Załącznik Nr 6 do SIWZ

Wzór: UMOWA NR ……/……..

(zwana dalej: „Umową")

zawarta w dniu ....……..…… roku 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 2019 r. poz. 310, ze zm.), zwanym dalej „**Zamawiającym**", reprezentowanym przez:

Pana/Panią – ....., działającą/-ego na podstawie upoważnienia nr …… r.,

(kopia upoważnienia stanowi Załącznik nr 1 do Umowy),

a

……. zamieszkałą/ zamieszkałym w…… (…-…), przy ul. …….., posiadającą/ posiadającym nr PESEL: ……., legitymującą/legitymującym się dowodem osobistym serii: …. numer ….., wydanym przez: ……., ważnym do: ……, prowadzącą/prowadzącym działalność gospodarczą pod firmą „……", przy ul. …….., posiadającą/posiadającym NIP: …….. oraz REGON: ……..., zwaną/zwanym dalej „**Wykonawcą",**

lub

…… z siedzibą w ……, adres: ul. ……..., …-…., …… wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy w ……., …. Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: ……, posiadającą NIP: ……. oraz REGON: ……,

kapitał zakładowy w wysokości: ……., opłacony w całości, zwaną dalej „**Wykonawcą**”,
reprezentowaną przez: …….

(wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Wykonawcy stanowi Załącznik nr 2 do Umowy)

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

*Umowa została zawarta w wyniku postępowania o udzielenie zamówienia publicznego, przeprowadzonego w trybie przetargu nieograniczonego w związku z art. 6a ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. 2019 r. poz. 1843, ze zm.), dalej: „**pzp**”.*

Osoba upoważniona przez Zamawiającego zapewnia, że udzielone mu/jej upoważnienie nie wygasło, ani nie zostały odwołane a jego treść nie uległa zmianie.

§ 1

1. Przedmiotem Umowy jest:

1) zakup i dostarczenie licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT, składających się z:
   1. odnowienia licencji pakietu McAfee Complete Data Protection Advanced lub oprogramowania równoważnego – w ilości 600 (sześciuset) szt. ważnych od dnia 15.12.2019 roku do dnia 25.05.2021 roku;
   2. odnowienia licencji pakietu McAfee Threat Intelligence Exchange lub oprogramowania równoważnego – w ilości 600 (sześciuset) szt. ważnych od dnia 15.12.2019 roku do dnia 25.05.2021 roku;
   3. odnowienia licencji pakietu McAfee Threat Complete EndPoint Protection Enterprise lub oprogramowania równoważnego – w ilości 600 (sześciuset) szt. ważnych od dnia 15.12.2019 roku do dnia 25.05.2021 roku;
   4. odnowienia licencji McAfee Virtual Advanced Threat Defence Appliance lub oprogramowania równoważnego – w ilości 1 (jednej) szt. ważnej od dnia 15.12.2019 roku do dnia 25.05.2021 roku;

5. odnowienia licencji pakietu McAfee Complete Data Protection Advanced lub oprogramowania równoważnego – w ilości 100 (stu) szt. ważnych od dnia 26.05.2020 roku do dnia 25.05.2021 roku;
6. odnowienia licencji pakietu McAfee Threat Intelligence Exchange lub oprogramowania równoważnego – w ilości 100 (stu) szt. ważnych od dnia 26.05.2020 roku do dnia 25.05.2021 roku;
7. odnowienia licencji pakietu McAfee Threat Complete EndPoint Protection Enterprise lub oprogramowania równoważnego – w ilości 100 (stu) szt., ważnych od dnia 26.05.2020 roku do dnia 25.05.2021 roku;
8. licencji pakietu McAfee Complete Data Protection Advanced lub oprogramowania równoważnego – w ilości dodatkowych 100 (stu) szt. ważnych od dnia wdrożenia przez Zamawiającego do dnia 25.05.2021 roku;
9. licencji pakietu McAfee Threat Intelligence Exchange lub oprogramowania równoważnego – w ilości dodatkowych 100 (stu) szt. ważnych od dnia wdrożenia przez Zamawiającego do dnia 25.05.2021 roku;
10. licencji pakietu McAfee Threat Complete EndPoint Protection Enterprise lub oprogramowania równoważnego – w ilości dodatkowych 200 (dwustu) szt. ważnych od dnia wdrożenia przez Zamawiającego do dnia 25.05.2021 roku;

    dalej łącznie jako „**Oprogramowanie**” oraz bieżąca aktualizacja Oprogramowania przez cały okres obowiązywania licencji na Oprogramowanie;

2) przeprowadzenie wdrożenia przez Wykonawcę – w tym migracji danych z systemu posiadanego przez Zamawiającego do nowego Oprogramowania, w siedzibie Zamawiającego przy ul. Nowogrodzkiej 47A w Warszawie, w terminie wskazanym w ofercie Wykonawcy, w godzinach ustalonych przez Strony w drodze bieżących ustaleń przedstawicieli Stron wskazanych w §11 ust. 1 Umowy, nie później jednak niż do 7 (siedmiu) dni kalendarzowych od dnia zawarcia Umowy.[1]

2. Szczegółowy opis Przedmiotu Umowy, ilość Oprogramowania, terminy i pozostałe wymagania Zamawiającego w zakresie wykonania Przedmiotu Umowy zawiera Szczegółowy Opis Przedmiotu Zamówienia, stanowiący Załącznik nr 3 do Umowy (dalej jako: „**SOPZ**”) oraz oferta Wykonawcy z dnia ....., stanowiąca Załącznik nr 4 do Umowy (dalej jako: „**Oferta**”).

[1] W przypadku dostarczenia rozwiązania równoważnego.

§ 2

1. Wykonawca zobowiązuje się do:

1) wykonania Przedmiotu Umowy zgodnie z SOPZ i Ofertą;

2) wykonania Przedmiotu Umowy zgodnie ze swoją najlepszą wiedzą oraz zgodnie z obowiązującymi przepisami prawa polskiego i unijnego;

3) wykonania Przedmiotu Umowy z zachowaniem należytej staranności wynikającej z zawodowego charakteru prowadzonej działalności;

4) zapewnienia profesjonalnego standardu wykonania Przedmiotu Umowy.

2. Wykonawca oświadcza, że:

1) posiada odpowiednie środki, uprawnienia, umiejętności i kwalifikacje niezbędne do należytego wykonania Umowy;

2) nie są mu znane żadne przeszkody natury technicznej, prawnej ani finansowej, które mogą uniemożliwić bądź utrudnić zawarcie Umowy lub wykonanie obowiązków wynikających z Umowy;

3) ponosi pełną i wyłączną odpowiedzialność za prawidłową realizację Przedmiotu Umowy.

