu Umowy;
7) nastąpi konieczność zmiany warunków i terminów płatności.

3. Strony mają prawo do przedłużenia terminu zakończenia wykonywania Przedmiotu Umowy o okres trwania przyczyn, z powodu których nie była możliwa realizacja Przedmiotu Umowy, w następujących sytuacjach:
   1) wystąpią opóźnienia w dokonaniu określonych czynności lub ich zaniechanie przez właściwe organy administracji państwowej, które nie są następstwem okoliczności, za które Wykonawca ponosi odpowiedzialność,
   2) gdy wystąpią opóźnienia w wydawaniu decyzji, zezwoleń, uzgodnień, itp., do wydania których właściwe organy są zobowiązane na mocy przepisów prawa, jeżeli opóźnienie przekroczy okres, przewidziany w przepisach prawa, w którym ww. decyzje powinny zostać wydane oraz nie są następstwem okoliczności, za które Wykonawca ponosi odpowiedzialność,
   3) wystąpienia zdarzeń natury siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy zgodnie z jej postanowieniami.
4. Strony są uprawnione do zmiany Umowy w zakresie materiałów, parametrów technicznych, technologii, sposobu i zakresu wykonania Przedmiotu Umowy, bez zmiany wysokości wynagrodzenia należnego Wykonawcy, w następujących sytuacjach:
   1) konieczności zrealizowania jakiejkolwiek części Przedmiotu Umowy, przy zastosowaniu odmiennych rozwiązań technicznych lub technologicznych, niż wskazane w opisie przedmiotu zamówienia, a wynikających ze stwierdzonych wad opisu przedmiotu zamówienia, zmiany stanu prawnego w oparciu, o który je przygotowano, gdyby zastosowanie przewidzianych rozwiązań groziło niewykonaniem lub nienależytym wykonaniem Przedmiotu Umowy,
   2) konieczności zrealizowania Przedmiotu Umowy przy zastosowaniu innych rozwiązań technicznych lub materiałowych ze względu na zmiany obowiązującego prawa,
   3) wystąpienia siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy zgodnie z jej postanowieniami.
5. Wszelkie zmiany, o których mowa powyżej, nie mogą spowodować zwiększenia całkowitej wartości wynagrodzenia brutto wskazanego w § 4 ust. 1 Umowy.

6. Z zastrzeżeniem wyjątków wskazanych w Umowie, wszelkie zmiany Umowy są dokonywane przez umocowanych przedstawicieli Zamawiającego i Wykonawcy w formie pisemnej w drodze aneksu do Umowy, pod rygorem nieważności.
7. W razie wątpliwości, przyjmuje się, że nie stanowią zmiany Umowy następujące zmiany:
   1) danych związanych z obsługą administracyjno-organizacyjną Umowy,
   2) danych teleadresowych,
   3) danych rejestrowych,
   4) będące następstwem sukcesji uniwersalnej po jednej ze stron Umowy,
   5) w zakresie zmiany treści załączników nr 6 i 7 do Umowy.
8. Zamawiający dopuszcza zmianę postanowień Umowy w stosunku do treści Oferty w sytuacji, gdy nie była możliwa do przewidzenia na etapie zawarcia Umowy, a ponadto jej dokonanie podyktowane jest zmianą stanu prawnego w zakresie mającym wpływ na realizację Umowy, tj. w szczególności zmianą:
   1) stawki podatku od towarów i usług oraz podatku akcyzowego;
   2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (t.j. Dz.U. z 2020 r. poz. 2207);
   3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne;
   4) zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (t.j. Dz. U. z 2020 r. poz. 1342)

   - jeżeli zmiany te będą miały wpływ na koszty wykonania Przedmiotu Umowy przez Wykonawcę. Każda ze Stron Umowy, w terminie 30 (trzydziestu) dni kalendarzowych od dnia wejścia w życie przepisów dokonujących tych zmian, może zwrócić się do drugiej Strony o przeprowadzenie negocjacji w sprawie odpowiedniej zmiany wysokości wynagrodzenia.

§ 12.

Podwykonawcy

1. Wykonawca może powierzyć wykonanie części Przedmiotu Umowy innemu podmiotowi wyłącznie na zasadach opisanych w niniejszym paragrafie.
2. Wykonawca powierza realizację części Przedmiot Umowy następującym podwykonawcom:
   1) [wskazanie firmy, danych kontaktowych, osób reprezentujących podwykonawcę] _____ - w zakresie _____,
   2) [wskazanie firmy, danych kontaktowych, osób reprezentujących podwykonawcę] _____ - w zakresie _____,
3. Wykonawca zobowiązany jest do poinformowania Zamawiającego w formie pisemnej lub za pomocą poczty elektronicznej, na adres wskazany w § 8 ust. 1 pkt 2 Umowy, o każdej zmianie danych dotyczących podwykonawców, jak również o ewentualnych nowych podwykonawcach, którym zamierza powierzyć prace w ramach realizacji Umowy.

4. Informacja o zmianie danych dotyczących podwykonawców powinna zostać przekazana Zamawiającemu w terminie 5 (pięciu) dni kalendarzowych od daty zmiany danych, w celu zachowania niezakłóconej współpracy.
5. Informacja o zamiarze powierzenia prac nowemu podwykonawcy powinna zostać przekazana Zamawiającemu nie później niż na 2 (dwa) dni kalendarzowe przed planowanym powierzeniem mu realizacji prac. Wykonawca zobowiązany jest do uzyskania uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności na powierzenie prac nowemu podwykonawcy lub nowym podwykonawcom.
6. W przypadku niewykonania zobowiązania, o którym mowa w ust. 3 - 5 powyżej, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 1.000,00 (jeden tysiąc) złotych za każdy dzień zwłoki w przekazaniu informacji.
7. Wykonawca zapewnia, że podwykonawcy, z których świadczeń będzie korzystał w trakcie wykonywania niniejszej Umowy będą podmiotami profesjonalnie świadczącymi zlecone im przez Wykonawcę zadania oraz posiadającymi wszelkie niezbędne kwalifikacje do wykonywania zleconych im przez Wykonawcę zadań.
8. Korzystając w ramach wykonywania niniejszej Umowy ze świadczeń podwykonawców, Wykonawca zobowiązany jest nałożyć na takiego podwykonawcę obowiązek przestrzegania wszelkich zasad, reguł i zobowiązań określonych w Umowie, w zakresie, w jakim odnosić się one będą do zakresu prac danego podwykonawcy.
9. Wykonawca pozostaje gwarantem wykonywania i przestrzegania przez podwykonawców wszelkich zasad, reguł i zobowiązań określonych w Umowie.
10. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ust. 1 ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.
11. Zmiany, o których mowa w niniejszym paragrafie nie wymagają dokonywania zmiany Umowy w formie aneksu.
12. Powierzenie wykonania części Przedmiotu Umowy podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie Umowy. Wykonawca w pełni i wyłącznie odpowiada za działania lub zaniechania podwykonawców jak za własne działania lub zaniechania.
13. Korzystanie ze świadczeń podwykonawców niezgodnie z postanowieniami niniejszego paragrafu traktowane będzie jako istotne naruszenie warunków Umowy oraz może stanowić przyczynę odstąpienia od Umowy przez Zamawiającego w terminie 30 (trzydziestu) dni kalendarzowych od powzięcia wiadomości o naruszeniu przez Wykonawcę postanowień niniejszego paragrafu.

§ 13.

Postanowienia końcowe

1. Prawa i obowiązki Wykonawcy wynikające z Umowy oraz wierzytelności wobec Zamawiającego nie mogą być przenoszone na osoby trzecie bez uprzedniej zgody Zamawiającego, wyrażonej na piśmie, pod rygorem nieważności.
2. Wszelkie spory wynikłe w związku z realizacją Umowy Strony będą się starały rozwiązać polubownie. W przypadku braku możliwości osiągnięcia przez Strony konsensusu w sposób wskazany w zdaniu poprzedzającym, spory te będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych Umową mają zastosowanie powszechnie obowiązujące przepisy prawa polskiego, w tym w szczególności pzp. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla NCBR jeden dla Wykonawcy. Jeśli Umowa zawierana będzie zgodnie z art. 78^1 k.c. – każda ze Stron jest uprawniona do druku dowolnej liczby egzemplarzy Umowy.
4. Wykonawca zwalnia Zamawiającego od wszelkiej odpowiedzialności w przypadku jakichkolwiek roszczeń osób trzecich dotyczących Przedmiotu Umowy.
5. Umowa zostaje zawarta z dniem podpisania jej przez ostatnią ze Stron.
6. Integralną część Umowy stanowią następujące załączniki:
   1) **Załącznik nr 1** – kopia upoważnienia do reprezentowania Zamawiającego;
   2) **Załącznik nr 2** – wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Wykonawcy, kopia dokumentu, który upoważnia przedstawiciela Wykonawcy do zawarcia Umowy;
   3) **Załącznik nr 3** - SOPZ;
   4) **Załącznik nr 4** - Oferta Wykonawcy;
   5) **Załącznik nr 5** – wzór Protokołu odbioru;
   6) **Załącznik nr 6 –** klauzula informacyjna z art. 13 RODO;
   7) **Załącznik nr 7** – klauzula informacyjna z art. 14 RODO.