§ 3

1. Oprogramowanie zostanie dostarczone na koszt i ryzyko Wykonawcy w terminie 7 (siedmiu) dni kalendarzowych od zawarcia Umowy. Dostarczenie Oprogramowania polega na udostępnieniu przez Wykonawcę Zamawiającemu kluczy do Oprogramowania obejmującego licencje objęte Umową za pośrednictwem poczty elektronicznej, wysyłając maila na adres licencje@ncbr.gov.pl.

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 jakichkolwiek wad prawnych oraz zgodne z wymogami określonymi w SOPZ.

5. Z czynności odbioru Oprogramowania i ewentualnego wdrożenia Oprogramowania[2], w terminie do 3 (trzech) dni od dnia dostarczenia Oprogramowania lub ewentualnego wdrożenia Oprogramowania[3], 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 § 11 ust. 2 pkt 1 Umowy.
6. W przypadku stwierdzenia w Protokole odbioru braków, 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 § 11 ust. 2 pkt. 1 Umowy.
7. Strony ustalają, że w przypadku, o którym mowa w ust. 6, zapłata wynagrodzenia zostanie wstrzymana do chwili dostarczenia kompletnego Oprogramowania zgodnego z Umową i będzie płatna na podstawie Protokołu odbioru stwierdzającego należyte wykonanie Umowy, bez zastrzeżeń.
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 (np. produkt o innych parametrach niż wymagany), wad dostarczonego Oprogramowania już po podpisaniu Protokołu odbioru, Zamawiający prześle reklamację na podany przez Wykonawcę w § 11 ust. 1 pkt 1 Umowy adres e-mail nie później niż w terminie 7 (siedmiu) dni kalendarzowych od dnia, w którym Zamawiający powziął informację o istniejących niezgodnościach. Wykonawca zobowiązuje się uwzględnić reklamację najpóźniej w terminie 14 (czternastu) dni roboczych od dnia jej otrzymania poprzez wymianę 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 § 7 ust. 4 Umowy.

[2] W przypadku dostarczenia rozwiązania równoważnego.
[3] W przypadku dostarczenia rozwiązania równoważnego.

§ 4

1. Z tytułu należytego wykonania Przedmiotu Umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w kwocie ……. (słownie: …… i …/100) złotych netto, powiększonej o kwotę należnego podatku od towarów i usług, tj. w kwocie ……. (słownie …… i …/100) 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. Wynagrodzenie płatne jest po realizacji dostawy Oprogramowania i ewentualnym przeprowadzeniu wdrożenia Oprogramowania[4] bez zastrzeżeń, na podstawie prawidłowo wystawionej i doręczonej do siedziby Zamawiającego faktury VAT albo odebranej przez Zamawiającego przesłanej przez Wykonawcę ustrukturyzowanej faktury elektronicznej, w sposób wskazany w art. 4 ust. 1 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 2018 r. poz. 2191, 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, w terminie 30 (trzydziestu) dni od dnia jej doręczenia albo odebrania.
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 drogą elektroniczną i wstrzymania płatności z faktury do czasu spełnienia przez Wykonawcę wymogu opisanego w zdaniu poprzednim, a termin płatności z danej faktury ulega wydłużeniu o czas tej zwłoki. 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 przekroczyłby 30 dni, liczonych od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury, Zamawiający zrealizuje płatność na rachunek wskazany przez Wykonawcę i złoży zawiadomienie o zapłacie należności na ten

[4] W przypadku dostarczenia rozwiązania równoważnego.

rachunek do naczelnika urzędu skarbowego właściwego dla Wykonawcy w terminie 3 (trzech) dni od dnia zlecenia przelewu oraz poinformuje Wykonawcę droga 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 2019 r. poz. 1292, z późn. zm.), obejmujących 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 2020 r. poz. 106, z późn. zm.) umieści wyrazy „mechanizm podzielonej płatności" zgodnie z art. 106e ust. 1 pkt 18a ustawy o podatku od towarów i usług.
7. Wykonawca wystawi fakturę VAT na podstawie podpisanego przez Zamawiającego Protokołu odbioru Oprogramowania, bez zastrzeżeń.
8. Za dzień zapłaty uważa się dzień wydania dyspozycji przelewu z rachunku bankowego Zamawiającego.

§ 5

1. Na dostarczone Oprogramowanie Wykonawca udziela Zamawiającemu gwarancji na okres **12 (dwunastu) miesięcy**, liczony od dnia następującego po dniu podpisania bez zastrzeżeń Protokołu odbioru Oprogramowania.
2. Obowiązki Wykonawcy wynikające z udzielonej gwarancji obejmują usuwanie wszelkich wad Oprogramowania, poprzez jego naprawę, jeśli jest to możliwe w danym przypadku lub wymianę na nowe wedle wyboru Zamawiającego. Ewentualnych napraw Wykonawca dokonuje w siedzibie Zamawiającego, przy ul. Nowogrodzkiej 47A w Warszawie.
3. W przypadku ujawnienia się jakiejkolwiek wady Oprogramowania w okresie gwarancji, Zamawiający dokona zgłoszenia tego faktu Wykonawcy na piśmie lub na adres mailowy Wykonawcy wskazany w § 11 ust. 1 pkt. 1 Umowy. Wykonawca usunie zgłoszoną wadę na koszt własny w terminie określonym przez Zamawiającego, zgodnym z SOPZ i gwarancją producenta Oprogramowania. Okres gwarancji ulega przedłużeniu o czas trwania usuwania wady przez Wykonawcę.
4. W przypadku przekroczenia terminu, w którym powinno nastąpić usunięcie wady, o którym mowa w ust. 3, Zamawiający może dokonać usunięcia wady, w tym dokonać wymiany Oprogramowania na niewadliwe na koszt i ryzyko Wykonawcy oraz niezależnie od powyższego, Zamawiający ma prawo naliczyć kary umowne, o których mowa w § 7 ust. 5 Umowy.

5. Na uzasadniony wniosek Wykonawcy, Zamawiający może wydłużyć pierwotnie określony termin do zrealizowania naprawy gwarancyjnej, o którym mowa w ust. 3.
6. Wykonawca będzie wykonywał usługi gwarancyjne przy wykorzystaniu własnych materiałów, sprzętu i narzędzi.
7. Postanowienia, o których mowa w ust. 1-6 stosuje się odpowiednio do realizacji uprawnień Zamawiającego z tytułu rękojmi. Strony zgodnie postanawiają, że gwarancja Wykonawcy nie wyłącza, nie ogranicza ani nie zawiesza uprawnień kupującego wynikających z przepisów o rękojmi za wady.
8. Wykonawca zapewnia, że Oprogramowanie jest wolne od jakichkolwiek wad fizycznych i wad prawnych.
9. W przypadku stwierdzenia wady prawnej Oprogramowania Zamawiający jest zobowiązany w terminie 15 (piętnastu) dni kalendarzowych zawiadomić o tym na piśmie Wykonawcę i w razie potrzeby wezwać go do udziału w sprawie.
10. Dokonanie odbioru Oprogramowania nie zwalnia Wykonawcy z odpowiedzialności z tytułu rękojmi lub gwarancji, choćby w chwili jego wydania lub odbioru, a także zawarcia Umowy, Zamawiający z łatwością mógł się dowiedzieć o wadzie.
11. Zamawiający nie ma obowiązku zbadania Oprogramowania. Strony wyłączają stosowanie do Umowy przepisu art. 563 § 1 i 2 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2019 r. poz. 1145, ze zm.).
12. Wykonawca zwalnia Zamawiającego od wszelkiej odpowiedzialności w przypadku jakichkolwiek roszczeń osób trzecich dotyczących Przedmiotu Umowy.
13. W przypadku jakichkolwiek roszczeń osób trzecich zgłoszonych wobec Zamawiającego w sądzie lub poza sądem, o ile takie roszczenia są związane z naruszeniem praw osób trzecich, Wykonawca podejmie na swój koszt wszelkie działania w celu rozwiązania takiego sporu, łącznie z prowadzeniem postępowania sądowego. W takim przypadku Wykonawca zobowiązany jest do naprawienia wszelkich strat powstałych z tego tytułu, w szczególności do pokrycia wszelkich odszkodowań oraz innych kosztów wynikających z tego tytułu. Powyższe zobowiązanie dotyczy również sytuacji zaistniałych mimo odstąpienia od Umowy.

§6

1. Zamawiający może od Umowy odstąpić w przypadku gdy:

1) Wykonawca nie wykonuje Umowy lub jej części 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 upływu terminu wyznaczonego w wezwaniu;
5) w celu zawarcia Umowy Wykonawca przedstawił fałszywe oświadczenia lub dokumenty – w terminie 30 (trzydziestu) kalendarzowych dni od dnia powzięcia wiadomości o powyższych okolicznościach;
6) podane przez Wykonawcę w ofercie informacje nie odpowiadają stanowi faktycznemu – w terminie 30 (trzydziestu) kalendarzowych dni 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 zmiany 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 wypadku może nastąpić w terminie 30 dni kalendarzowych od powzięcia wiadomości o tych okolicznościach, co wynika z art. 145 ust 1 ustawy pzp.

2. W przypadkach określonych w ust. 1, Wykonawca może żądać od Zamawiającego wyłącznie wynagrodzenia z tytułu należytego wykonania części Umowy do momentu złożenia przez Zamawiającego oświadczenia o odstąpieniu od Umowy, o ile Przedmiot Umowy wykonany do czasu złożenia przez Zamawiającego oświadczenia o odstąpieniu od Umowy przez Zamawiającego, przejawia dla Zamawiającego jakąkolwiek wartość. 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.

§7

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 opóźnienia 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 opóźnienia.
4. W razie odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 20 % 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 5 % 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.

§8

1. Wykonawca zobowiązuje się zachować w poufności wszelkie informacje techniczne, technologiczne, ekonomiczne, finansowe, handlowe, prawne, organizacyjne i inne dotyczące drugiej Strony, otrzymane od drugiej Strony 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 i przekazane drugiej Stronie, zwane dalej "Informacjami". Powyższe zobowiązanie pozostaje w mocy również po wygaśnięciu Umowy, bezterminowo.
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. 4 i 5.
3. Wymogi zawarte w niniejszym paragrafie nie będą miały zastosowania odnośnie jakichkolwiek Informacji, które zostały opublikowane lub podane do publicznej wiadomości przed zawarciem Umowy.
4. W przypadku skierowania przez uprawniony organ żądania ujawnienia Informacji, Wykonawca, dokona natychmiastowego powiadomienia Zamawiającego o wystąpieniu takiego żądania i jego okolicznościach towarzyszących.
5. Jeżeli ujawnienie Informacji jest konieczne z uwagi na obowiązujące przepisy prawa, Wykonawca ujawniający Informacje zobowiązuje się dołożyć wszelkich starań dla uzyskania wiarygodnego zapewnienia od podmiotu, któremu Informacje są ujawniane, że nie będą ujawniane dalej.
6. Wykonawca ponosi odpowiedzialność za przestrzeganie postanowień niniejszego paragrafu przez wszystkie osoby, którymi posługuje się przy wykonywaniu Umowy.

§9

1. Wykonawca wniósł zabezpieczenie należytego wykonania Umowy w wysokości 5% wynagrodzenia brutto określonego w § 4 ust. 1 Umowy, w formie ....
2. W trakcie realizacji Umowy Wykonawca może dokonać zmiany formy zabezpieczenia na zasadach określonych w art. 149 ustawy pzp.
3. Zmiana formy zabezpieczenia, o której mowa w ust. 2, musi być dokonana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.
4. Zamawiający 100% wysokości zabezpieczenia zwróci w terminie 30 (trzydziestu) dni kalendarzowych od dnia zakończenia okresu obowiązywania licencji na Oprogramowanie.

§10

Prawa i obowiązki Wykonawcy wynikające z realizacji Umowy oraz wierzytelności wobec Zamawiającego nie mogą być przenoszone na osoby trzecie bez uprzedniej pisemnej zgody Zamawiającego.

§11

1. Strony postanawiają, że do kontaktów pomiędzy Stronami oraz do podejmowania bieżących uzgodnień związanych z realizacją Umowy wyznaczeni są:

1) ze strony Wykonawcy: **.....,** tel.: **.....,** adres e-mail: **.....;**
2) ze strony Zamawiającego: **……..**, tel.: **……..**, adres e-mail: **……..**.