…….…….. ……..

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 3

Szczegółowy opis przedmiotu zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) odnowienie usługi wsparcia technicznego producenta dla McAfee Complete EndPoint Protection – Business – w ilości 900 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy;
2) dostawa licencji McAfee Complete EndPoint Protection – Business – w ilości 150 szt. ważnych od dnia 26 maja 2022 r. przez czas nieoznaczony wraz z usługą wsparcia technicznego producenta na okres 36 miesięcy;
3) odnowienie subskrypcji McAfee MVISION TIE – w ilości 800 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
4) dostawa subskrypcji McAfee MVISION TIE – w ilości 100 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
5) odnowienie subskrypcji McAfee Virtual Advanced Threat Defence Appliance – w ilości 1 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy,

lub dostawa rozwiązania równoważnego.

II. Opis rozwiązania równoważnego

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 2021 r., poz. 1129 ze zm.).
2) Zaoferowane rozwiązanie równoważne musi spełniać następujące kryteria minimalne:

1. Wymagania ogólne:

Lp.	Konfiguracja minimalna
1.	Rozwiązanie musi wspierać, co najmniej następującą platformę wirtualizacyjną (jeżeli zostanie dostarczony w postaci maszyn wirtualnych): VMware.
2.	Rozwiązanie musi 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) Rozwiązanie musi wspierać następujące serwerowe systemy operacyjne: a) Windows Server 2012/2012 R2 b) Windows Server 2016/2016 R2 c) Windows Server 2019
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.	Rozwiązanie musi umożliwiać uruchomienie serwera do obsługi stacji roboczych znajdujących się poza siecią lokalną Zamawiającego. Serwer taki musi być przystosowany do pracy w DMZ.
6.	Zaproponowane rozwiązanie 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 rozwiązania muszą komunikować się między sobą w bezpieczny sposób (transmisja pomiędzy maszynami musi być szyfrowana).

2. 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 musi 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,
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.

3. 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.

4. Oprogramowanie do ochrony stacji końcowych przed zagrożeniami (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) musi być możliwa poprzez instalację ręczną oraz instalację automatyczną z użyciem konsoli zarządzającej lub zewnętrznego oprogramowania wymagającego plików MSI.

3.	Oprogramowanie OOPZ musi umożliwić pracę w środowiskach całkowicie izolowanych, gdzie nie ma dostępu do Internetu. Musi 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. Muszą 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 musi posiadać wbudowane reguły realizujące ochronę kluczowych obszarów stacji roboczej, d) w ramach ochrony przed modyfikacją systemu operacyjnego, musi 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. 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.).

5. 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 2012/2012R2, Windows Server 2016/2016R2, Windows Server 2019, 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.

6. Funkcjonalności ogólne:

Lp.	Funkcjonalności ogólne:
1.	**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 musi 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 Server 2012, Windows Server 2012 R2, Windows Server 2016/2016 R2, Windows Server 2019) 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 rozwiązania 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 5

PROTOKÓŁ ODBIORU OSTATECZNY / CZĘŚCIOWY*

Zamawiający: ……..…….

Reprezentowany przez ……

Wykonawca: ……..

Przedmiot odbioru: ……

Data dokonania odbioru: ……

Zakres wykonanych prac:……..…

……..……

……

Przedstawiciele **zamawiającego**:

1. ……
2. ……
3. ……

Przedstawiciele **wykonawcy**:

1. ……
2. ……
3. ……

W wyniku czynności odbioru **zamawiający** oraz **wykonawca** stwierdzają, co następuje:

1. Zakres prac został wykonany zgodnie/niezgodnie* z umową/zleceniem*

   nr …… z dnia ……

2. Prace zostały rozpoczęte dnia ……. i zakończone dnia ……

   Termin wykonania umowy został dotrzymany.