2. Osobą uprawnioną do podpisania Protokołu odbioru jest:

1) ze strony Wykonawcy: ....., tel.: ....., adres e-mail: .....;
2) ze strony Zamawiającego: **……**, tel.: **……**, adres e-mail**: ……**

3. Zmiana osób i danych, o których mowa w ust. 1 i 2, następuje poprzez pisemne powiadomienie drugiej Strony i nie stanowi zmiany treści Umowy.
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. Wykonawca oświadcza, iż wobec danych osobowych wskazanych w § 14 pełni rolę Administratora danych osobowych a w przypadku opisanym w § 14 ust. 3 i 4, udostępniając opisane dane NCBR, za każdym razem będzie uprawniony do tego typu czynności.
7. Dane osobowe przedstawicieli Stron wymienionych w § 11 oraz 14 udostępniane będą drugiej Stronie, która stanie się ich administratorem danych i przetwarzane będą przez nią w celu realizacji umowy.
8. NCBR podaje, iż wszelkie informacje dotyczące przetwarzania 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.
9. W przypadku, gdy NCBR będzie przetwarzał w ramach niniejszej dane pracowników lub współpracowników Wykonawcy w tym w stosunku do osób uprawnionych do wykonywania prac, o których mowa w § 11 ust. 1 pkt 1 oraz ust. 2 pkt jak i § 14 ust. 2 pkt 1 i 2 Umowy, NCBR 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.
10. Zmiana załączników wskazanych w ust. 8 i 9 nie wymaga zmiany umowy, Strony mogą aktualizować dane zawarte w powyżej wskazanych Klauzulach informacyjnych również poprzez przesłanie wiadomości email.
11. W przypadku konieczności powierzenia Wykonawcy przetwarzania danych osobowych, Strony przed powierzeniem Wykonawcy przetwarzania danych osobowych, zawrą stosowną umowę, zgodnie ze wzorem obowiązującym w NCBR. Odpowiednio w przypadku konieczności udostępnienia Wykonawcy danych osobowych pracowników lub przedstawicieli NCBR, Strony przed udostępnieniem Wykonawcy danych osobowych, zawrą stosowną umowę, zgodnie ze wzorem obowiązującym w NCBR.

§12

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.

§13

1. Zważywszy, że Umowa zawierana jest w związku z wyborem oferty Wykonawcy w przeprowadzonym przez Zamawiającego postępowaniu o udzielenie zamówienia publicznego pt. "Dostawa licencji na system ochrony infrastruktury IT dla NCBR" przeprowadzonym w trybie przetargu nieograniczonego o wartości przekraczającej kwoty określonej w przepisach wydanych na podstawie art. 11 ust. 8 oraz art. 6a ustawy pzp, Strony zgodnie przyjmują, iż, postanowienia Umowy interpretować należy z przyznaniem pierwszeństwa postanowieniom niniejszego paragrafu.
2. Strony mają prawo do przedłużenia terminu zakończenia wykonywania Przedmiotu Umowy o okres trwania przyczyn, z powodu których nie było możliwe wykonanie dostawy, w następujących sytuacjach:

1) jeżeli przyczyny, z powodu których nie było możliwe wykonanie dostawy są następstwem okoliczności, za które odpowiedzialność ponosi Zamawiający,
2) wystąpią opóźnienia w dokonaniu określonych czynności lub ich zaniechanie przez właściwe organy administracji państwowej, które nie są następstwem okoliczności, za które Wykonawca ponosi odpowiedzialność,
3) 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,
4) wystąpienia zdarzeń natury siły wyższej uniemożliwiającej wykonanie Przedmiotu Umowy zgodnie z jej postanowieniami.

3. 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.

4. Wszelkie zmiany Umowy są dokonywane przez umocowanych przedstawicieli Zamawiającego i Wykonawcy w formie pisemnej w drodze aneksu do Umowy, pod rygorem nieważności.
5. 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.

§14

1. Wykonawca może korzystać w toku realizacji Umowy ze świadczeń podwykonawców wyłącznie na zasadach opisanych w niniejszym paragrafie.
2. Wykonawca wykona Przedmiot Umowy przy udziale następujących podwykonawców:
   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 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 2 (dwóch) 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.
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 opóźnienia 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. 22a 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 aneksu.
12. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie Umowy. Wykonawca w pełni i wyłącznie odpowiada za działania lub zaniechania podwykonawców jak za działania własne.
13. Korzystanie ze świadczeń podwykonawców niezgodnie z postanowieniami niniejszego paragrafu traktowane będzie jako istotne naruszenie warunków Umowy oraz przyczynę odstąpienia od Umowy przez Zamawiającego.

§15

Umowa zostaje zawarta na czas oznaczony, tj. od dnia jej zawarcia do dnia wykonania wszystkich obowiązków wynikających z Umowy jednak nie później niż do dnia 26 czerwca 2021 roku.

§16

1. Ewentualne spory wynikłe w związku z realizacją Umowy Strony zobowiązują się rozpatrywać bez zbędnej zwłoki w drodze wspólnych negocjacji, a w przypadku niemożności osiągnięcia kompromisu, spory te będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
2. W sprawach nieregulowanych Umową zastosowanie mają przepisy ustawy Kodeks cywilny oraz ustawy pzp.
3. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego i jeden dla Wykonawcy.
4. Integralną część Umowy stanowią załączniki:

1) Załącznik nr 1 – kopia upoważnienia;
2) Załącznik nr 2 - wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Wykonawcy;
3) Załącznik nr 3 - Szczegółowy opis przedmiotu zamówienia;
4) Załącznik nr 4 – Oferta Wykonawcy z dnia .....;
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 do Umowy

Szczegółowy opis przedmiotu zamówienia (SOPZ)

1. Zamawiający informuje, że jest w posiadaniu licencji ważnych do dnia 2019-12-14:
   1..1. **McAfee Complete Data Protection Advanced – 600 szt.**
   1..2. **McAfee Threat Intelligence Exchange - 600 szt.**
   1..3. **McAfee Complete EndPoint Threat Protection Enterprise - 600 szt.**
   1..4. **McAfee Virtual Advanced Threat Defence Appliance - 1 szt.**
2. Zamawiający informuje, że jest w posiadaniu licencji do dnia 2020-05-25:
   3.2. **McAfee Complete Data Protection Advanced – 100 szt.**
   3.2. **McAfee Threat Intelligence Exchange - 100 szt.**
   3.2. **McAfee Complete EndPoint Threat Protection Enterprise - 100 szt.**
3. Przedmiotem zamówienia jest:

Zakup i dostawa licencji na oprogramowanie McAfee lub oprogramowanie równoważne na system ochrony infrastruktury IT, składających się z:

3.1 Odnowienie McAfee Complete Data Protection Advanced – w ilości 600 (sześciuset) szt. ważnych od dnia 2019-12-15 do dnia 2021-05-25 roku;

3.2 Odnowienie McAfee Threat Intelligence Exchange - w ilości 600 (sześciuset) szt. ważnych od dnia 2019-12-15 do dnia 2021-05-25 roku;