3. Jakość wykonanych prac ocenia się jako dobrą/niedobrą*

4. Niezgodności/braki ……..……

……

5. Termin usunięcia niezgodności/braków ustalono na ……

6. Uwagi komisji ……..……

……

7. Zakres prac został przyjęty/nieprzyjęty* na skutek ……

……

Podpisy/zatwierdzenie/akceptacja zgodnie z zapisami w umowie

Przedstawiciele **zamawiającego**:	Przedstawiciele **wykonawcy**:
1. ……	1. ……
2. ……	2. ……
3. ……	3. ……

*niepotrzebne skreślić

Załącznik nr 6

Klauzula informacyjna – przedstawiana w przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą

Zgodnie z art. 13 ust. 1 i ust. 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 (dalej „RODO"), informuję Panią/Pana że:

1) administratorem danych osobowych jest Narodowe Centrum Badań i Rozwoju (dalej: „NCBR") z siedzibą w Warszawa 00-695, Nowogrodzka 47a;

2) z inspektorem ochrony danych można się skontaktować poprzez adres e-mail: iod@ncbr.gov.pl;

3) dane osobowe są przetwarzane w celu zawarcia i realizacji Umowy nr…… pomiędzy NCBR a ……

4) dane osobowe są przetwarzane z uwagi na zawartą powyżej umowę, a przetwarzanie jest niezbędne do wykonania Umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem Umowy (art. 6 ust. 1 lit. b RODO);

5) dane osobowe będą przetwarzane w okresie realizacji Umowy – do czasu wykonania wszystkich obowiązków i ewentualnych roszczeń wynikających z Umowy oraz przechowywane będą w celach archiwalnych przez okres przechowywania zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;

7) odbiorcami danych osobowych będą organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa, a także podmioty świadczące usługi niezbędne do realizacji zadań przez NCBR, w szczególności takim podmiotem jest NCBR+ sp. z o.o. Dane te mogą być także przekazywane partnerom IT, podmiotom realizującym wsparcie techniczne lub organizacyjne;

8) przysługują Pani/Panu prawa w stosunku do NCBR do: żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także do przenoszenia dotyczących Pani/Pana danych osobowych. W sprawie realizacji praw można kontaktować się z inspektorem ochrony danych pod adresem mailowym udostępnionym w pkt 2 powyżej;

9) posiada Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych lub do innego organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia;

11) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego;

12) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 7

Klauzula informacyjna – przedstawiana w przypadku zbierania danych osobowych niebezpośrednio od osoby, której dane dotyczą

Zgodnie z art. 14 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego 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, dalej „RODO"), informuję Panią/Pana, że:

1) administratorem danych osobowych jest Narodowe Centrum Badań i Rozwoju (dalej „NCBR") z siedzibą w Warszawa 00-695, Nowogrodzka 47a;
2) dane osobowe zostały pozyskane od .....
3) z inspektorem ochrony danych (IOD) można się skontaktować poprzez adres e-mail: iod@ncbr.gov.pl;
4) NCBR będzie przetwarzało następujące kategorie Pani/Pana danych osobowych: imię, nazwisko, adres e-mail, numer telefonu, miejsce zatrudnienia, stanowisko;
5) dane osobowe są przetwarzane w celu zawarcia i realizacji Umowy nr…….. pomiędzy NCBR a .....
6) dane osobowe są przetwarzane z uwagi na zawartą powyżej umowę do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f RODO);
7) dane osobowe będą przetwarzane w okresie realizacji Umowy – do czasu wykonania wszystkich obowiązków oraz ewentualnych roszczeń wynikających z niej oraz przechowywane będą w celach archiwalnych przez okres przechowywania zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;
8) odbiorcami danych osobowych będą organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa, a także podmioty świadczące usługi niezbędne do realizacji zadań przez NCBR, w szczególności takim pomiotem jest NCBR+ sp. z o.o. Dane te mogą być także przekazywane partnerom IT, podmiotom realizującym wsparcie techniczne lub organizacyjne;
9) przysługują Pani/Panu prawa w stosunku do NCBR do: żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także do wniesienia sprzeciwu wobec przetwarzania dotyczących Pani/Pana danych osobowych. W sprawie realizacji praw można kontaktować się z inspektorem ochrony danych pod adresem mailowym udostępnionym w pkt 3 powyżej;
10) posiada Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych lub do innego organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia;
11) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego;
12) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.