3.3 Odnowienie McAfee Threat Complete EndPoint Protection Enterprise – w ilości 600 (sześciuset) szt. ważnych od dnia 2019-12-15 do dnia 2021-05-25 roku;

3.4 Odnowienie McAfee Virtual Advanced Threat Defence Appliance – w ilości 1 (jednej) szt. ważnej od dnia 2019-12-15 do dnia 2021-05-25 roku

3.5 Odnowienie McAfee Complete Data Protection Advanced – w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku

3.6 Odnowienie McAfee Threat Intelligence Exchange - w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku

3.7 Odnowienie McAfee Complete EndPoint Threat Protection Enterprise - w ilości 100 (stu) szt. ważnej od dnia 2020-05-26 do dnia 2021-05-25 roku

3.8 Nowe licencje McAfee Complete Data Protection Advanced – w ilości 100 (stu) szt. ważnych od dnia wdrożenia do dnia 2021-05-25 roku

3.9 Nowe licencje McAfee Threat Intelligence Exchange – w ilości 100 (stu) szt. ważnych od dnia wdrożenia do dnia 2021-05-25 roku

3.10 Nowe licencje McAfee Threat Complete EndPoint Protection Enterprise – w ilości 200 (dwustu) szt. ważnych od dnia wdrożenia do dnia 2021-05-25 roku

W razie możliwości należy scalić ze sobą pozycje:

- 3.1 z 3.5 oraz 3.8

- 3.2 z 3.6 oraz 3.9

- 3.3 z 3.7 oraz 3.10

UWAGA

1. Wszystkim użytym w SIWZ nazwom własnym w opisie przedmiotu zamówienia towarzyszą wyrazy **„lub równoważne"**. Zamawiający posłużył się nazwą własną producenta dla ułatwienia opisu przedmiotu, w oparciu o przesłanki art. 29 ust. 3 ustawy Prawo zamówień publicznych.

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).

Moduł służący do ochrony przed wyciekiem danych: Data Loss Prevention (zwany dalej DLP):

Lp.	Konfiguracja minimalna
1.	Oprogramowanie musi zapewniać ochronę przed wyciekiem poufnych danych.
2.	Oprogramowanie musi umożliwiać monitorowanie i powiadamianie o incydentach wycieku danych w czasie rzeczywistym.
3.	Moduł musi posiadać agenta instalowanego na stacjach końcowych oraz Centralną Konsolę Zarządzania (dalej CKZ), pozwalającą z jednego miejsca zarządzać konfiguracją (co najmniej w zakresie obsługi DLP) wszystkich chronionych punktów infrastruktury informatycznej i powiadomieniami modułu DLP.
4.	Rozwiązanie musi być skalowalne i powinno być w stanie zarządzać infrastrukturą złożoną z co najmniej 700 stacji końcowych.
5.	Oprogramowanie musi umożliwiać egzekwowanie polityk ochrony przed wyciekiem danych co najmniej na poziomie stacji końcowych.
6.	Moduł musi być odpowiedzialny za klasyfikację treści oraz wymuszanie ochrony zaklasyfikowanych treści, przeciwdziałając wyciekowi danych. Moduł DLP powinien przeprowadzać klasyfikację treści przy użyciu poniższych mechanizmów: - wyrażenia regularne: dane o określonej strukturze, - atrybuty plików: właściwości plików, takie jak typ i rozmiar, - słowa kluczowe: lista wrażliwych słów i wyrażeń. Klasyfikacja w oparciu o typ/zawartość pliku musi być nadawana w oparciu o następujące parametry: a. Słowa kluczowe występujące w pliku. Powinny być dostępne słowniki predefiniowane oraz możliwość tworzenia własnych. b. Wykrycie fraz w pliku zgodnie ze zdefiniowanym wyrażeniem regularnym. Powinny być predefiniowane wyrażenia wyszukujące co najmniej PESEL, NIP, REGON oraz powinna istnieć możliwość definicji własnych wyrażeń regularnych. c. Podobieństwo do innych, wcześniej zeskanowanych dokumentów. Jeśli dokument zawiera część tekstu zbieżną ze wcześniej zeskanowanym repozytorium – dokument

	powinien być automatycznie klasyfikowany (tzw. fingerprinting). d. Rodzaj pliku poprzez zbadanie faktycznej zawartości pliku niezależnie od rozszerzenia, jakim opatrzony jest dany plik. e. Rozszerzenie pliku niezależnie od zawartości pliku. Nazwy etykiet klasyfikacji danych musi być konfigurowalne przez administratora. Sklasyfikowane dane muszą mieć mechanizm chroniący przed zmianą klasyfikacji poprzez manipulacje nad plikiem. a. Klasyfikacja takiego pliku nie może się zmieniać (w szczególności być gubiona) w przypadku co najmniej zmiany nazwy pliku, zmiany formatu/typu pliku. b. W przypadku skopiowania fragmentu sklasyfikowanego pliku do innego dokumentu, nowy dokument musi dziedziczyć taką samą klasyfikację jak plik oryginalny. W przypadku późniejszego usunięcia tego fragmentu, który przyczynił się do nadania klasyfikacji – klasyfikacja powinna być też usunięta. c. W przypadku przepisania odpowiednio długiego fragmentu pliku do innego dokumentu (bez użycia schowka).
7.	System musi chronić dane przed wyciekiem za pomocą następujących kanałów danych: a. Ochrona przed wyciekiem przy użyciu wydruku. I. Definiowanie ograniczeń w drukowaniu wskazanych dokumentów, w tym możliwość wskazania, które dokumenty mogą być drukowane. II. Monitorowanie, blokowanie drukowania danych na wskazanych drukarkach lokalnych i sieciowych oraz raportowanie takiego zdarzenia obejmujące minimum: nazwę drukarki, nazwę użytkownika, proces, który wysłał dokument do drukowania, adres IP komputera użytkownika, czas zdarzenia. b. Ochrona przed wyciekiem do sieci WEB I. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych, z użyciem przeglądarek webowych do Internetu (protokół http/HTTPS), w tym możliwość wskazania, na jakie adresy powinna być możliwa wysyłka a na jakie nie. II. Monitorowanie, blokowanie wysyłania plików oraz raportowanie takiego zdarzenia obejmującego minimum adres URL, nazwę procesu przeglądarki internetowej. III. Powinny być wspierane co najmniej przeglądarki: Internet Explorer, Firefox oraz Chrome. c. Ochrona przed wyciekiem przez EMAIL I. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych, z użyciem klienta pocztowego Microsoft Outlook. Możliwość uzależnienia ochrony od domen adresów email lub konkretnych adresów email. II. Monitorowanie, blokowanie wysyłania plików oraz raportowanie takiego zdarzenia obejmującego minimum docelowy adres email, proces klienta pocztowego.

	d. Ochrona przed generowaniem zrzutów ekranów I. Definiowanie ograniczeń przy generowaniu zrzutów ekranu, jeśli wyświetlony na nim jest plik sklasyfikowany. II. Monitorowanie, blokowanie realizacji funkcji zrzutu ekranu oraz raportowanie takiego zdarzenia obejmującego minimum aplikację wyświetlającą sklasyfikowaną treść podczas próby zrealizowania zrzutu. e. Ochrona przed skopiowaniem plików na zewnętrzne nośniki danych I. Definiowanie ograniczeń przy kopiowaniu sklasyfikowanych plików na nośniki zewnętrzne. II. Monitorowanie, blokowanie kopiowania oraz raportowanie takiego zdarzenia obejmującego minimum nazwę pliku kopiowanego, numer seryjny nośnika zewnętrznego. f. Ochrona przed użyciem schowka systemowego I. Definiowanie ograniczeń przy kopiowaniu fragmentów dokumentu poprzez schowek systemowy do innych dokumentów. II. Funkcja schowka powinna działać w obrębie tego samego dokumentu bez żadnych przeszkód. III. Monitorowanie, blokowanie kopiowania treści oraz raportowanie takiego zdarzenia obejmującego minimum nazwę aplikacji źródłowej i docelowej. g. Ochrona przed wysyłką danych poprzez sieć I. Definiowanie ograniczeń przy dostępie do sieci dla aplikacji, która wykonuje operacje plikowe na sklasyfikowanych plikach. II. W momencie wykrycia operacji na plikach sklasyfikowanych – aplikacja powinna zostać pozbawiona dostępu do sieci, działanie powinno zostać monitorowane oraz zaraportowane – minimum nazwę procesu, adres IP źródłowy, adres IP docelowy, port źródłowy, port docelowy i kierunek ruchu.
8.	2. Dostępność różnych rodzajów reakcji modułu DLP na wykryte naruszenie polityki ochrony: a. blokowanie akcji (np. blokada wysyłki email ze sklasyfikowanymi załącznikami), b. monitorowania akcji, c. powiadomienie użytkownika (wyświetlenie użytkownikowi informacji, że podjęta akcja została zablokowana/jest monitorowana przez moduł DLP), d. zapytanie użytkownika o podanie powodów wykonywania akcji – powód wpisany przez użytkownika musi być zachowany. e. możliwość automatycznego szyfrowania chronionych plików podczas ich przesyłania do katalogu sieciowego lub na wymienny dysk zewnętrzny – przy czym administrator systemu ma możliwość konfiguracji sposobu szyfrowania, m.in. siły zabezpieczenia.

	f. zachowanie danych rekordów – niezależnie od operacji podstawowej, program zapisze dane oznaczone jako naruszenie polityki do dalszej analizy.
9.	System musi umożliwiać konfigurowanie różnych reguł w zależności od tego, czy system znajduje się w sieci korporacyjnej czy poza nią.
10.	Wszystkie incydenty związane z naruszeniem danych muszą mieć nadany priorytet w co najmniej pięciostopniowej skali tak, by możliwe było odróżnienie incydentów bardziej istotnych od mniej istotnych.
11.	1. Moduł DLP musi umożliwiać natywne, okresowe przeszukiwanie dysków twardych na stacjach roboczych pod kątem występowania tam plików niesklasyfikowanych a spełniających wymogi do sklasyfikowania. W razie wykrycia takiego pliku powinno być możliwe wykonanie akcji: a. przesłanie powiadomienia do serwera zarządzającego lub zapis w logu, b. przeniesienie pliku do bezpiecznej lokalizacji, c. automatyczne szyfrowanie plików. 2. musi istnieć możliwość definiowania harmonogramu skanowania okresowego w celu przeszukiwania dysków twardych.
12.	1. System musi posiadać możliwość kontroli urządzeń podłączanych do komputera. Powinna być możliwość kontroli dowolnego urządzenia wykrywanego przez system Windows w ramach urządzeń Plug and Play. 2. W ramach kontroli urządzeń powinna istnieć możliwość dopuszczania urządzeń o specyficznych atrybutach. 3. W przypadku przenośnych nośników danych – powinna istnieć możliwość blokowania dostępu do takich urządzeń w oparciu o numer seryjny urządzenia lub podmontowanie urządzenia w trybie tylko do odczytu.
13.	Oprogramowanie musi posiadać możliwość wysyłania powiadomienia za pomocą poczty elektronicznej oraz SNMP.
14.	Oprogramowanie musi posiadać możliwość pracy agenta zainstalowanego na stacji końcowej w trybie offline, bez kontaktu z serwerem zarządzającym.

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.	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.
20.	System musi zapewniać automatyczne szyfrowanie tzw. pliku wymiany Windows (pagefile).

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 nośnikizewnętrzne USB oraz CD/DVD. c. integrację z podsystemem ochrony przed wyciekiem danych – DLP opisanym powyżej – co najmniej poprzez wymuszenie szyfrowania plików kopiowanych na nośniki USB z poziomu polityki DLP.
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.

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).

	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.

9.	**Sandbox** 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.).
10.	**Wirtualne patche** Moduł ochrony przed znanymi, niezałatanymi podatnościami (Wirtualne Patche, zwany dalej WP). 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 powinien wspierać systemy począwszy od wersji klienckich Windows 7/8 po serwerowe Windows 2012/R2. Moduł będzie chronił co najmniej stacje robocze.
11.	**Zapobieganie epidemii**

	W celu ochrony komputerów przed zagrożeniami zaproponowane rozwiązanie skanuje pliki i wykonuje określone czynności przy każdym wykrytym zagrożeniu bezpieczeństwa. Bardzo duża liczba zagrożeń bezpieczeństwa wykrytych w krótkim przedziale czasu sugeruje epidemię. W celu odizolowania epidemii, muszą istnieć mechanizmy wdrażania zasady ochrony przed epidemią i izolacji zarażonych komputerów tak długo, aż zagrożenia zostaną usunięte.
Moduł Antywirusowy (dalej AV)	
12.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z AV.
13.	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.
14.	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.
15.	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.
16.	System AV musi zapewnić ochronę przed programami typu Spyware oraz Potencjalnie Niechcianymi Programami.
17.	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.
18.	System AV musi mieć możliwość skanowania sektorów rozruchowych dysków.
19.	System AV musi mieć możliwość skanowania dysków sieciowych.
Modułu firewall (dalej FW)	
20.	Moduł FW ma za zadanie kontrolować ruch przychodzący i wychodzący ze stacji roboczej i wymuszać politykę dopuszczonego ruchu wymuszaną przez Administratora.
21.	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.
22.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu

	Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z FW.
23.	Wszystkie reguły muszą być zarządzane z poziomu Centralnej Konsoli Zarządzania i rozpatrywane w kolejności wystąpienia.
24.	Wszystkie reguły muszą mieć możliwość logowania wystąpienia danego ruchu i jego przeglądania z poziomu Centralnej Konsoli Zarządzającej.
25.	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.
26.	Moduł FW musi mieć możliwość izolacji ruchu sieciowego pomiędzy różnymi interfejsami sieciowymi.
27.	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.
28.	Moduł FW powinien dawać możliwość ograniczania ruchu do/ze stacji roboczej zanim usługi modułu FW będą aktywne.
Modułu ochrony przeglądarek webowych przed złośliwymi stronami web (dalej WP)	
29.	Moduł WP musi współpracować co najmniej z następującymi przeglądarkami: Microsoft Internet Explorer, Mozilla Firefox i Google Chrome działającymi na stacjach roboczych.
30.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z ochroną ruchu webowego.
31.	Producent modułu WP musi dokładać wszelkich starań, by zapewniać wsparcie dla nowych wersji przeglądarek niedługo po ich ukazaniu się.
32.	Zaproponowane rozwiązanie winno posiadać mechanizm uniemożliwiający wyłączenie ochrony ruchu webowego przez użytkownika na stacji roboczej.
33.	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.
34.	W przypadku zidentyfikowania próby dostępu do strony o złej reputacji, mechanizmy aplikacji winny umożliwiać blokowanie dostępu do strony, jednocześnie wyświetlając użytkownikowi stosowny komunikat.
35.	Moduł WP musi posiadać możliwość sprawdzania reputacji obiektów ściągniętych ze strony oraz skanowania ich poprzez przekazanie ich do innych modułów, w tym AV.
36.	Moduł WP musi wykrywać ładowanie stron typu „phishing”, które podszywają się pod inne strony cieszące się dobrym zaufaniem.
37.	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.

38.	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.
39.	Zasady ostrzegania i blokowania dostępu do stron muszą działać także w sytuacji, kiedy stacja robocza pracuje poza siecią firmową Zamawiającego.
Modułu Host IPS (dalej HIPS)	
40.	Oferowane oprogramowanie musi oferować funkcjonalność Host IPS i zapobiegać włamaniom, korzystając z reguł zabezpieczających stację roboczą i uniemożliwiających wykorzystanie podatności aplikacji i systemu operacyjnego.
41.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z obsługą IPS.
42.	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.
43.	Oprogramowanie host IPS musi wykrywać i zapobiegać atakom przepełnienia bufora (Buffer Overflow) we wszystkich aplikacjach działających na chronionej stacji roboczej.
44.	Do każdej sygnatury musi być dołączony opis, który opisuje działanie sygnatury i w miarę możliwości odwołuje się do bazy CVE.
45.	Zaoferowane rozwiązanie musi oferować możliwość pisania własnych sygnatur IPS i wysłania ich na chronione systemy.
46.	Oprogramowanie musi uniemożliwiać zmianę konfiguracji IPS przez użytkownika na stacji roboczej.
Modułu kontroli portów (dalej KP)	
47.	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.
48.	Moduł musi mieć możliwość: logowania zdarzeń, powiadamiania użytkowników o zdarzeniach, blokowania/dopuszczania urządzeń zgodnie z konfiguracją.
49.	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.
50.	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).
51.	Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania zewnętrznych nośników danych USB na podstawie ich numeru seryjnego, ID producenta i ID produktu.
52.	Polityka działania modułu musi umożliwiać przypisanie różnych polityk zależnie od przynależności użytkownika do grup użytkowników synchronizowanych z Active Directory.
Modułu kontroli aplikacji (dalej KA)	
53.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy kontroli aplikacji (KA).
54.	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.
55.	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.
56.	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.
57.	Oprogramowanie KA musi być chronione przed nieupoważnionym zatrzymaniem lub odinstalowaniem.
58.	Rozwiązanie musi zapewnić taki sam poziom ochrony niezależnie od tego czy stacja robocza pracuje w sieci firmowej czy poza nią – bez dostępu do CKZ.
59.	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.
60.	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.

61.	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.
62.	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.
63.	Rozwiązanie KA musi umożliwiać wyświetlenie użytkownikowi komunikatu na stacji z informacją o zablokowaniu uruchomienia aplikacji/procesu.
64.	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)	
65.	Moduł OPE ma realizować ochronę serwerów poczty elektronicznej pracujących pod kontrolą MS Exchange 2013 i nowszych, wykorzystywanych przez Zamawiającego.
66.	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.

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: - DLP, - 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.

Moduł DLP:

Lp.	
1.	**Ochrona na bramie SMTP** Oprogramowanie musi umożliwiać egzekwowanie polityk ochrony przed wyciekiem danych na poziomie bramy kontrolującej ruch poczty elektronicznej.
2.	**Ochrona na bramie WEB** Oprogramowanie musi umożliwiać egzekwowanie polityk ochrony przed wyciekiem danych na poziomie bramy kontrolującej ruch webowy.
3.	**Moduł klasyfikacji treści** Moduł DLP musi umożliwić przeprowadzenie klasyfikacji plików w oparciu o etykiety.

	Klasyfikacja w oparciu o etykiety powinna być nadawana ręcznie lub automatycznie. Powinny być dostępne co najmniej następujące mechanizmy nadawania etykiet: a. Automatyczne nadawanie etykiet w zależności od udziału sieciowego, z którego dany plik został skopiowany na stację roboczą. b. Automatyczne nadawanie etykiet w zależności od aplikacji, która wytworzyła dany plik na danej stacji roboczej. c. Ręczne nadawanie etykiet dla wskazanych w konfiguracji użytkowników, pozwalające na klasyfikację plików poprzez manualne wskazanie przez użytkownika typu pliku i jego ważności. Klasyfikacja w oparciu o etykiety powinna mieć mechanizmy chroniące przed „zgubieniem" tych etykiet poprzez manipulacje nad plikiem. a. Klasyfikacja takiego pliku nie może się zmieniać (w szczególności być gubiona) w przypadku, co najmniej zmiany nazwy pliku, zmiany formatu/typu pliku. b. W przypadku skopiowania fragmentu tak sklasyfikowanego pliku do innego dokumentu, nowy dokument musi dziedziczyć taką samą klasyfikację jak plik oryginalny. W przypadku późniejszego usunięcia tego fragmentu, który przyczynił się do nadania klasyfikacji – klasyfikacja powinna być też usunięta. c. W przypadku przepisania odpowiednio długiego fragmentu pliku do innego dokumentu (bez użycia schowka), nowy dokument musi dziedziczyć taką samą klasyfikację jak plik oryginalny. Nazwy etykiet klasyfikacji danych – zarówno dotyczących klasyfikacji w oparciu o typ/zawartość jak i klasyfikacji w oparciu o etykiety powinny być konfigurowalne przez administratora. Etykiety klasyfikacji plików dołączanych do wiadomości e-mail powinny być przekazywane przez email poprzez nadawanie nagłówków do wiadomości lub w inny, podobny sposób tak, by w momencie zapisywania na system plików na innej stacji roboczej – odpowiednia klasyfikacja była automatycznie nadawana.
4.	**Moduł akceptacji polityk bezpieczeństwa** Moduł DLP musi umożliwiać wyświetlenie użytkownikowi, przy pierwszym użyciu aplikacji, informacji o zasadach polityki procesu klasyfikacji wraz z funkcją potwierdzenia przez użytkownika zapoznania się z w/w polityką.
5.	**Moduł budowania etykiet** Moduł DLP posiada kreator podpowiedzi, oparty o konfigurowalny mechanizm pytań powiązanych z algorytmem decyzyjnym, który pozwoli podjąć użytkownikowi decyzję jak zaklasyfikować dane.
6.	**DLP - obsługa dodatkowych typów transmisji** Moduł DLP **wspiera przynajmniej pięć** z poniższych typów/protokołów transmisji danych: 1. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania

	przesyłanych danych z wykorzystaniem protokołu FTP. 2. Oprogramowanie posiada możliwość monitorowania i ochrony przesyłanych danych z wykorzystaniem aplikacji wiadomości błyskawicznych. 3. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania przesyłanych danych z wykorzystaniem protokołu SMB. 4. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania przesyłanych danych z wykorzystaniem poczty elektronicznej obsługiwanej za pośrednictwem stron Webowych zarówno w zakresie załączników jak i tekstu wpisywanego bezpośrednio do maila. 5. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania przesyłanych danych z wykorzystaniem aplikacji wymiany plików peer-to-peer. 6. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania przesyłanych danych z wykorzystaniem SMTP zarówno w zakresie dołączonych załączników jak i tekstu wpisywanego bezpośrednio do maila. 7. Oprogramowanie posiada możliwość monitorowania i ochrony w tym blokowania danych nagrywanych na nośniki optyczne CD/DVD.

Ochrona serwerów fizycznych oraz wirtualnych

Lp.	Ochrona serwerów
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. System musi zapewnić również technologię wirtualnych patchy (WP), która pozwala na „przykrycie” podatności i blokowanie ataków na nią skierowanych bez rzeczywistego jej łatania. 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.

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 do Umowy

PROTOKÓŁ ODBIORU OSTATECZNY / CZĘŚCIOWY*

Zamawiający: …….

Reprezentowany przez ……

Wykonawca: ……...

Przedmiot odbioru: ……..

Data dokonania odbioru: ……

Zakres wykonanych prac: ……

…….....

……..

Przedstawiciele **Zamawiający**:	Przedstawiciele **Wykonawcy**:
1. ……	1. ……
2. ……	2. ……
3. ……	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 zakończono 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 / nie przyjęto na skutek ……

……..

……..

Podpisy

Przedstawiciele **Zamawiający**:	Przedstawiciele **Wykonawcy**:
1. ……	1. ……
2. ……	2. ……
3. ……	3. ……

**** niepotrzebne skreślić***

Załącznik nr 6 do Umowy

Klauzula Informacyjna

Zgodnie z art. 13 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 (dalej ogólne rozporządzenie o ochronie danych, „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 (IOD) można się skontaktować poprzez e-mail: iod@ncbr.gov.pl;
3) dane osobowe są przetwarzane w celu zawarcia i realizacji nr ……zawartej w Warszawie w dniu ……. 2020 pomiędzy NCBR a **……..(Wykonawcą)** ;
4) dane osobowe są przetwarzane na podstawie umowy – 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, a następnie w celu archiwalnym przez okres zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;
6) odbiorcami danych osobowych będą Ministerstwo Nauki i Szkolnictwa Wyższego lub 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. Dane te mogą być także przekazywane partnerom IT, podmiotom realizującym wsparcie techniczne lub organizacyjne;
7) 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 danych. W sprawie realizacji praw można kontaktować się z inspektorem ochrony danych pod adresem mailowym udostępnionym w pkt 2 powyżej;
8) przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
9) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego;
10) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Załącznik nr 7 do Umowy

Klauzula informacyjna

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 (dalej ogólne rozporządzenie o ochronie danych, „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 **……..(Wykonawcy).**
3) z inspektorem ochrony danych (IOD) można się skontaktować poprzez adres e-mail – iod@ncbr.gov.pl;
4) NCBR bedzie przetwarzała następujące kategorie Pani/Pana danych osobowych: .....;
5) dane osobowe są przetwarzane w celu zawarcia i realizacji umowy nr ……zawartej w Warszawie w dniu ……. 2020 pomiędzy NCBR a …….**(Wykonawcą)**;
6) - dane osobowe są przetwarzanie do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – realizacją umowy ramowej (art. 6 ust. 1 lit. f RODO);
7) dane osobowe będą przetwarzane w okresie realizacji Umowy, a następnie w celu archiwalnym przez okres zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;
8) odbiorcami danych osobowych będą Ministerstwo Nauki i Szkolnictwa Wyższego lub 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. Dane te mogą być także przekazywane partnerom IT, podmiotom realizującym wsparcie techniczne lub organizacyjne; dane osobowe w zakresie wizerunku w ramach świadczenia usług tłumaczenia będę udostępniane członkom wydarzeń, które podlegać będą tłumaczeniu jak również możliwe będzie uwiecznianie takich wydarzeń wskutek czego dane dotyczące wizerunku będę udostępnianie nieograniczonemu kręgowi osób w Internecie;
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 przenoszenia danych jak również do wniesienia sprzeciwu. W sprawie realizacji praw można kontaktować się z inspektorem ochrony danych pod adresem mailowym udostępnionym w pkt 2 powyżej;
10) przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
11) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego;
12) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.